Exhibit A

Geisel, Sally (DFS)

From: portal@dfs.ny.gov
Sent: Monday, November 03, 2014 3:11 PM
To: dfs.sm.Electronic.FOIL.Submissions
Subject: A new FOIL e-form was submitted. Submission #83898

This is an auto-generated message sent to notify you that a FOIL e-form was submitted on 2014-11-03 at 15:11:10.

Submission ID = 83898
First Name = Theo
Last Name = Chino
Business Name =
Address = 640 riverside Drive 10B New York, NY 10031 Daytime Phone = 212 694 9968 Email = dfsFOIL@theochino.com

Client would like to recieve copies by: Email

Record Description = New York's DFS may create 'Transitional BitLicense' for bitcoin

I am requesting the drafts proposed about the Transitional BitLicense regarding small businesses.
Bureaus believed to have these records:
Requested Service Office = NYC

Regards,
Portal Admin

NEW YORK STATE
DEPARTMENT of
FINANCIAL SERVICES

Andrew M. Cuomo
Governor

Benjamin M. Lawsky
Superintendent

December 5, 2014

Theo Chino
640 Riverside Drive, Apt. 10B
New York, NY 10031
Email: dfsFOIL@theochino.com

Re: **Freedom of Information Law ("FOIL") Request No. 14-222: Copies of Proposed Drafts Relative to Transitional BitLicense and Small Businesses.**

Dear Mr. Chino:

The Department of Financial Services (Banking Division) is currently in the process of responding to your Freedom of Information Law ("FOIL") request. Please note the number of your request captioned above.

The Department attempts to process FOIL requests as expeditiously as possible. However, because of the Department's limited legal staff and large number of requests for records it is anticipated that a response will be forthcoming ***within*** 120 days from the date of this letter. Please call me at (212) 709-1656 should you have any questions.

Sincerely,

Harold D. Frye

Administrative Assistant

NEW YORK STATE
DEPARTMENT of
FINANCIAL SERVICES

Andrew M. Cuomo
Governor

Benjamin M. Lawsky
Superintendent

November 6, 2014

Theo Chino
640 Riverside Drive, Apt. 10B
New York, NY 10031
Email: dfsFOIL@theochino.com

Re: **Freedom of Information Law ("FOIL") Request No. 14-222: Copies of Proposed Drafts Relative to Transitional BitLicense and Small Businesses.**

Dear Mr. Chino:

The Department of Financial Services (Banking Division) is currently in the process of responding to your Freedom of Information Law ("FOIL") request. Please note the number of your request captioned above.

It is anticipated that the response will be completed within 20 business days from the date of this acknowledgment letter. Please feel free to contact me at (212) 709-1656 should you have any questions.

Sincerely,

Harold D. Frye
Administrative Assistant

NEW YORK STATE
DEPARTMENT *of*
FINANCIAL SERVICES

Andrew M. Cuomo
Governor

Benjamin M. Lawsky
Superintendent

April 3, 2015

Theo Chino
640 Riverside Drive, Apt. 10B
New York, NY 10031
Email: dfsFOIL@theochino.com

Re: FOIL Request No. 14-222

This is in response to your above-referenced request for information made to New York State Department of Financial Services ("the Department") under New York's Freedom of Information Law (New York Public Officers Law ("POL") §87). As to the records you requested, please be advised that:

☐ 1. The Department is providing all the records requested.

☐ 2. The Department is providing all records requested that are in its possession.

☐ 3. The Department does not have any of the records requested.

☐ 4. The Department is in possession of all of the records requested. Certain records provided have been redacted and/or not provided in whole for the reason(s) indicated below.

X 5. The Department is in possession of some of the records requested. Certain of those records have been redacted and/or not provided in whole for the reason(s) indicated below.

☐ A. **Exempt from disclosure by State or Federal statute** POL 87(2) (a)

a) ☐ **Examination/Investigatory material** exempt under BL 36(10)

b) ☐ **Other**

☐ B. **Unwarranted invasion of personal privacy** POL 87(2) (b)

☐ C. **Impairment of contract awards negotiations** POL 87(2) (c)

☐ D. **Trade secrets or submitted to an agency by, or derived from information obtained by, a commercial enterprise, which if disclosed would cause substantial injury to the competitive position of the enterprise** POL 87(2)(d)

☐ E. **Compiled for law enforcement purposes which, if disclosed, would cause one or more of the harms** POL 87(2) (e) (i)-(iv)

☐ F. **Endanger life or safety** POL 87(2) (f)

X J. **Inter-agency/intra-agency materials which are not described in** POL 87(2) (g) (i)-(iv)

Any decision of the Department not to disclose records based on the section(s) of law specified above may be appealed, in writing, to the Department of Financial Services within 30 days pursuant to New York Public Officers Law § 89. If you have any questions, please contact Harold Frye, Administrative Assistant, at (212) 709-1656.

Sincerely,

Dana Syracuse
Associate General Counsel
Office of General Counsel

Exhibit B

NEW YORK STATE
DEPARTMENT *of*
FINANCIAL SERVICES

Andrew M. Cuomo
Governor

Anthony J. Albanese
Acting Superintendent

August 4, 2015

Transmitted via E mail: DFSFoilRequest@theochino.com
Mr. Theo Chino
640 Riverside Drive #10 B
New York, NY 10031

Re: DFS FOIL No. 2015-061185: Request for information on phone inquiries to the NY State Department of Financial Services concerning Bit Licenses

Dear Mr. Chino:

This is in response to your above-referenced request for information made to New York State Department of Financial Services ("the Department") under New York's Freedom of Information Law (New York Public Officers Law ("POL") §87). As to the records you requested, please be advised that:

☐ 1. The Department is providing all the records requested.

☐ 2. The Department is providing all records requested that are in its possession.

☒ 3. The Department does not have any of the records requested.

☐ 4. The Department is in possession of all of the records requested. Certain records provided have been redacted and/or not been provided in whole for the reason(s) indicated below.

☐ 5. The Department is in possession of some of the records requested. Certain of those records have been redacted and/or not provided in whole for the reason(s) indicated below.

☐ A. **Exempt from disclosure by State or Federal statute** POL 87(2) (a)

a)) ☐ Examination/Investigatory material exempt under BL 36(10)

b) ☐ **Other**

☐ B. Unwarranted invasion of personal privacy POL 87(2) (b)

☐ C. **Impairment of contract awards negotiations** POL 87(2) (c)

☐ D. **Trade secrets or submitted to an agency by, or derived from information obtained by, a commercial enterprise, which if disclosed would cause substantial injury to the competitive position of the enterprise** POL 87(2)(d)

☐ E. **Compiled for law enforcement purposes which, if disclosed, would cause one or more of the harms** POL 87(2) (e) (i)-(iv)

☐ F. **Endanger life or safety** POL 87(2) (f)

☐ G. **Inter-agency/intra-agency materials which are not described in** POL 87(2) (g) (i)-(iv)

Any decision of the Department not to disclose records based on the section(s) of law specified above may be appealed, in writing, to the Department of Financial Services within 30 days pursuant to New York Public Officers Law § 89. If you have any questions, please contact George Bogdan at (212) 480-4758 or George.Bogdan@dfs.ny.gov.

Sincerely,

George Bogdan
Senior Attorney
Office of General Counsel

Exhibit C

NEW YORK STATE
DEPARTMENT *of*
FINANCIAL SERVICES

Andrew M. Cuomo
Governor

Anthony J. Albanese
Acting Superintendent

August 4, 2015

Transmitted via E mail: DFSFoilRequest@theochino.com
Mr. Theo Chino
640 Riverside Drive #10 B
New York, NY 10031

Re: DFS FOIL No. 2015-061185: Request for information on phone inquiries to the NY State Department of Financial Services concerning Bit Licenses

Dear Mr. Chino:

This is in response to your above-referenced request for information made to New York State Department of Financial Services ("the Department") under New York's Freedom of Information Law (New York Public Officers Law ("POL") §87). As to the records you requested, please be advised that:

☐ 1. The Department is providing all the records requested.

☐ 2. The Department is providing all records requested that are in its possession.

☒ 3. The Department does not have any of the records requested.

☐ 4. The Department is in possession of all of the records requested. Certain records provided have been redacted and/or not been provided in whole for the reason(s) indicated below.

☐ 5. The Department is in possession of some of the records requested. Certain of those records have been redacted and/or not provided in whole for the reason(s) indicated below.

☐ A. **Exempt from disclosure by State or Federal statute** POL 87(2) (a)

a)) ☐ Examination/Investigatory material exempt under BL 36(10)

b) ☐ **Other**

☐ B. Unwarranted invasion of personal privacy POL 87(2) (b)

☐ C. **Impairment of contract awards negotiations** POL 87(2) (c)

☐ D. **Trade secrets or submitted to an agency by, or derived from information obtained by, a commercial enterprise, which if disclosed would cause substantial injury to the competitive position of the enterprise** POL 87(2)(d)

☐ E. **Compiled for law enforcement purposes which, if disclosed, would cause one or more of the harms** POL 87(2) (e) (i)-(iv)

☐ F. **Endanger life or safety** POL 87(2) (f)

☐ G. **Inter-agency/intra-agency materials which are not described in** POL 87(2) (g) (i)-(iv)

Any decision of the Department not to disclose records based on the section(s) of law specified above may be appealed, in writing, to the Department of Financial Services within 30 days pursuant to New York Public Officers Law § 89. If you have any questions, please contact George Bogdan at (212) 480-4758 or George.Bogdan@dfs.ny.gov.

Sincerely,

George Bogdan
Senior Attorney
Office of General Counsel

Exhibit D

Ithaca Hours

From Wikipedia, the free encyclopedia

The **Ithaca HOUR** is a local currency used in Ithaca, New York and is the oldest and largest local currency system in the United States that is still operating.[1] It has inspired other similar systems in Madison, Wisconsin; Corvallis, Oregon;[2] and a proposed system in the Lehigh Valley, Pennsylvania.[3] One Ithaca HOUR is valued at US$10 and is generally recommended to be used as payment for one hour's work, although the rate is negotiable.

Ithaca Hours	
ISO 4217 code	N/A, local currencies don't have ISO 4217 codes
Central bank	Ithaca Hours, Inc
Website	ithacahours.info (http://ithacahours.info)
Date of introduction	November 1991
User(s)	Ithaca, NY, United States
Pegged with	1 hour = US$10
Plural	hours
Banknotes	
Freq. used	1/10, ⅛, ¼, ½, 1 & 2 Hours

Contents

The currency

Ithaca HOURS are not backed by national currency and cannot be freely converted to national currency, although some businesses may agree to buy them.[4]

HOURS are printed on high-quality paper and use faint graphics that would be difficult to reproduce, and each bill is stamped with a serial number, in order to discourage counterfeiting.[2][5]

In 2002, a one-tenth hour bill was introduced, partly due to the encouragement and funding from Alternatives Federal Credit Union and feedback from retailers who complained about the awkwardness of only having larger denominations to work with; the bills bear the signatures of both HOURS president Steve Burke and the president of AFCU.[5]

While the Ithaca Hour continues to exist, in recent years it has fallen into disuse. Media accounts from the year 2011 indicate that the number of businesses accepting Hours has declined.[6] Several reasons are attributed to this. First has been the founder, Paul Glover, moving out of town. While in Ithaca, Glover had acted as an evangelist and networker for Hours, helping to spread their use and helping businesses find ways to spend Hours they had received. Secondly, a general shift away from cash transactions towards electronic transfers with debit or credit cards. Glover has emphasized that every local currency needs at least one full-time networker to "promote, facilitate and troubleshoot" currency circulation.

Origin

Ithaca Hours were started by Paul Glover in November 1991.[7] The system has historical roots in scrip and alternative and local currencies that proliferated in America during the Great Depression.[7]

While doing research into local economics during 1989, Glover had seen an "Hour" note 19th century British industrialist Robert Owen issued to his workers for spending at his company store. After Ithaca Hours began, he discovered that Owen's Hours were based on Josiah Warren's "Time Store" notes of 1827.

In May 1991, local student Patrice Jennings interviewed Glover about the Ithaca LETS enterprise. This conversation strongly reinforced his interest in trade systems. Jennings's research on the Ithaca LETS and its failure was integral to the development of the HOUR currency; conversations between Jennings and Glover helped to ensure that HOURS used knowledge of what had not worked with the LETS system.[8]

Within a few days, he had designs for the HOUR and Half HOUR notes. He established that each HOUR would be worth the equivalent of $10, which was about the average hourly amount that workers earned in surrounding Tompkins County,[9] although the exact rate of exchange for any given transaction was to be decided by the parties themselves. At GreenStar Cooperative Market, a local food co-op, Glover approached Gary Fine, a local massage therapist, with photocopied samples. Fine became the first person to sign a list formally agreeing to accept HOURS in exchange for services. Soon after, Jim Rohrrsen, the proprietor of a local toy store, became the first retailer to sign-up to accept Ithaca HOURS in exchange for merchandise.

When the system was first started, 90 people agreed to accept HOURS as pay for their services.[9] They all agreed to accept HOURS despite the lack of a business plan or guarantee. Glover then began to ask for small donations to help pay for printing HOURS.

Fine Line Printing completed the first run of 1,500 HOURS and 1,500 Half HOURS in October 1991. These notes, the first modern local currency, were nearly twice as large as the current Ithaca HOURS. Because they didn't fit well in people's wallets, almost all of the original notes have been removed from circulation.

The first issue of Ithaca Money was printed at Our Press, a printing shop in Chenango Bridge, New York, on October 16, 1991. The next day Glover issued 10 HOURS to Ithaca Hours, the organization he founded to run the system, as the first of four reimbursements for the cost of printing HOURS. The day after that, October 18, 1991, 382 HOURS were disbursed and prepared for mailing to the first 93 pioneers.

On October 19, 1991, Glover bought a samosa from Catherine Martinez at the Farmers' Market with Half HOUR #751—the first use of an HOUR. Several other Market vendors enrolled that day.

Stacks of the Ithaca Money newspaper were distributed all over town with an invitation to "join the fun."

A Barter Potluck was held at GIAC on November 12, 1991, the first of many monthly gatherings where food and skills were exchanged, acquaintances made, and friendships renewed.

Management & philosophy

In 1996, Glover was running the Ithaca Hours system from his home, and the system had an advisory board and a governing board called the "Barter Potluck".[9] The board and Glover put forth the idea that economic interactions should be based on harmony rather than on more Hobbsian forms of competition. In one interview, Glover stated that "There's a growing movement called "ecological economics" and Ithaca HOURS is part of that cosmos. Last year I wrote an article which discusses moving us toward the provision of food, fuel, clothing, housing, transportation, [and other] necessities in ways which are healing of nature, or which are less depleting at least and which bring people together on the basis of their shared pride, not arrogance." Thus one underlying principle of the local currency movement is to create "fair trade" with a minimum of conflict or exploitation of either people or natural resources.[10]

The Advisory Board incorporated the Ithaca HOUR system as Ithaca Hours, Inc. in October 1998, and hosted the first elections for Board of Directors in March 1999. The first Board of Directors included Monica Hargraves, Dan Cogan, Margaret McCasland, Erica Van Etten, Greg Spence Wolf, Bob LeRoy, LeGrace Benson, Wally Woods, Jennifer Elges, and Donald Stephenson. In May 1999 Glover turned the administration of Ithaca HOURS over to the newly elected Board of Directors. Glover has continued to support Ithaca Hours through community outreach to present, most notably through the Ithaca Health Fund (now incorporated as part of the Ithaca Health Alliance) and Ithaca Community News.

The current Board of Directors, 2014-2015, includes Erik Lehmann (Chair), Danielle Klock, and Bob LeRoy.

Economic development

Several million dollars value of HOURS have been traded since 1991 among thousands of residents and over 500 area businesses, including the Cayuga Medical Center, Alternatives Federal Credit Union, the public library, many local farmers, movie theatres, restaurants, healers, plumbers, carpenters, electricians, and landlords.

One of the primary functions of the Ithaca Hours system is to promote local economic development. Businesses who receive Hours must spend them on local goods and services, thus building a network of inter-supporting local businesses. While non-local businesses are welcome to accept Hours, those businesses need to spend them on local goods and services to be economically sustainable.

In their mission to promote local economic development, the Board of Directors also makes interest-free loans of Ithaca HOURS to local businesses and grants to local non-profit organizations.

See also

- Local currency
- List of community currencies in the United States
- Labour voucher
- Time-based currency
- Wörgl

References

1. "Richard P. Carpenter, "PLAN TO TOUCH THE HEART OF THE APPLE OF YOUR EYE", "Boston Globe",

Jan. 29, 2006". Nl.newsbank.com. 2006-01-29. Retrieved 2009-07-10.
2. "Emily Lambert, "Funny Money", "Forbes", Feb. 14th, 2006". Forbes.com. 2006-02-14. Archived from the original on 2013-01-23. Retrieved 2009-07-10.
3. Soper, Spencer (2009-01-07). "Spencer Soper, "Lehigh Valley group eyes a local alternative to money", "The Morning Call", Jan. 7, 2009". Courant.com. Retrieved 2009-07-10.
4. " "New age town in U.S. embraces dollar alternative", www.chinadaily.com.cn, Jun. 21, 2007". Chinadaily.com.cn. Retrieved 2009-07-10.
5. By:M. Tye Wolfe 10/02/2002 (2009-06-13). "M. Tye Wolf, "Making Money - The brand new one-tenth Ithaca Hour bill hits the streets", "Ithaca Times", Oct. 2, 2002". Zwire.com. Retrieved 2009-07-10.
6. By:Dana Khromov (2011-04-10). " "Ithacaa Hour Revival Would Require Community Support", "Ithaca.com", April 13, 2011". Retrieved 2012-04-10.
7. " "ITHACA JOURNAL; An Alternative to Cash, Beyond Banks or Barter", "New York Times", May 31, 1993". Nytimes.com. 1993-05-31. Retrieved 2009-07-10.
8. *Bill Maurer, "Mutual life, limited: Islamic banking, alternative currencies, lateral reason", Princeton University Press, 2005, p. 47*. Books.google.com. 1986-06-26. Retrieved 2009-07-10.
9. Nieves, Evelyn (1996-01-21). "Evelyn Nieves, "Our Towns;Ithaca Hours: Pocket Money For Everyman", "New York Times", Jan. 21, 1996". Nytimes.com. Retrieved 2009-07-10.
10. Fortier, Jana "Underthrowing the System: How Low Finance Undermines Corporate Culture (http://www.academia.edu/2307226/Underthrowing_the_System_How_Low_Finance_Undermines_Corporate_Culture)" *Conscious Choice: Journal of Ecology and Healthy Living* Sept/Oct 1996.'

External links

- Official Ithaca Hours Website (http://ithacahours.info/)
- Founder's Website (http://www.paulglover.org/hours.html)
- E F Schumacher Society Local Currency website (http://neweconomicsinstitute.org/content/local-currencies)
- Brief History of Local Currencies (http://www.schumachersociety.org/local_currencies/2004_conference_report.html)
- Community Currency Online Magazine (http://ccmag.net/)

Categories: Ithaca, New York | Local currencies | Time-based economics

---

Exhibit E

NEW YORK STATE
DEPARTMENT *of*
FINANCIAL SERVICES

FROM: Benjamin M. Lawsky, Superintendent of Financial Services

DATE: August 12, 2013

RE: Notice of Inquiry on Virtual Currencies

New York has a long history of promoting technological innovation – both within the financial sector and across our economy.

As innovative products emerge, it is critical to take steps that allow new technologies and industries to flourish, while also working to ensure that consumers and our national security remain protected.

The emergence of Bitcoin and other virtual currencies has presented a number of unique opportunities and challenges. Building innovative platforms for conducting commerce can help improve the depth and breadth of our nation's financial system. However, we have also seen instances where the cloak of anonymity provided by virtual currencies has helped support dangerous criminal activity, such as drug smuggling, money laundering, gun running, and child pornography.

If virtual currencies remain a virtual Wild West for narcotraffickers and other criminals, that would not only threaten our country's national security, but also the very existence of the virtual currency industry as a legitimate business enterprise.

Indeed, it is in the common interest of both the public and the virtual currency industry to bring virtual currencies out of the darkness and into the light of day through enhanced transparency. It is vital to put in place appropriate safeguards for consumers and law-abiding citizens.

As such, the Department of Financial Services (DFS) has launched an inquiry into the appropriate regulatory guidelines that it should put in place for virtual currencies. DFS has already conducted significant preliminary work regarding this inquiry, including making requests for information from virtual currency firms. Based on that initial work, we are concerned that – at a minimum – virtual currency exchangers may be engaging in money transmission as defined in New York law, which is an activity that is licensed and regulated by DFS.

Under current DFS regulations, firms engaging in money transmission are required to post collateral in order to better safeguard customer account funds. Additionally, they are required to undergo periodic safety and soundness examinations, as well as comply with applicable anti-money laundering laws. These guidelines for money transmitters help protect consumers and root out illegal activity.

However, DFS is also considering whether it should issue new regulatory guidelines specific to virtual currencies – rather than simply apply existing money transmission regulations. As such, we could also move forward with new guidelines that are tailored to the unique characteristics of virtual currencies.

We believe that – for a number of reasons – putting in place appropriate regulatory safeguards for virtual currencies will be beneficial to the long-term strength of the virtual currency industry.

First, safety and soundness requirements help build greater confidence among customers that the funds that they entrust to virtual currency companies will not get stuck in a digital black hole. Indeed, some consumers have expressed concerns about how quickly their virtual currency transactions are processed. Taking steps to ensure that these transactions – particularly redemptions – are processed promptly is vital to earning the faith and confidence of customers.

Second, serving as a money changer of choice for terrorists, drug smugglers, illegal weapons dealers, money launderers, and human traffickers could expose the virtual currency industry to extraordinarily serious criminal penalties. Taking steps to root out illegal activity is both a legal and business imperative for virtual currency firms.

Finally, both virtual currency companies – and the currencies themselves – have received significant interest from investors and venture capital firms. Similar to any other industry, greater transparency and accountability is critical to promoting sustained, long-term investment.

We look forward to working with the virtual currency industry and other stakeholders as our inquiry proceeds, and we move to put in place appropriate regulatory guardrails to protect consumers and our national security.

Exhibit F

Manhattan District Attorney Cyrus R. Vance, Jr.

Testimony Before the Department of Financial Services

Hearing on Digital Currency – Remarks as Prepared

January 29, 2014

Good morning Superintendent Lawsky and members of the Department of Financial Services. I am New York County District Attorney Cyrus R. Vance, Jr. Thank you for the opportunity today to discuss the criminal implications surrounding digital currencies.

As a young ADA, I prosecuted cases that had yellow tape blocking off a physical crime scene in Manhattan. While many Assistant District Attorneys in my office continue to prosecute these kinds of cases, we also face a newer and still emerging threat, as the internet becomes a global, boundary-free crime scene of the 21st Century. The internet provides cybercriminals with anonymity, which makes the task of investigating and prosecuting crime that is committed using cyber techniques more difficult.

Exploiting digital currency payment systems is no different. The anonymity offered by these payment systems attracts criminals who can now more easily move, conceal, and launder their illicit profits. My Office has investigated and prosecuted these kinds of cases, and I will highlight two momentarily. While we have and will continue to aggressively prosecute individuals who use digital currency to facilitate their criminal activities, we need stronger tools to combat new emerging threats derived from these payment systems.

Without stronger government oversight, we are allowing cybercriminals, identity thieves, traffickers of child pornography, and other malevolent actors to operate in a digital Wild West. Therefore, it is my position that digital currency exchanges should be required to obtain licenses as money transmitters in order to do business in New York State, and therefore, come under this regulatory framework.

This action by itself, however, would not be enough. I also ask that digital currency exchanges be required to perform enhanced due diligence with regard to the identification of their customers.

Let me give you two concrete examples of cases from my Office where digital currency was used to facilitate criminal activity:

Last year, my Office secured convictions against 14 members of a major cybercrime ring that crisscrossed the globe, from Russia, Ukraine, and Moldova, to the Czech Republic to California to Brooklyn. The ring trafficked nearly 100,000 stolen credit card numbers, resulting in more than $5 million in credit card fraud. One of the top defendants in this case was sentenced to 22-to-44 years in prison – just one example of how seriously the criminal justice system is now taking these types of crimes.

At the center of this international criminal organization was a corporation based in Manhattan called Western Express. The company served as the principal digital currency exchanger for the trafficking ring, allowing the buyers and sellers of stolen credit card information to move money anonymously using two types of digital currencies, E-Gold and WebMoney.

Briefly, this is how the trafficking operation worked:

- The buyers of stolen credit card information used Western Express to exchange U.S. Currency (in the form of cash or money orders or other structured payments) into E-Gold or WebMoney.
- The buyers then took this digital currency and used it to buy stolen credit card information from the vendors. They used this stolen information to manufacture forged credits cards, which they used to purchase merchandise online and in stores, and then fenced those products online or on the street for profit.
- The vendors needed to convert all the E-Gold and WebMoney they received as payment for stolen data either into a different digital currency, or into conventional currency. They used Western Express for this purpose.
- Western Express also facilitated the global flow of digital currency for criminal activity,

to the tune of $15 million dollars, and sent bank wires around the world.

- Western Express charged a fee for every transaction that it facilitated.

Similarly, in 2006, my Office prosecuted a company called Goldage, a digital currency exchanger operated by two men who moved millions of dollars for their customers.

Here, individuals used Goldage to exchange Egold digital currency. When purchasing Egold, customers could choose their method of payment to Goldage. Specifically, they could wire money, make cash deposits, or mail postal money orders and checks. When selling Egold to Goldage, customers could obtain payments through wire transfers to accounts anywhere in the world or have checks sent to individuals anywhere in the world. Goldage's owners charged customers a fee on both ends of the transactions and maintained various bank accounts under the guise of different subsidiary companies.

In both of these cases, the fact that the defendants ultimately converted digital currency back into cash helped investigators to trace the money. But now that retailers, both large and small, are starting to accept digital currency as payment, criminals might not have to convert their illegal proceeds back into cash. For example, criminals can use digital currency to buy high-end merchandise from major online retailers, and then sell those products for cash. Or they can simply refrain from ever converting their digital currency to cash, simply continuing to finance criminal conduct and engage in business, whether criminal or legitimate, using such currency. This makes it even more difficult for law enforcement to trace their transactions.

An even greater challenge to law enforcement may be the emergence of Bitcoin ATMs, in which individuals can insert dollars and get Bitcoins in return. Unlike users of debit or credit cards, the identification of Bitcoin ATM users can remain untraceable.

I want to note that I am not taking a position on the legitimacy of digital currency as a method of payment for goods and services. Additionally, I recognize that many digital currencies are not specifically designed to attract illicit activity.

But in this ever changing technological landscape, our laws have to keep up with reality. Digital currency is quickly becoming a part of our mainstream economy, bringing along with it criminals who exploit the gaps in our regulatory and criminal justice system. Law enforcement must be given appropriate updated tools to address criminal behavior as it actually exists today.

Under current law, money transmitters must comply with anti-money laundering requirements. Financial institutions facilitating deposits and withdrawals of large amounts of cash must file Currency Transaction Reports with FinCEN. Cross-border movements of large amounts cash also require governmental reporting. These valuable filings allow law enforcement to identify and investigate potential suspicious activity.

There should be no ambiguity that digital currency exchanges that transmit value act as "money transmitters," and are therefore required to comply with the same licensing, reporting, and anti-money laundering regulations imposed on banks and other money exchangers. This is consistent with numerous prior prosecutions conducted by my Office.

And there is no question that digital currency providers act as a medium of exchange in the sale and purchase of goods and services. Therefore, it is my opinion that the nature of a transaction in which digital currency is purchased is indeed a form of money transmission, no different than where a buyer directs a bank to send money to a vendor.

Furthermore, digital currency exchanges should be required to perform enhanced due diligence with respect to their customers' identification.

Digital currency exchangers, at minimum, should be required to do the following:

- Maintain records relating to transactions.
- Obtain customers' identifying information. This includes requiring a customer to provide his real name, his physical address, the name of his business, and the nature of that business. The customer should also be required to confirm that the "digital wallet" in which the currency is being sent is actually owned and controlled by the customer.
- Implement procedures to ensure the accuracy of this information – for example, that the

address is actually owned and controlled by the customer. This would help with the chain of custody in establishing who is receiving the digital currency.

- File periodic applications in order to do business. These filings should identity the owners and mangers of the exchange, and those principals should make sworn affirmations as to the accuracy and truth of the filings.

As we have seen in so many cases, digital currency is being used by bad actors to commit very serious crimes – multi-million dollar identity theft rings, child pornography, underground markets for drugs, guns, and other contraband.

The federal government is starting to bring digital currency exchangers under their regulatory umbrella. New York State should also recognize the dangers of these payment systems. It should be made clear that digital currency exchanges must be licensed as money transmitters in order to do business our state. We must also adequately supervise the exchanges to ensure that their customers are providing proper identification and are not using the exchanges for criminal activities. And we must also act to ensure that unlicensed digital currency exchangers are identified and prosecuted.

Thank you. I'm happy to take your questions.

Exhibit G

DISTRICT ATTORNEY
COUNTY OF NEW YORK
ONE HOGAN PLACE
New York, N.Y. 10013
[redacted]

CYRUS R. VANCE, JR.
DISTRICT ATTORNEY

October 21, 2014

Dana V. Syracuse, Esq.
New York State Department of Financial Services
Office of the General Counsel
One State Street
New York, NY 10004-1561

Re: Proposed Title 23, Ch. 1
Part 200 Virtual Currencies Rules

Dear Ms. Syracuse:

I write to comment regarding the "BitLicense" regulatory framework that has been proposed by the New York State Department of Financial Services ("DFS"). I applaud the efforts of DFS to ensure that businesses dealing in virtual currency are both honest with their consumers, and at the same time, are robust in their anti-money laundering and anti-fraud practices.

That said, I am respectfully concerned that the BitLicense regulatory framework inadvertently lacks an important piece, similar to that which is used by New York State law enforcement agencies for prosecuting individuals and business entities that violate regulations covering money transmitters under Article 13-B of the New York State Banking Law (the "Banking Law"). Without clear regulatory guidance stating that virtual currency businesses are subject to the Banking Law, or alternatively, a corollary New York State statute criminalizing violations of the proposed BitLicense regulations, New York State law enforcement agencies may lose some of their ability to prosecute those who use Bitcoin to further their illegitimate and unlawful activities. As New York State is the home to the financial capital of the world, the State and its law enforcement agencies and partners cannot afford to take this threat lightly.

On January 29th of this year, at a hearing held by DFS, I had the opportunity to address the growing concern that virtual currency businesses pose to law enforcement, particularly given that cybercriminals can cloak themselves with layers of anonymity, far beyond those currently utilized, through the use of virtual currency.

As I testified to at the hearing:

> The anonymity offered by [virtual currency] payment systems attracts criminals who can now more easily move, conceal, and launder their illicit profits. My Office has investigated and prosecuted these kinds of cases . . . . While we have and will continue to aggressively prosecute individuals who use digital currency to facilitate their criminal activities, we need stronger tools to combat new emerging threats derived from these payment systems.

I further testified at the hearing that:

> There should be no ambiguity that digital currency exchanges that transmit value act as "money transmitters," and are therefore required to comply with the same licensing, reporting, and anti-money laundering regulations imposed on banks and other money exchangers.

Virtual currency exchanges are, undoubtedly, businesses that facilitate the movement of value. Even if DFS chooses to regulate these virtual currency businesses under a "BitLicense" regulatory framework, it is important to clearly state that these virtual currency businesses are also money transmitters, in order to ensure that such businesses are brought under the ambit of Article 13-B of the Banking Law. Bringing these businesses under the Banking Law's regulation of money transmitters would provide state law enforcement agencies with a critical and essential tool: the ability to prosecute violators of the Banking Law by using the criminal penalties of Banking Law section 650. The criminal penalties (which include felony level offenses) would provide a direct means to enforce the law against unlicensed virtual currency businesses.

However, as currently proposed, the BitLicense regulatory frameworks seems to enable an individual or business entity to obtain a "BitLicense" while not necessarily being considered a money transmitter. By not specifically stating that virtual currency businesses are money transmitters covered by the Banking Law, the proposed regulatory framework creates an air of ambiguity for both the state judiciary and state law enforcement agencies, and potentially removes what should be an indispensable tool for law enforcement.

As I testified at the hearing, the nature of a virtual currency exchange, in converting cash to virtual currency and allowing an individual to send the virtual currency to any "address" designated by the customer (absent at least some means of the virtual currency business being certain that a customer is doing no more than simply purchasing virtual currency for his or her own personal account), clearly constitutes money transmission. The potential risk for abuse is not a burden that should be borne by the public, particularly when the entire public does not and may never use virtual currency. Rather, any business dealing in virtual currency—

like all other regulated money transmitters—should bear the burden of ensuring that its services are not being used for illegitimate and unlawful means.

In this regard, it is notable and important that both the federal judiciary and the federal government have apparently taken the position that virtual currency business are, in fact, money transmitters under the parallel federal regulatory scheme. This allows for both federal regulatory and federal criminal enforcement actions against violators. This past August, in a matter pending before United States District Judge Jed S. Rakoff, the Court concluded that "Bitcoin clearly qualifies as 'money.'"[1] The Court upheld the federal indictment and reached its conclusion in a prosecution charging the defendant with, among other crimes, conducting an "unlicensed money transmission business." Id. The Court's decision was in line with guidance issued by the Financial Crimes Enforcement Network ("FinCEN") a year earlier, which also concluded that virtual currency businesses are money transmitters.[2] I believe that DFS should reach the same result as the federal authorities and conclude, at the very least, that virtual currency businesses constitute money transmitters under Article 13-B of the Banking Law.

Of course, there are aspects about virtual currency businesses that may justify further, more robust and enhanced regulation under the proposed BitLicense regulatory framework, and I support DFS in those endeavors. First and foremost, however, the status of virtual currency businesses as subject to the Banking Law must be unequivocally affirmed. Absent such regulatory clarity, the ability of New York State law enforcement agencies to investigate and criminally prosecute virtual currency businesses that violate New York State law may be needlessly and dangerously eviscerated. I respectfully call on DFS to ensure that such a lapse does not occur.

Respectfully,

Cyrus R. Vance, Jr.
District Attorney
New York County

---

[1] United States v. Faiella, 2014 US Dist. LEXIS 116114 (SD NY August 19, 2014).

[2] See FIN-2013-G001, issued March 18, 2013 ("[A]n administrator or exchanger is a [Money Services Business] under FinCEN's regulations, specifically, a money transmitter, unless a limitation to or exemption from the definition applies to the person.") (http://fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf)

Exhibit H

The Opinion Pages | OP-ED CONTRIBUTORS

When Phone Encryption Blocks Justice

By CYRUS R. VANCE Jr., FRANÇOIS MOLINS, ADRIAN LEPPARD and JAVIER ZARAGOZA AUG. 11, 2015

Sébastien Thibault

In June, a father of six was shot dead on a Monday afternoon in Evanston, Ill., a suburb 10 miles north of Chicago. The Evanston police believe that the victim, Ray C. Owens, had also been robbed. There were no witnesses to his killing, and no surveillance footage either.

With a killer on the loose and few leads at their disposal, investigators in Cook County, which includes Evanston, were encouraged when they found two smartphones alongside the body of the deceased: an iPhone 6 running on Apple's iOS 8 operating system, and a Samsung Galaxy S6 Edge running on Google's Android operating system. Both devices were passcode protected.

An Illinois state judge issued a warrant ordering Apple and Google to unlock the phones and share with authorities any data therein that could potentially solve the murder. Apple and Google replied, in essence, that they could not — because they did not know the user's passcode.

The homicide remains unsolved. The killer remains at large.

Until very recently, this situation would not have occurred.

Last September, Apple and Google, whose operating systems are used in 96 percent of smartphones worldwide, announced that they had re-engineered their software with "full-disk" encryption, and could no longer unlock their own products as a result.

According to Apple's website: "On devices running iOS 8.0 ... Apple will not perform iOS data extractions in response to government search warrants because the files to be extracted are protected by an encryption key that is tied to the user's passcode, which Apple does not possess."

A Google spokeswoman said, "Keys are not stored off of the device, so they cannot be shared with law enforcement."

Now, on behalf of crime victims the world over, we are asking whether this encryption is truly worth the cost.

Between October and June, 74 iPhones running the iOS 8 operating system could not be accessed by investigators for the Manhattan district attorney's office — despite judicial warrants to search the devices. The investigations that were disrupted include the attempted murder of three individuals, the repeated sexual abuse of a child, a continuing sex trafficking ring and numerous assaults and robberies.

Criminal defendants have caught on. Recently, a suspect in a Manhattan felony, speaking on a recorded jailhouse call, noted that "Apple and Google came out with these softwares" that the police cannot easily unlock.

Apple, Google and other proponents of full-disk encryption have offered several rationales for this new encryption technology. They have portrayed the new policy as a response to the concerns raised by Edward J. Snowden about data collection by the National Security Agency. They say full-disk encryption makes devices generally more secure from cybercrime. And they assert that, if the companies had master encryption keys, then repressive governments could exploit the keys.

These reasons should not be accepted at face value. The new Apple encryption would not have prevented the N.S.A.'s mass collection of phone-call data or the interception of telecommunications, as revealed by Mr. Snowden. There is no evidence that it would address institutional data breaches or the use of malware. And we are not talking about violating civil liberties — we are talking about the ability to unlock phones pursuant to lawful, transparent judicial orders.

In the United States, Britain, France, Spain and other democratic societies, the legal system gives local law enforcement agencies access to places where criminals hide evidence, including their homes, car trunks, storage facilities, computers and digital networks.

Carved into the bedrock of each of these laws is a balance between the privacy rights of individuals and the public safety rights of their communities. For our investigators to conduct searches in any of our jurisdictions, a local judge or commissioner must decide whether good cause exists. None of our agencies engage in bulk data collection or other secretive practices. We engage in targeted requests for information, authorized after an impartial, judicial determination of good cause, in which both proportionality and necessity are tested.

It is this workable balance that proscribes the operations of local law enforcement in our cities, and guides our residents in developing their expectations of privacy. But in the absence of laws that keep pace with technology, we have enabled two Silicon Valley technology companies to upset that balance fundamentally.

The Evanston case is just one example. In France, smartphone data was vital to the swift investigation of the Charlie Hebdo terrorist attacks in January, and the deadly attack on a gas facility at Saint-Quentin-Fallavier, near Lyon, in June. And on a daily basis, our agencies rely on evidence lawfully retrieved from smartphones to fight sex crimes, child abuse, cybercrime, robberies or homicides.

Full-disk encryption significantly limits our capacity to investigate these crimes and severely undermines our efficiency in the fight against terrorism. Why should we permit criminal activity to thrive in a medium unavailable to law enforcement? To investigate these cases without smartphone data is to proceed with one hand tied behind our backs.

The new encryption policies of Apple and Google have made it harder to protect people from crime. We support the privacy rights of individuals. But in the absence of cooperation from Apple and Google, regulators and lawmakers in our nations must now find an appropriate balance between the marginal benefits of full-disk encryption and the need for local law enforcement to solve and prosecute crimes. The safety of our communities depends on it.

Cyrus R. Vance Jr. is the Manhattan district attorney. François Molins is the Paris chief prosecutor. Adrian Leppard is the commissioner of the City of London Police. Javier Zaragoza is the chief prosecutor of the High Court of Spain.

Exhibit I

The “Yes” to Full Disk Encryption of Axelle Lemaire

The Op-Ed in the New York Times by the Paris chief prosecutor, François Molins and his American, British and Spanish counterpart is not of the taste of the minister of State for Digital Affairs, Axelle Lemaire. “As far as I am concerned, I am favorable to full disk encryption because it guarantees the protection of the users’ private data”, she explain to Express. In the middle of the preparation on a digital law bill, the Socialist aligns herself with report published last May by the United Nations, consider that these technologies protect the liberty of expression and the human rights from government wishing to control their population. **Marcelo Wesfreid**

Axelle Lemaire

From Wikipedia, the free encyclopedia

For other uses, see Lemaire (surname).

Axelle Lemaire (born 18 October 1974) is a French Socialist politician who currently serves as a Secretary of State in the French Government.

In 2012, she was elected as Deputy for the Third constituency for French overseas residents in the National Assembly of the French Parliament.[1]

In May 2014, Prime Minister Manuel Valls appointed her to the French Finance Ministry as minister responsible for Digital Affairs.

Contents

Education and personal life

Lemaire was born in Canada to a French mother and a Quebecois father. After being brought up in Hull, Quebec where she attended Collège Saint-Joseph de Hull, Lemaire lived as a teenager in Montpellier.

She read Modern Literature and Political Science at the Institut d'études politiques de Paris, before completing degrees in Law at Panthéon-Assas University (DEA, 2000) and King's College London (LLM, 2003).[2] Lemaire subsequently taught legal studies at university level and worked in a law firm, before working at the House of Commons as a researcher for the former Labour MP and Minister, Denis MacShane.[3]

Mrs Lemaire lived in London with her husband and two children from 2002 until 2014 before relocating to Paris.[4]

Axelle Lemaire

Axelle Lemaire in 2015

Minister for Digital Affairs	
Incumbent	
Assumed office	9 April 2014
President	François Hollande
Prime Minister	Manuel Valls
Preceded by	Fleur Pellerin
Assembly Member for Northern Europe	
In office	20 June 2012 – 9 May 2014
Preceded by	*Position created*
Succeeded by	Dr Christophe Premat
Personal details	
Born	18 October 1974 Ottawa, Canada
Nationality	French-Canadian

Political career

Political party	Parti socialiste (PS)
Children	2
Residence	Paris
Alma mater	Institut d'études politiques de Paris Panthéon-Assas University King's College London
Occupation	Politician
Profession	Lawyer
Website	Official Website (http://www.axellelemaire.eu)

Lemaire served as Secretary of the French Socialist Party (PS)[5] in London from 2008 until her election to the National Assembly in 2012. According to *Le Point*, she turned down a ministerial post in Jean-Marc Ayrault's second government having no desire to leave London being the mother of two young children.[6] She has served as Chair of the UK-France Parliamentary Friendship Group.

However she accepted appointment as Minister of State for Digital Affairs in Valls' new government in April 2014.

Assembly Member

In 2012 Lemaire was returned as Deputy for one of the eleven newly-created constituencies, each elected by French overseas citizens to the French National Assembly. The constituency she represented as inaugural Deputy includes all registered French citizens living in the ten countries throughout Northern Europe – namely, Iceland, Norway, Denmark (including the Faroe Islands and Greenland), Sweden, Finland, Great Britain and Northern Ireland, Ireland, Estonia, Latvia and Lithuania: on New Year's Day 2011, it recorded 140,731 French citizens on its electoral roll, with the vast majority of these (113,655) living in the United Kingdom, which has the third largest French expat population in the world. Consequently her election campaign received considerable attention at the time from the British press.[7][8]

Having won 54.76% of the vote, during her term as Deputy she regularly appeared in the British media regarding French politics.

In May 2014, upon assuming French governmental ministerial office, Lemaire resigned her parliamentary seat[9] being succeeded by Dr Christophe Premat.

Minister of State for Digital Affairs

Since joining the Ministry for the Economy, Industry and Digital Affairs in Paris, Lemaire has been a leading proponent of net neutrality legislation.[10]

She is a major actor in the French Tech movement, which unites french digital startups worldwide.

References

1. "Législatives 2012 : Londres et l'Europe du Nord élisent Axelle Lemaire (PS)". *Huffington Post*. 18 June 2012. Retrieved 28 July 2012.
2. "The Franco-British Connections". Fb-connections.org. 16 June 2012. Retrieved 28 July 2012.
3. "Tate Modern made to reprint Hirst catalogue – Diary – News – Evening Standard". *London Evening Standard*. 18 June 2012. Retrieved 28 July 2012.

4. "Axelle Lemaire: Canadian wins bid for French parliament seat – in London". Canada.com. 20 June 2012. Retrieved 28 July 2012.
5. "Accueil | PS – Parti socialiste" (in French). Parti-socialiste.fr. Retrieved 28 July 2012.
6. "Hollande a voulu recruter une ministre sur Canal+". *Le Point*.
7. over a year left to listen (1 January 1970). "BBC Radio 4 – Woman's Hour, Women in Greece, Gender Pay Audits, Portrait Painting , Axelle Lemaire". BBC.
8. "She got the va-va-vote... Axelle Lemaire is Hollande's woman in London – London Life – Life & Style". *London Evening Standard*. 21 September 2012.
9. www.assemblee-nationale.fr (http://www.assemblee-nationale.fr/14/tribun/fiches_id/610873.asp)
10. http://www.journaldunet.com/ebusiness/le-net/axelle-lemaire-axelle-lemaire.shtml

External links

- Official website (http://www.axellelemaire.eu/ma-bio/)
- www.economie.gouv.fr (http://www.economie.gouv.fr/)

Categories: 1974 births | Living people | Politicians from Ottawa | People from Gatineau | Socialist Party (France) politicians | Politicians of the French Fifth Republic | Sciences Po alumni | University of Paris alumni | Alumni of King's College London | French Quebecers | Panthéon-Assas University alumni | French people of Canadian descent | French emigrants to the United Kingdom | French women lawyers | French Ministers of Commerce and Industry

---

Exhibit J

Author Diana Ngo Tip 1 tip

2014-08-06 05:50 PM

French Senate: "Bitcoin offers multiple opportunities for the future"

The French Senate's committee on finance recently issued a rather positive report on virtual currencies. The document stated that the technology "can no longer be disregarded by public authorities", and, despite the risks, "Bitcoin offers multiple opportunities for the future, both as payment system and, above all, as a decentralized validation protocol," said the report.

On July 23, the committee of finance heard a communication by Senators Philippe Marini and François Marc on the topic of virtual currencies. The 140 page report noted that despite the risks of volatility, anonymity and the lack of legal guarantee, Bitcoin's technology offers a wide range of opportunities and "public authorities should work on a well-balanced regulatory framework", which is said "to be carried out at a European level, and if possible at the international level, considering the transnational nature of virtual currencies."

Hot stories

The Ongoing Bitcoin Malleability Attack

Over the past 72 hours, the Bitcoin protocol has been suffering from a malleability attack. The attack has been happening to quite a few use...

2015-10-04 by Jamie Redman

'Neucoin Will Have More Consumers Using It Than Bitcoin within One Year' - Founder

NeuCoin (NEU), a cryptocurrency specifically designed to aid the implementation of online microtransactions and tipping within online produc...

2015-10-07 by Erin Lace

Edward Snowden: Governments Want to Own Your Phone Instead of You

NSA whistleblower and American fugitive Edward Snowden has revealed information on the scope and

- Sénat of France

Based on researches and comparisons made by the French Treasury for the account of the committee, France is said to be standing halfway between countries with the strictest regulations, e.g. China, Japan and Russia; and those with the lightest, e.g. the US, Canada or Israel. However, France's Bitcoin economy is relatively large and falls in the top ten in the world based on the number of Bitcoin clients downloaded. Additionally, back in May, the first ever Bitcoin center - La Maison du Bitcoin – opened its doors to Bitcoin fans and the public alike in Paris. The project is focused to educate the public on cryptocurrencies.

And according to the report, the Senate has been focusing on the impacts of the digital revolution on the economical sector, and it is with little surprise that the authority is now taking interest in Bitcoin and virtual currencies. The authority noted that virtual currencies have significantly questioned the monopoly of Central Banks on money creation, which is said to be the ultimate demonstration of its Regalian power.

The report mentioned Bitcoin as the most popular and successful virtual currency, defining it as "open-source, anonymous and decentralized, providing its users the ability to exchange goods and services without recurring to the traditional currency." Therefore, the document added that Bitcoin couldn't be considered as a legal currency, neither as a legal tender, regarding the French Monetary and Financial Code (code monétaire et financier), and is said to be a "virtual barter system".

Among Bitcoin's attributes, the report noted its near-zero transaction fees, as well as its high-level security, adding that transactions were encrypted and had to be confirmed by a network of computers in a decentralized manner. This goes in the opposite of a "central" system, which is by definition more vulnerable.

The document also cited the "ingenuous mechanism of 'monetary creation'" which consists in rewarding miners for allocating their calculation power to confirm transactions. So far, it is estimated that 100,000 processors are participating in this operation.

On the other hand, one of the major risks is its volatility. This characteristic is said to be one the consequences of the system itself; a system that the authority qualified as "intrinsically speculative" due to its "organized rarity" (limited supply). However, the document noted that it is also a success factor as there is no "Bitcoin printing press".

The lack of legal guarantee is a major risk for investors, as Bitcoin isn't backed by any "real" asset. In fact, Bitcoin's value is majorly based on the level of credibility attributed to the virtual currency by the members of its community.

Although the validation process is said to be secure, it isn't necessarily the case of Bitcoin storage. The report illustrated this argument with the case of Mt.Gox, once the largest Bitcoin exchange platform.

Finally, the anonymous character of Bitcoin makes it a staggering windfall for cyber-criminality and money laundering, said the document.

However, the report said excessive alarmism is not needed at this stage and added that volatility and the absence of a legal framework were the elements

capabilities of the United Kingdom's GCHQ i...

2015-10-12 by Evander Smart

Editor Recommends

New CEO Dorsey Files Square IPO amid Twitter Mass Lay-Offs

Payment processor Square has filed for an IPO to list its stock on the New York Stock Exchange.

2015-10-15 by William Suberg

Coinbase CEO Armstrong: I'd Like to Increase the Block Size in December

The Bitcoin debate of the year has been about how the blockchain block size matters. Whether to increase block size, how to do it, and when ...

2015-10-14 by Evander Smart

Bitcoin Price Analysis: Is Volume Preceding Price?

The Price has not only broken through the 50 day EMA, but has now moved above the 100 day EMA as well. A test of the 200 day at ~US$256 sho...

2015-10-13 by George Samman

limiting Bitcoin's development.

Moreover, the document also stated that, due to its negligible money supply - between 5 and 8 billions of dollars versus thousands of billions of dollars for important fiat currencies - Bitcoin wasn't a threat to the macroeconomic stability.

On January 15, the committee on finance had organized an audition with the concerned administrations to express their positions on virtual currencies. The meeting was composed of representatives from the French Treasury, the Customs, the Bank of France and the anti-money laundering service Tracfin, as well as an entrepreneur and a scholar working on the topic.

On July 11, Tracfin issued its report on the subject, enouncing concrete measures such as anonymity limitations, a ceiling payment amount in virtual currencies and a clarification of the fiscal regime.

Although a formal regulatory plan is yet to be issued, the French Senate's committee of finance stressed that an European, and if possible, a global clarification should be carried out, considering the transnational nature of virtual currencies:

"Bitcoin isn't the only 'virtual currency' [...] there had been some (Liberty Reserve, e-Gold), and there will be others (Litecoin is an example inspired by Bitcoin) [...] Thus, it is important that public authorities do not step back and reinforce these innovations with an appropriate regulatory framework [...] [Public authorities] should work on an adapted regulatory framework. All these actions are to be undertaken at the European level in order to be truly effective. "

Did you enjoy this article? You may also be interested in reading these ones:

- France: Bitcoin Revenue Must be Declared
- Bitcoin Exchange Dismantled by French Police
- La Maison du Bitcoin is now opened

Do you want to read CoinTelegraph from your mobile device? Then go to our Indiegogo campaign, contribute, collect your prize and enjoy the mobile app!

France | Bitcoin | government | future for bitcoin | future of bitcoin

About us

CoinTelegraph covers everything FinTech, Blockchain, Bitcoin, bringing you the latest news, prices, breakthroughs and analysis from across the future of money.

Site map

Catalog | Advertise | Contests | Projects | About us | Our vacancies |

International Sites

Bitcoin USA
Bitcoin Czech Republic
Bitcoin Germany
Bitcoin Italy
Bitcoin Poland
Bitcoin Greece
Bitcoin South Africa
Bitcoin Philippines
Bitcoin Great Britain
Bitcoin Slovenia

Franchise Information

Exhibit K

SÉNAT

COMMISSION DES FINANCES

République Française

REGULATION & INNOVATION:

PUBLIC AUTHORITIES AND THE DEVELOPMENT OF VIRTUAL CURRENCIES

This is an English summary of the report by Philippe MARINI, president of the committee on finance of the French Senate, and François MARC,* rapporteur général*, on the development of digitial currencies, published on 4th August 2014.

The full version of the report is available here:
http://www.senat.fr/notice-rapport/2013/r13-767-notice.html

CONCLUSIONS AND RECOMMENDATIONS OF THE COMMITTEE ON FINANCE

Meeting on 23rd July 2014, under the chairmanship of Mr. Philippe Marini, president, the committee on finance heard a communication by Mr. Philippe Marini and Mr. François Marc, *rapporteur général*, on the questions raised by the development of the *bitcoin* and other virtual currencies.

The committee on finance noted that:

1° The development of virtual currencies, among which is the *bitcoin*, is a long-term trend, raising important legal and economic matters, that **can no longer be disregarded by public authorities**.

2° Despite a number of clearly identified risks resulting from its volatility, its anonymity and its lack of legal guarantee, **the *bitcoin* offers multiple opportunities for the future**, both as a payment system and, above all, as a decentralized validation protocol.

3° Public authorities should work on a well-balanced regulatory framework, in order to prevent abuses while preserving the capacity of innovation. To that effect, **the use of existing legal categories** seems like the most relevant solution for now, for the definition of both virtual currencies and associated services.

4° The international comparisons realized by the French Treasury for the committee on finance show that **France's choices are halfway between the strictest regulations** – adopted by countries such as China, Japan or Russia – **and the lightest regulations** – adopted by countries such as the United States, Canada or Israel.

5° The clarification of the regulatory framework applicable to virtual currencies is to be carried out **at the European level, and if possible at the international level**, considering the transnational nature of virtual currencies.

ENGLISH VERSION OF THE COMMUNICATION BY PHILIPPE MARINI AND FRANÇOIS MARC

This is an English translation of the speech given on 23rd July 2014 by Mr. Philippe Marini, president of the committee on finance of the French Senate, and Mr. François Marc,* rapporteur général *of the committee on finance of the French Senate.

Mr. Philippe Marini, president of the committee on finance. – Dear colleagues, I will first make general observations about the development of virtual currencies, and I will then let the *rapporteur général* tell us about the conclusions we can draw from the elements provided by the administration. A few months ago, we asked for a number of comparisons with other countries, since virtual currencies undeniably require an international approach.

On 15th January 2014, the committee on finance of the Senate held a joint public hearing on the development of virtual currencies, and among them the well-know *bitcoin*. The Treasury, the Customs, the *Banque de France* and the anti-money laundering service *Tracfin* were given the chance to expose their positions, as well as an entrepreneur and a scholar working on the subject. As agreed upon, we then sent a questionnaire to the administration and to the economic services of our embassies.

Many things have changed in the last six months: virtual currencies have continued to thrive, carrying along a number of nice innovations and lame ducks; the *bitcoin* hit the headlines on a regular basis; and public authorities have pursued their thinking in order to set up some kind of regulation. On 11th July 2014, the minister of finance and public accounts, Michel Sapin, eventually made a series of announcements based on all this work.

The interest of the committee on finance for virtual currencies should not surprise anyone: this is part of our ongoing interest for the deep transformations caused by the irruption of digital technologies in economic and financial life. As a matter of fact, the digital revolution leaves pretty much nothing unchanged. There are, in the first place, important consequences for our taxation systems: the concentration of value on intangible assets, easily located in fiscal heavens, has led to an erosion of taxation bases – happily major countries are now aware of this problem. Beyond taxation, the digital revolution has turned upside down a number of economic sectors: the monopoly of taxi drivers is disputed by mobile applications like *Uber*, while hotels are now challenged by online booking websites and alternative accommodation offers such has *Airbnb*.

With the development of virtual currencies, something even more important is at stake: the monopoly of emission held by central banks, traditionally considered as a major attribute of sovereignty. The *bitcoin* is the

most famous and most successful example of virtual currencies; it is a free, anonymous and decentralized payment system, which allows the exchange of goods and services without using traditional currencies. Strictly speaking, though, the *bitcoin* is not a legal tender for payments, and is not issued in exchange for lawful money. It has no legal status. It is only a support for transactions. So far, the *bitcoin* is, above all, a digital version of barter – sometimes, an archaism can become an innovation, with a little help from technology.

It is not possible, though, to disregard this new trend on the grounds that it might just be another short-lived buzz. More and more e-commerce businesses accept *bitcoins* for payments, including the payment system *PayPal* itself. Such a success builds on real advantages. First of all, extremely low transaction fees – at least allegedly. A recent study from Goldman Sachs found an average of 1% for transaction fees, compared to 2.5% for credit card payments. However, it must be said that an "honest" estimation should include the cost of computer equipment and power supply, as well as the cost of risk associated with the volatility of the *bitcoin* and its insurance. More importantly, the *bitcoin* system is based on an innovative "money creation" mechanism: the users of the system are "rewarded" in *bitcoins* for their participation to the decentralized transaction validating process.

We are well aware that this system carries important risks. These risks have been known from the start, but appeared very clearly in the last few months, and led public authorities to issue a number of public warnings. Firstly, the *bitcoin* suffers from its very important volatility: one *bitcoin* was worth less than one dollar until 2011, and then surged to 1,200 dollars by fall 2013, before moving back to 650 dollars today. As a matter of fact, the *bitcoin* protocol is inherently speculative, because the rhythm of creation of new *bitcoins* is decreasing, until a "cap" of 21 million units is reached in 2140 – in comparison, 12 million units exist today. The system is "locked" for its lifetime. This "organized scarcity" is also the condition of its success, because it guarantees *bitcoin* holders against a devaluation of their assets: artificial "*bitcoin* pumping" is simply not possible.

Another weakness of the system is the absence of a legal guarantee for exchange in "real" currencies. The system entirely relies on the trust people place into it… and a sudden loss of confidence could easily bring it to an end.

Moreover, if *bitcoin transactions* are very secure, the same does not apply to *bitcoin storage*. Most users chose to open virtual "wallets" at online exchange platforms, but the bankruptcy of *Mt. Gox* on 18th February 2014 shows that hacking is more than just a possibility. Of course, people can still chose to store their *bitcoins* at home, on a personal hard drive. That's what James Howell did, after buying 7,500 *bitcoins* for just a few pounds sterling in 2009 : this young man would certainly be a multi-millionaire today if he had not unintentionally dumped his hard drive in the meantime…

Most importantly, the fact that *bitcoin* transactions are anonymous makes the system a big opportunity for cybercrime and money laundering. On the 15th January public hearing, we were told that the Customs had

arrested a drug trafficker who asked for payments in *bitcoins*. Of course, the website *The Silk Road*, the biggest online shopping center for drug dealers and weapon seekers, was shut down by the FBI at the end of 2013. But closing the website does not eliminate the risk: on 28th January 2014, the vice-president of the *Bitcoin Foundation* was arrested in New York and charged on money laundering.

However, those risks should not be overestimated – even if regulators such as the *Banque de France* and *Tracfin* are just doing their job when calling for increased vigilance. For now, the volatility of the *bitcoin* and its lack of legal status should limit its development to a small group of initiated persons: whether you are an individual, a business, or even a criminal network, would you accept to make your payments with something that can shrink to half of its value in a few minutes? Besides, the *bitcoin* does not represent any threat to the global financial stability, given its negligible money stock, just worth a few billions of dollars, as opposed to several billions of billions of dollars for main international currencies. In short, today, the *bitcoin* seems to be more like a niche speculative asset than a credible alternative to money. And as for the few *Monoprix* retail shops that accept *bitcoins* as a means of payment, this is probably not much more than an advertising campaign…

The most important point is that focusing *exclusively* on the risks leads to ignoring the multiple opportunities opened by the development of virtual currencies. The fact that an innovation questions our traditional conceptions should not lead us to reject it automatically. Besides, this rejection would likely remain very theoretical, since it is not possible to prevent individuals to use online exchange platforms…

As an alternative to legal currencies, the *bitcoin* is just beginning to unveil its potential. Those with a far-reaching imagination are already thinking about credit offers or *crowdfunding* systems based on virtual currencies. I personally hold strong reserves about these ideas, but they undeniably deserve to be analyzed – and further developments could make them more interesting.

Beyond that, it is important to understand that the *bitcoin*, more than a "*currency*", is actually a *technology*, an open-source, decentralized and very secure validation protocol. So, if it is possible to validate transactions, why not use this protocol to validate other things, such as passwords, identity documents, degrees and certificates, and even electronic votes? In the near future, it could become impossible to lie on your graduation – and that would be a great improvement. As for electronic votes, this may be an opportunity to improve the voting system for the French citizens living abroad, which as been under criticism for its lack of security… The decentralized validation protocol is an improvement of cryptography: no central entity acting as a "third party" will ever be in possession of the whole information, and yet this information is perfectly accurate and verified.

Although the *bitcoin* has acquired an important position, there are other virtual currencies – there were others yesterday, such as *Liberty Reserve*

or *e-Gold*, and there will be others tomorrow. It is therefore extremely important for public authorities and regulators to understand the full extent of their development, to be proactive, and to step in whenever it appears necessary. The *rapporteur général* will now tell us more about innovation/regulation dialectics, and how to give *bitcoin* stakeholders the security they need.

Mr. François Marc, *rapporteur général*. – Dear colleagues, I remember the time when I was a young university researcher working on payment systems. At that time, the development of credit cards was causing a widespread suspicion among specialists, who saw it as an extremely risky system that was not deemed to have any great future. Even though *bitcoin* might not exactly be the same subject, it's interesting to note that we always face, at first, a global environment of fear and suspicion towards this kind of innovations. While we do not understand every single aspect of this subject yet, the need for regulation is already here.

It is uneasy to give a legal answer to a phenomenon that challenges both our geographical borders and intellectual categories. Nevertheless, regulation is absolutely necessary, in order to secure users and investors, and to prevent abuses which would otherwise undermine the credibility of the whole system.

The president talked about the closing of websites such as *The Silk Road* and the bankruptcy of platforms such as *Mt. Gox*. I would add to the list an event that took place in France: two weeks ago, the *Gendarmes* of the region of Midi-Pyrénées arrested three individuals who operated an illegal *bitcoin* exchange platform, and seized 388 *bitcoins*, worth more or less 200 000 euros.

Luckily, as the public hearing held on 15th January 2014 demonstrated, some private *bitcoin*-related businesses are calling for a regulatory framework. Unsurprisingly, they ask for maximum flexibility, whereas public authorities push for more control. Here's what is at stake: regulating effectively without killing innovation.

I am pleased to say that France reacted promptly to set up a regulatory framework. Ten days ago, Michel Sapin, the minister of finance and public accounts, announced several measures based on the work conducted at the initiative of our committee:

1. A clarification of the tax regime of virtual currencies. The gains from buying and selling *bitcoins* will be taxed under the progressive rate of the income tax (*impôt sur le revenu*) as commercial profits (*bénéfices industriels et commerciaux – BIC*) if the activity is ordinary, or as non-commercial profits (*bénéfices non commerciaux – BNC*) if the activity is occasional. As a consequence, losses will be deductible under certain conditions. Virtual currencies will also be considered as part of an individual's assets, and subsequently liable for wealth tax (*impôt de solidarité sur la fortune*) and transfer duties (*droits de mutation à titre gratuit*). As for VAT, France will support at the European level a tax exemption, in order to avoid reiterating the unfortunate experience of the massive VAT fraud over CO2 quotas.

2. A limitation of anonymity. Exchange platforms should be required to identify individuals when proceeding to an account opening, a cash withdrawal or deposit, and a transaction. A discussion has been launched on this topic, which is particularly complex since it has to see with the very principles of the system.

3. A cap on payments in virtual currencies, as it already exists for cash payments. In both cases, the reason is to compensate for the anonymity of transactions.

In addition, the prudential supervising authority (*Autorité de contrôle prudentiel et de resolution – ACPR*) estimated that companies operating as exchange platforms of virtual currencies vs. legal currencies would be considered – and regulated – as "provider of payment services" (*prestataire de service de payment – PSP*). For example, the exchange platform *Bitcoin-central* operated by *Paymium* holds an agreement from the ACPR, as its founder explained on the public hearing in January. *Providers of payment services* must respect a number of prudential ratios and anti-money laundering regulations.

How do French positions compare to those adopted by other countries? We have sent a questionnaire to the economical services of our embassies, and another one to the ministry of finance. The answers constitute an original work that will help understand and take upcoming decisions, especially at the European level.

Although all countries are facing the same questions, all do not come up with the same answers – this could be worrying as regards to the transnational nature of virtual currencies. In this international benchmark, France is situated halfway between the most regulatory jurisdictions and the most liberal ones:

1. As for the legal definition of virtual currencies, France has not been more successful than most other countries in establishing an official definition. In some countries like China, Thailand and South Korea, though, virtual currencies are assimilated to "goods", or more precisely "virtual goods" such as "mp3" audio files. The governor of the Chinese central bank made a parallel between *bitcoins* and stamps collections... Perhaps in a less poetical and so far more isolated way, the German supervision authority (*BaFin*) defined virtual currencies as "units of account", part of the boarder category of "financial instruments", like foreign currencies.

2. Many countries have been keener to tax virtual currencies than to define them – yet tax regimes remain very different. Virtual currency gains are liable for income tax in China, just like online gaming gains; they are taxed as real estate gains in Germany and as capital gains in the United States. Germany, the United Kingdom and other jurisdictions also chose to collect VAT on virtual currencies, but they are still looking for an effective way to do it... In Japan, tax payers are kindly invited to declare their transactions in *bitcoins*.

3. As for the regulation of transactions and exchange platforms, most authorities issued official warnings about the risks taken by users of virtual currencies, and the risks of money laundering and terrorism financing. However, not all countries decided to take regulatory actions in consequence – in fact, most of them tend to think, like Japan, that regulation equals legitimation, and therefore promotion. Countries such as Germany, Israel and Canada only warned *bitcoin* users that they were operating "at their own risks", without a public guarantee of any kind. "Hardline jurisdictions" are represented by China and Russia: these countries forbid, with some exceptions, the use of virtual currencies, and link it with a suspicion of money laundering. France could, in comparison, be deemed "carefully liberal": French authorities do not ban the use of virtual currencies but they subject platforms to the strict regulation of "provider of payment services" (PSP).

4. As for innovation, the United States, Canada and Israel are, unsurprisingly, among the most welcoming countries. Start-ups and business angels thrive while public authorities remain in a largely benevolent laissez-faire attitude. In Cyprus, the University of Nicosia accepts *bitcoins* for the payment of tuitions fees – although it seems few students have actually taken the plunge. That said, France has no reason to be ashamed when it comes to innovation: our finance technologies companies can be remarkably creative in the field of virtual currencies, but also in the field of alternative payments and funding (*crowdfunding*, smartphone payment, etc.).

In short, there are three ways to face the development of virtual currencies. The skeptical way, chosen by several legal experts and economists, who rightly underline that *bitcoin* is not a real currency – thereby forgetting the promising "technical" dimension of the system. The anxious way, chosen by most regulators – it is their job to foresee risks and prevent crises. And the optimistic way, chosen by those who believe that *bitcoin* will change transactions the same way e-mail changed traditional mailing, and the same way Internet changed traditional publishing. It is important to reassure the skeptical and the anxious, without discouraging the optimistic.

As a consequence, we make the following proposals. Public authorities should keep working and analyzing in the long term the development of virtual currencies. They should keep informing users and other stakeholders about the risks associated with virtual currencies, but also about the rights and protections they have. They should work on an adapted regulatory framework. All these actions are to be undertaken at the European level in order to be truly effective.

As for the legal definition of virtual currencies, we recommend to keep "testing" the use existing categories rather than creating new ones. Several countries, including France, chose to consider *bitcoins* as "goods": this "default status" allows the application of usual provisions for consumer protection, fraud and commercial disputes. This applies to the "thing" – as for the "service", it is already defined and regulated as a "provider of payment services" (PSP).

As in past revolutions brought along by digital technologies, France and Europe have opportunities to take. If we want to succeed together, we must support innovation and, at the same time, keep an eye on it to avoid taking the wrong way.

N° 767 rectifié

SÉNAT

SESSION EXTRAORDINAIRE DE 2013-2014

Enregistré à la Présidence du Sénat le 23 juillet 2014

RAPPORT D´INFORMATION

FAIT

au nom de la commission des finances (1) sur les **enjeux liés** *au* **développement** *du* **Bitcoin** *et des* **autres monnaies virtuelles**,

Par MM. Philippe MARINI et François MARC,

Sénateurs.

(1) Cette commission est composée de : M. Philippe Marini, *président ;* M. François Marc, *rapporteur général ;* Mme Michèle André, *première vice-présidente ;* Mme Marie-France Beaufils, MM. Jean-Pierre Caffet, Yvon Collin, Mmes Fabienne Keller, Frédérique Espagnac, MM. Albéric de Montgolfier, Aymeri de Montesquiou, Roland du Luart, *vice-présidents ;* MM. Philippe Dallier, Jean Germain, Claude Haut, François Trucy, *secrétaires ;* MM. Philippe Adnot, Claude Belot, Michel Berson, Éric Bocquet, Yannick Botrel, Joël Bourdin, Christian Bourquin, Mme Nicole Bricq, MM. Jacques Chiron, Serge Dassault, Vincent Delahaye, Francis Delattre, Mme Marie-Hélène Des Esgaulx, MM. Éric Doligé, Philippe Dominati, Jean-Paul Emorine, André Ferrand, François Fortassin, Thierry Foucaud, Yann Gaillard, Charles Guené, Edmond Hervé, Pierre Jarlier, Roger Karoutchi, Yves Krattinger, Dominique de Legge, Hervé Marseille, Gérard Miquel, Georges Patient, François Patriat, Jean-Vincent Placé, Jean-Marc Todeschini, Maurice Vincent, Richard Yung.

SOMMAIRE

LES CONCLUSIONS ET RECOMMANDATIONS DE LA COMMISSION DES FINANCES

Réunie le 23 juillet 2014 sous la présidence de M. Philippe Marini, président, la commission a entendu une communication de MM. Philippe Marini et François Marc, rapporteur général, sur les enjeux liés au développement du *bitcoin* et des autres monnaies virtuelles.

La commission a relevé que :

1° Le développement des monnaies virtuelles, et notamment du *bitcoin*, représente un phénomène de long terme, qui pose d'importantes questions économiques et juridiques, et qui **ne saurait être ignoré des pouvoirs publics**.

2° En dépit de risques clairement identifiés tenant à sa volatilité, à son anonymat et à son absence de garantie légale, **le *bitcoin* est porteur de multiples opportunités pour l'avenir**, en tant que moyen de paiement mais surtout en tant que technologie de validation décentralisée des informations.

3° Les pouvoirs publics doivent donc travailler à la mise en place d'un encadrement juridique équilibré, afin d'empêcher les dérives sans compromettre la capacité d'innovation. À cet égard, **le recours aux catégories juridiques de droit commun** apparaît pour l'instant la solution la plus raisonnable, à la fois pour qualifier les monnaies virtuelles et les services qui leur sont associés.

4° Les comparaisons internationales réalisées par la direction générale du Trésor à la demande des rapporteurs montrent que **la France se situe à mi-chemin entre les pays qui ont adopté les règles les plus strictes** – tels que la Chine, le Japon ou la Russie – **et les pays les plus ouverts** – tels que les États-Unis, le Canada ou Israël.

5° La clarification du régime applicable aux monnaies virtuelles devra nécessairement se faire **à l'échelle européenne, et si possible mondiale**, compte tenu du caractère transnational des monnaies virtuelles.

CONCLUSIONS AND RECOMMENDATIONS OF THE COMMITTEE ON FINANCE

Meeting on 23rd July 2014, under the chairmanship of Mr. Philippe Marini, president, the committee on finance heard a communication by Mr. Philippe Marini and Mr. François Marc, *rapporteur général*, on the questions raised by the development of the *bitcoin* and other virtual currencies.

The committee on finance noted that:

1° The development of virtual currencies, among which is the *bitcoin*, is a long-term trend, raising important legal and economic matters, that **can no longer be disregarded by public authorities**.

2° Despite a number of clearly identified risks resulting from its volatility, its anonymity and its lack of legal guarantee, **the *bitcoin* offers multiple opportunities for the future**, both as a payment system and, above all, as a decentralized validation protocol.

3° Public authorities should work on a well-balanced regulatory framework, in order to prevent abuses while preserving the capacity of innovation. To that effect, **the use of existing legal categories** seems like the most relevant solution for now, for the definition of both virtual currencies and associated services.

4° The international comparisons realized by the French Treasury for the committee on finance show that **France's choices are halfway between the strictest regulations** – adopted by countries such as China, Japan or Russia – **and the lightest regulations** – adopted by countries such as the United States, Canada or Israel.

5° The clarification of the regulatory framework applicable to virtual currencies is to be carried out **at the European level, and if possible at the international level**, considering the transnational nature of virtual currencies.

PREMIÈRE PARTIE : LA RÉGULATION À L'ÉPREUVE DE L'INNOVATION

LES POUVOIRS PUBLICS FACE AU DÉVELOPPEMENT DES MONNAIES VIRTUELLES

Les « monnaies virtuelles » connaissent depuis plusieurs années un développement très rapide, et suscitent de plus en plus l'attention des autorités, des médias et du grand public. La plus connue d'entre elles est le *bitcoin*, à la fois moyen de paiement et système de paiement libre, anonyme et décentralisé qui connaît un grand succès depuis deux ans.

La commission des finances du Sénat avait organisé une audition conjointe sur le sujet le 15 janvier 2014, afin de confronter les points de vue des différentes administrations – le Trésor, les douanes, la Banque de France, Tracfin – mais aussi d'un entrepreneur et d'un universitaire spécialiste du sujet. Deux questionnaires avaient dans la foulée été adressés au Gouvernement, l'un de portée générale et l'autre visant à comparer les positions adoptées par différents pays. Les réponses à ces questionnaires, qui sont annexées au présent rapport, pourront permettre **d'éclairer et de guider les décisions futures, notamment au niveau européen**.

L'intérêt que porte la commission des finances du Sénat à la question des monnaies virtuelles ne doit pas surprendre : depuis plusieurs années, la commission s'attache à comprendre les transformations profondes liés à **l'irruption du numérique dans la vie économique et financière**. Celles-ci emportent tout d'abord des **conséquences fiscales** : de fait, la concentration de la valeur sur des actifs immatériels extrêmement mobiles, et notamment les droits de propriété intellectuelle, a provoqué une attrition des assiettes fiscales dans les grands pays de consommation[1]. Au-delà de la fiscalité, **la révolution numérique vient bouleverser de fond en comble des secteurs économiques entiers** : le monopole des taxis est remis en cause par des applications de réservation sur *smartphone*, les hôtels subissent la double pression des sites de réservation en ligne et des solutions alternatives d'hébergement proposées sur Internet, et les professionnels de l'immobilier ont vu leur rôle d'intermédiaire contesté par des sites d'annonces entre particuliers.

[1] *Voir notamment le rapport d'information n° 614 (2011-2012) du 27 juin 2012 de Philippe Marini, fait au nom de la commission des finances,* « Une feuille de route pour une fiscalité numérique neutre et équitable », *ainsi que rapport d'information n° 93 (2013-2014) du 23 octobre 2013 de Albéric de Montgolfier et Philippe Dallier, fait au nom de la commission des finances,* « Les douanes face au commerce en ligne : une fraude fiscale importante et ignorée ».

Avec les monnaies virtuelles, c'est un élément plus fondamental encore qui est remis en cause : le monopole d'émission des banques centrales, manifestation par excellence du pouvoir régalien et clé de voûte de la politique monétaire. Exemple le plus connu et le plus « réussi », le *bitcoin*, créé en en 2009 par Satoshi Nakamoto[1], se veut une alternative libre, anonyme et décentralisée, permettant aux utilisateurs d'échanger entre eux des biens et des services sans avoir recours à la monnaie classique.

Stricto sensu, toutefois, il ne s'agit ni d'une monnaie ayant cours légal[2], ni d'un moyen de paiement au sens du code monétaire et financier (CMF) : contrairement à la « monnaie électronique », le *bitcoin* n'est pas émis contre la remise de fonds[3]. Il est un support de transactions. **Pour l'instant, le *bitcoin* relève avant tout d'une forme de troc en version numérique**.

Toutefois, vos rapporteurs estiment que l'on ne peut écarter d'un revers de main cette innovation, sous prétexte qu'il ne s'agirait que d'un épiphénomène. Le *bitcoin* connaît un succès croissant auprès des e-commerçants tels que le voyagiste *Expedia* ou encore l'éditeur de *blogs WordPress*, et il est désormais accepté par service de paiement en ligne *PayPal*. **Si le *bitcoin* connaît un tel développement, c'est qu'il présente des avantages tangibles, en dépit de risques clairement identifiés**.

I. LES MONNAIES VIRTUELLES : DES RISQUES CONNUS, DES OPPORTUNITÉS À DÉCOUVRIR

A. DES AVANTAGES AVÉRÉS

Le principal intérêt du *bitcoin* réside dans des frais de transaction réputés quasi-nuls : une étude de Goldman Sachs parue en mars 2014 estime ces frais de transaction à 1 %, contre 2,9 % prélevés par le service *PayPal*, lequel facture en outre 30 *cents* par transaction. **Signalons toutefois que ce débat n'est pas tranché**, dans la mesure où une estimation exacte devrait inclure, d'une part, le coût de l'équipement informatique et de l'électricité, et d'autre part, le coût du risque associé à la volatilité du *bitcoin* et des éventuelles couvertures à prévoir en conséquence.

Un autre intérêt notable tient à l'ingénieux mécanisme de « création monétaire » qui rémunère les utilisateurs du système : les transactions sont validées par les ordinateurs connectés au réseau ; en échange de la mise à disposition de leur puissance calcul, les « mineurs » se voient rétribués en *bitcoins* générés automatiquement par l'algorithme du

[1] *Satoshi Nakamoto n'a pas été identifié. Ce nom pourrait être le pseudonyme d'un programmeur ou d'une équipe de programmeurs.*
[2] *Il est par conséquent possible de refuser les paiements en* bitcoins *sans contrevenir aux dispositions de l'article R. 642-3 du code pénal, qui punit le fait de refuser les paiements libellés en euros, ayant cours légal.*
[3] *Article 4.15 de la directive 2007/64/CE du 13 novembre 2007 sur les services de paiement (DSP).*

système. On estime à environ 100 000 le nombre de processeurs participant aux opérations, parfois regroupés en véritables « fermes de minage », consommant d'importantes ressources mais pouvant engendrer d'importants profits.

Surtout, le *bitcoin* offre une très grande sécurité des transactions : celles-ci sont cryptées et validées par un grand nombre d'ordinateurs, de manière décentralisée, sans passer par un système « central » par définition plus vulnérable.

B. DES RISQUES À SURVEILLER

Il est vrai que le système comporte des risques notoires, qui ont conduit les régulateurs à multiplier les avertissements ces derniers mois[1].

En premier lieu, le *bitcoin* se caractérise par une très forte volatilité : un *bitcoin* valait moins d'un dollar jusqu'en 2011, presque 1 200 dollars à l'automne 2013, et environ 650 dollars aujourd'hui. **De fait, le système est intrinsèquement spéculatif, puisque la rareté y est pour ainsi dire programmée** : le rythme de création des *bitcoins* prévu par l'algorithme suit en effet une courbe décroissante, jusqu'à atteindre un maximum de 21 millions d'unités qui devrait être atteint en 2140, contre environ 12 millions d'unités aujourd'hui. Mais cette « rareté organisée » est aussi la condition de son succès puisqu'elle garantit les détenteurs contre une dévaluation de leurs avoirs : il n'existe pas de « planche à *bitcoins* ».

Autre faiblesse majeure, le *bitcoin* ne bénéficie d'aucune garantie de convertibilité en monnaie « réelle » par les pouvoirs publics. Ceci laisse les utilisateurs bien dépourvus en cas de perte généralisée de confiance dans le système. La valeur du *bitcoin* n'étant adossée à aucun actif « réel », tout l'édifice repose en effet sur la seule crédibilité que lui attribue la communauté des investisseurs.

Ensuite, si le protocole de validation des transactions est lui-même très sécurisé, il n'en va pas nécessairement de même pour le « stockage » des *bitcoins*. La plupart des utilisateurs décident de stocker leurs *bitcoins* sur des « comptes » ouverts auprès de plateformes d'échange en ligne. Mais **le piratage puis la faillite de *Mt. Gox*, la plus grande plateforme au monde, qui a ruiné près de 127 000 utilisateurs le 28 février 2014**, démontre la fragilité de ces « coffres forts » virtuels – d'autant que l'issue des recours judiciaires engagés aux États-Unis ou au Japon paraît bien incertaine. Bien sûr, il est aussi possible de stocker ses *bitcoins* sur un support physique personnel, tel qu'un disque dur, une tablette ou un *smartphone*. Mais les risques de perte ou de destruction accidentelle ne sont pas moindres : ainsi, James Howell, un Britannique qui avait acquis 7 500 *bitcoins* contre une poignée de livres sterling en 2009, a par erreur jeté son disque dur en croyant

[1] *Voir à ce sujet les réponses aux questions 1, 3 et 7 du questionnaire « général ».*

se débarrasser d'un matériel informatique obsolète ; la valeur des *bitcoins* stockés sur ce disque dur atteindrait aujourd'hui plusieurs millions de livres sterling…

Surtout, l'anonymat qui s'attache aux transactions fait du *bitcoin* une aubaine pour la cybercriminalité ou le blanchiment. C'est à ce jour la principale préoccupation des autorités des pays étudiés (cf. *infra*). De fait, les transactions en *bitcoins* sont bien plus difficiles à tracer que les transactions interbancaires classiques, même si cela n'est pas impossible. Par exemple, les services des douanes ont arrêté un trafiquant de stupéfiants qui se faisait payer en *bitcoins*, comme cela a été évoqué lors de l'audition du 15 janvier 2014. Certes, **le site *The Silk Road*, où l'on pouvait se procurer drogues, armes et contrefaçons diverses moyennement un paiement en *bitcoins*, a été fermé fin 2013** par le *Federal Bureau of Investigations* (FBI) américain. Mais il ne faudrait pas en déduire que tout risque est écarté, comme en témoigne l'arrestation, le 28 janvier 2014 à New York, de Charlie Shrem, vice-président de la *Bitcoin Foundation*, accusé d'avoir blanchi plus d'un million de dollars en *bitcoins* par l'intermédiaire d'une plateforme clandestine.

Toutefois, il convient de se garder de tout alarmisme à ce stade – même si la Banque de France, Tracfin et l'AMF sont dans leur rôle en appelant à la vigilance face aux risques encourus par les utilisateurs. **Pour l'heure, c'est précisément la volatilité et l'absence de statut légal du *bitcoin* qui devraient limiter son développement au-delà d'un cercle d'initiés** : en effet, quel particulier ou quel commerçant aurait intérêt à réaliser ses transactions au moyen d'un étalon dont la valeur peut être divisée par deux en moins d'une heure ? De deux choses l'une : soit le *bitcoin* connaît un développement encore plus important, et c'est que ses principales faiblesses auront été écartées ; soit les risques persistent, et la croissance sera entravée.

Par ailleurs, le *bitcoin* ne constitue en aucun cas une menace pour la stabilité macroéconomique, compte tenu de la masse monétaire négligeable qu'il représente : entre 5 et 8 milliards de dollars, contre des milliers de milliards de dollars pour les grandes devises. Aujourd'hui, il semble donc que le *bitcoin* tienne davantage du produit spéculatif de niche que d'une véritable alternative à la monnaie.

C. DE MULTIPLES POSSIBILITÉS À EXPLORER

L'attention accordée presque exclusivement aux risques revient à ignorer les multiples opportunités qu'ouvrent les monnaies virtuelles. Ce n'est pas parce qu'une innovation vient mettre au défi nos conceptions traditionnelles de l'économie et de la souveraineté qu'il faut les rejeter en bloc, d'autant qu'il serait très difficile d'empêcher les particuliers d'en faire usage sur des plateformes *offshore*, hébergées à l'étranger.

D'abord, en tant qu'alternative aux monnaies légales, les monnaies virtuelles n'ont sans doute pas encore déployé tout leur potentiel. Les plus

optimistes parlent ainsi de mettre en place des offres de crédit ou encore de financement participatif (*crowdfunding*) en *bitcoins*.

Mais surtout, plus encore qu'une « monnaie », le *bitcoin* est une technologie, un protocole de validation des transactions entièrement décentralisé, « auditable » par tous et très sécurisé. En effet, dans le protocole *bitcoin*, aucun « tiers de confiance » n'est jamais en possession de l'information complète, celle-ci étant néanmoins parfaitement vérifiée. **Or, s'il est possible de valider des transactions par cette méthode, pourquoi ne pas s'en servir pour valider autre chose ?** Par exemple, des mots de passe, des titres d'identités, des diplômes et autres certificats, ou même des votes électroniques. La fraude sur l'authenticité de nombreux documents ou procédures pourrait s'en trouver considérablement réduite.

D'ailleurs, le *bitcoin* n'est pas la seule « monnaie virtuelle », loin s'en faut : il y en a eu d'autres hier (*Liberty Reserve*, *e-Gold*), il y en aura d'autres demain (le *litecoin* est par exemple inspiré du *bitcoin*). **Il est donc très important pour les pouvoirs publics de ne pas rester en retrait et d'accompagner ces innovations par une régulation adaptée.**

II. RÉGULER SANS ENTRAVER : LE CHEMIN ÉTROIT DES POUVOIRS PUBLICS

A. LES CHOIX DE LA FRANCE : UNE RÉGULATION INACHEVÉE ?

La régulation des monnaies virtuelles apparaît aujourd'hui comme une nécessité, à la fois pour sécuriser les utilisateurs et les acteurs qui prennent le risque d'innover, et pour prévenir les dérives qui, sinon, continueront à décrédibiliser le système dans son ensemble. Toutefois, il est difficile d'apporter une réponse normative à un phénomène qui se joue des frontières géographiques autant que des cadres conceptuels.

L'audition du 15 janvier 2014 au Sénat a montré que **certains acteurs privés présents sur le marché du *bitcoin* étaient en attente d'une régulation**, ce dont il faut se féliciter. De nombreux acteurs français, regroupés au sein de l'*Association Bitcoin France*, ont ainsi appelé le 9 juillet 2014 à l'établissement d'un cadre réglementaire stable[1]. Sans surprise, les professionnels demandent un maximum de souplesse et un « moratoire » sur la fiscalité, là où les autorités plaident pour des contrôles plus pointilleux et un traitement fiscal normal. **L'enjeu est ici de réguler efficacement sans « tuer » l'innovation**.

La France a su réagir assez rapidement en matière de régulation. Le 11 juillet 2014, en se fondant notamment sur les travaux conduits à

[1] *Association Bitcoin France, «* Quatre propositions pour un développement responsable de Bitcoin en France *», 9 juillet 2014.*

l'initiative de votre commission ainsi que sur le rapport du groupe de travail piloté par Tracfin[1], **le ministre des finances et des comptes publics, Michel Sapin, a annoncé plusieurs mesures très concrètes** :

1) Une clarification du régime fiscal applicable aux monnaies virtuelles par l'instruction fiscale du 11 juillet 2014. Les plus-values seront ainsi imposées au **barème progressif de l'impôt sur le revenu**, au premier euro, au titre des bénéfices non-commerciaux (BNC) si celle-ci est occasionnelle[2], ou des bénéfices industriels et commerciaux (BIC) si l'activité d'achat-revente est habituelle[3] – le cas devrait être peu fréquent au-delà des plateformes d'échange. **Par voie de conséquence, les moins-values seront déductibles sous certaines conditions**[4]. Les *bitcoins* et leurs équivalents entreront par ailleurs dans le patrimoine imposé au titre de l'**impôt de solidarité sur la fortune (ISF)** et seront soumis aux **droits de mutation à titre gratuit (DMTG)**. En revanche, **la France soutiendra au niveau européen un non-assujettissement à la TVA des échanges de *bitcoins***[5], afin d'éviter de réitérer l'expérience malheureuse des « quotas carbone » qui ont donné lieu à un gigantesque « carrousel TVA ».

2) Une limitation de l'anonymat : le ministre entend imposer aux plateformes d'échange une obligation de prise d'identité à l'occasion d'une ouverture de compte, d'un retrait ou d'un dépôt. Au niveau européen, il est proposé d'imposer aux professionnels d'identifier l'auteur et le bénéficiaire de chaque transaction, ainsi que l'origine des fonds. Une concertation a été engagée avec les professionnels sur ce sujet.

3) Un plafonnement des paiements en monnaies virtuelles, comme cela existe pour le numéraire[6] : dans les deux cas, cela se justifie par l'anonymat qui s'attache aux transactions.

En ce qui concerne la régulation des « services » liés au *bitcoin*, il faut signaler que **l'Autorité de contrôle prudentiel et de régulation (ACPR) considère que les intermédiaires proposant d'échanger des « monnaies virtuelles » contre des monnaies ayant cours légal sont soumis au statut de prestataire de services de paiement (PSP)**. À ce titre, ils doivent solliciter un agrément de l'ACPR, respecter diverses obligations prudentielles, et sont assujettis aux règles de lutte contre le blanchiment et le financement du

[1] *Groupe de travail « monnaies virtuelles », «* L'encadrement des monnaies virtuelles : recommandations visant à prévenir leurs usages à des fins frauduleuses ou de blanchiment *», juin 2014.*
[2] *Article 92 du code général des impôts.*
[3] *Article 34 du code général des impôts.*
[4] *Les moins-values sont déductibles sur la totalité du bénéfice dans le cas des BIC, et seulement dans la même catégorie d'activité dans le cas des BNC.*
[5] *Les biens et services vendus en* bitcoins *restent bien sûr, à l'instar des biens vendus en euros, soumis à la TVA dans les conditions de droit commun.*
[6] *Aux termes de l'article article D. 112-3 du code monétaire et financier, le plafond des paiements en espèces à un commerçant est fixé à 3 000 euros, ou 15 000 euros si le domicile fiscal est situé hors de France.*

terrorisme. Ainsi, les utilisateurs qui ouvrent un compte auprès d'une plateforme d'échange telle que la française *Paymium* (anciennement *Bitcoin-Central*), ouvrent en même temps un compte auprès de cet établissement de paiement agréé. Trois personnes qui opéraient une plateforme d'échange de *bitcoins* sans autorisation ont, à l'inverse, été arrêtées le 7 juillet 2014 par les gendarmes de la région Midi-Pyrénées, qui ont à cette occasion « saisi » 388 bitcoins, soit environ 200 000 euros.

D'un point de vue comptable, les *bitcoins* sont, d'après les éléments transmis à vos rapporteurs, considérés par les entreprises comme des **stocks**, et inscrits au bilan à leur valeur vénale au moment de l'achat et de la vente. Aucune autorité comptable n'a toutefois pris de position officielle à ce jour.

B. UNE COMPARAISON INTERNATIONALE

Les réponses au questionnaire adressé par vos rapporteurs aux missions économiques de la direction générale du Trésor montrent que **si tous les pays se posent à peu près les mêmes questions, tous n'y apportent pas les mêmes réponses**. Pour l'instant, ces divergences sont davantage le reflet d'hésitations que de conceptions opposées de la part des différents pays. Toutefois, **à terme, le maintien de qualifications juridiques hétérogènes pourrait poser problème**, le phénomène des monnaies virtuelles étant par essence transnational. Il ne faudrait pas que le *bitcoin* s'ajoute à la liste des « produits hybrides » qui permettent, grâce à une qualification juridique différente selon les pays, d'échapper à toute régulation ou à toute taxation[1].

Les comparaisons avec les treize pays étudiés par les services de la direction générale du Trésor montrent que **la France se situe à mi-chemin entre les pays les plus régulateurs et les pays les plus permissifs**.

1. La qualification juridique des monnaies virtuelles

Il n'existe pas à ce jour de consensus quant à la nature juridique des monnaies virtuelles, entre les différents pays ou, en « interne », entre leurs différentes administrations. À cet égard, la France évolue dans le même flou que la plupart des autres pays, tels que le Canada, Chypre, l'Inde, Israël, le Japon ou encore le Royaume-Uni.

Toutefois, certains pays comme la Chine, la Thaïlande ou la Corée du Sud considèrent explicitement les monnaies virtuelles comme des « biens » ou des « marchandises », fussent-elles numériques, à l'instar d'un

[1] *Le projet « BEPS » (« Base Erosion and Profit Shifting ») de l'OCDE (Organisation de coopération et de développement économiques), qui vise à lutter contre l'érosion des bases fiscales et le transfert de bénéfices, considère précisément les produits et dispositifs hybrides l'une des principales « failles » de la fiscalité internationale.*

fichier musical « mp3 ». Le gouverneur de la Banque central chinoise a ainsi comparé les *bitcoins* aux timbres échangés par les philatélistes[1].

La BaFin, l'autorité de supervision financière allemande, fait figure d'exception en qualifiant les monnaies virtuelles d'« unités de compte », qui entrent dans la catégorie des instruments financiers au même titre que les devises. Cette définition sous-entend que le *bitcoin* s'apparenterait à une quasi-monnaie. En France, l'Autorité des marchés financiers (AMF) a récemment défini la monnaie virtuelle comme une « monnaie non-régulée et numérique », sans toutefois être suivie en cela par le Gouvernement[2].

2. Le régime fiscal applicable aux monnaies virtuelles

Plusieurs pays ont choisi d'imposer la détention et les transactions de monnaies virtuelles, quand bien même celles-ci n'auraient pas reçu de définition légale.

Les régimes fiscaux choisis demeurent toutefois très hétérogènes : assimilés aux gains aux jeux en ligne par la Chine et à ce titre taxés à l'impôt sur le revenu, les *bitcoins* sont imposés comme des biens immobiliers par l'Allemagne et comme des revenus du capital par les États-Unis, ce qui emporte une taxation des plus-values.

En matière de TVA, il convient de distinguer la vente de biens et de services contre des *bitcoins*, et les échanges de *bitcoins* contre des monnaies légales. Dans le premier cas, il semble que la TVA doive s'appliquer dans les conditions de droit commun ; la taxe est alors calculée d'après la valeur en monnaie légale des biens et services. Dans le cas des échanges de *bitcoins* eux-mêmes et des services liés, les appréciations divergent entre les pays qui se sont exprimés sur le sujet – Allemagne, Royaume-Uni, Singapour etc. **Au niveau européen, la France prônera un non-assujettissement**, compte tenu des risques de fraude qui s'attachent au remboursement des créances de TVA sur les actifs immatériels.

Enfin, certains pays n'ont émis aucune règle ni donné aucune précision quant au traitement fiscal des monnaies virtuelles : c'est le cas de Chypre, de l'Inde (malgré un projet inabouti), d'Israël, de la Russie ou encore de la Thaïlande.

3. La régulation des échanges de monnaies virtuelles

En ce qui concerne la régulation des transactions et des plateformes d'échange, **la plupart des pays ont multiplié les avertissements**, d'abord sur

[1] *À noter que la Chine dispose, par ailleurs, d'une définition ad hoc pour les monnaies virtuelles utilisées dans les jeux en ligne.*
[2] *Autorité des marchés financiers, « Cartographie 2014 des risques et des tendances sur les marchés financiers et pour l'épargne », conférence de presse du 4 juillet 2014.*

les risques encourus par les utilisateurs des monnaies virtuelles, et surtout sur les risques de blanchiment et de financement du terrorisme. Toutefois, tous n'en concluent pas que cela justifie une intervention du régulateur, voire du législateur : **beaucoup considèrent, à l'instar du Japon, que réguler revient à légitimer, et donc à encourager**. Ainsi des pays comme l'Allemagne, Israël ou le Canada se contentent-ils de **prévenir les utilisateurs de *bitcoins* qu'ils agissent « à leurs risques et périls »**, sans garantie publique d'aucune sorte.

Les positions les plus strictes viennent de la Russie, de la Chine et du Japon. La Chine et le Japon interdisent tout usage du *bitcoin* aux établissements financiers, et notamment l'échange contre des devises ; en Chine, les détenteurs de *bitcoins* sont toutefois autorisés à échanger cette « marchandise » entre eux. Plus stricte encore, **la Russie attache tout simplement à l'usage des monnaies virtuelles une présomption de « *participation à des opérations illégales*, *notamment de blanchiment d'argent et de financement du terrorisme* »**.

La France fait à cet égard preuve d'un libéralisme prudent, en n'interdisant pas les monnaies virtuelles mais en assujettissant les plateformes au statut encadré de **prestataire de service de paiement (PSP)**. Un choix comparable a été fait par les États-Unis, les plateformes ayant l'obligation de s'enregistrer auprès du *Financial Crimes Enforcement Network* (FinCEN) chargé de la lutte anti-blanchiment.

4. Le soutien à l'innovation

Sans surprise, c'est aux États-Unis, au Canada ou encore en Israël que l'innovation en matière de monnaies virtuelles est la plus dynamique. Les incubateurs, *business angels* et autres *start-ups* s'y multiplient, dans un contexte de bienveillance des autorités publiques – aucun fonds public spécifique n'ayant toutefois pu être identifié lors des recherches. Aux États-Unis, près de 100 millions de dollars ont été levés depuis la création du *bitcoin* en 2009, au bénéfice de 19 *start-ups*. Au Canada, la ville de Vancouver se targue d'avoir hébergé le premier « distributeur automatique » de *bitcoins*. En Israël, plusieurs dizaines de commerces acceptent *bitcoins* et « *Isracoins* », une monnaie virtuelle locale créée en 2014. À Chypre, l'université de Nicosie accepte le paiement des frais de scolarité en *bitcoins*, même si peu d'étudiants ont semble-t-il sauté le pas.

C. LES RECOMMANDATIONS DE VOS RAPPORTEURS

Trois « profils » résument les différentes attitudes adoptées face au développement des monnaies virtuelles. D'abord, **les « sceptiques »**, parmi lesquels figurent de nombreux juristes et économistes : ceux-ci soulignent à bon droit que le *bitcoin* n'est pas une véritable monnaie, mais ils oublient la

très prometteuse dimension « technique » du système. Ensuite, **les « inquiets »**, dont font partie la plupart des régulateurs, car il est de leur devoir d'anticiper les problèmes et de les prévenir. Enfin, **les « optimistes »**, qui considèrent, pour reprendre une expression souvent utilisée, que le *bitcoin* est aux transactions ce que *l'email* a été au courrier et le *web* à l'édition.

Le potentiel de développement des monnaies virtuelles est important, et justifie l'élaboration d'un cadre juridique qui permette de favoriser l'innovation tout en prévenant les dérives. Les pouvoirs publics doivent ainsi mener dans la durée un véritable travail de veille et de réflexion sur les monnaies virtuelles, et continuer à informer les utilisateurs sur les risques mais aussi les droits associés.

Il importe surtout de **mettre en place une régulation au niveau de l'Union européenne et si possible au niveau international**, condition *sine qua non* de son efficacité : les monnaies virtuelles sont des monnaies sans frontières.

Concernant la qualification juridique des monnaies virtuelles, et dans l'attente d'une réflexion juridique plus aboutie, il convient de **continuer à « tester » pour l'instant le recours aux catégories du droit existantes, et d'appliquer dans la mesure du possible le droit commun** plutôt que de créer une catégorie *ad hoc*. De fait, l'absence de qualification juridique des monnaies virtuelles, correspondant au choix de la plupart des pays aujourd'hui, emporte **plusieurs avantages** :

- d'une part, l'application par défaut du droit commun des biens « ordinaires », notamment en termes de protection des consommateurs, d'escroquerie et de litiges commerciaux. Ainsi, l'absence de qualification spécifique ne signifie pas qu'il existe un vide juridique.

- d'autre part, une imposition au barème de l'impôt sur le revenu dans les conditions de droit commun, au titre des BIC ou des BNC, ainsi qu'un assujettissement à l'ISF et aux droits de mutation, comme le précise l'instruction fiscale du 11 juillet 2014 (cf. *supra*). La question de l'application effective de ce traitement fiscal, et notamment du contrôle des déclarations souscrites par les contribuables, reste toutefois posée – même si les enjeux financiers sont pour l'instant très faibles.

Par ailleurs, **le fait que les plateformes d'échanges soient soumises au statut de prestataires de services de paiement (PSP) (cf. *supra*) permet l'application des règles de lutte anti-blanchiment aux monnaies virtuelles**, même si ces dernières n'y sont pas soumises *en tant que telles* faute de qualification juridique. De fait, les monnaies virtuelles n'offrent d'intérêt en termes de blanchiment et d'activités illicites que si elles peuvent *in fine* être converties en monnaies « officielles », ce qui suppose de passer à un moment où un autre par une plateforme d'échange. **Toutefois, il pourrait être opportun de mentionner *explicitement* dans le droit en vigueur l'application des règles de lutte contre le blanchiment et le financement du**

terrorisme : la révision en cours de la directive sur les services de paiement (DSP)[1], pourrait être l'occasion de le faire, et d'harmoniser les positions des différents États membres. Par ailleurs, une mention pourrait être introduite dans le code monétaire et financier (CMF), par anticipation ou transposition.

À défaut de s'en tenir au droit commun, **trois solutions pourraient être envisagées** :

1) Assimiler les monnaies virtuelles aux « instruments financiers » au sens de l'article L. 211-1 du code monétaire et financier (CMF), **par référence notamment aux devises**, avec deux conséquences principales :

- l'application de règles spécifiques aux marchés financiers, dont l'application relève de l'Autorité des marchés financiers (AMF) et de l'Autorité de contrôle prudentiel et de régulation (ACPR).

- un traitement fiscal analogue aux plus-values sur les opérations de change. Toutefois, d'après les éléments transmis à votre président et à votre rapporteur général, il n'existe pas à ce jour de disposition spécifique concernant la fiscalité des devises…

2) Qualifier les monnaies virtuelles de « biens meubles » immatériels au sens de l'article 150 UA du code général des impôts, ce qui entraînerait l'application d'une **exonération des plus-values lorsque le prix de cession est inférieur à 5 000 euros** – c'est par exemple la solution retenue pour les « quotas carbone ». Une imposition « par défaut » au premier euro, dans les conditions de droit commun, semble toutefois préférable à ce stade compte tenu du montant de la plupart des transactions.

3) Assimiler les monnaies virtuelles à l'or, ce qui permettrait de déclencher la **compétence de la direction générale des douanes et des droits indirects (DGDDI)** – qui est à l'origine de la proposition – au titre des transferts physiques de capitaux au-delà du seuil de 10 000 euros[2]. L'application pratique de cette mesure pose toutefois question, compte tenu de la nature différente de l'or et des monnaies virtuelles.

En conclusion, la France dispose de véritables atouts dans le contexte du développement des monnaies virtuelles. **D'abord, un certain nombre d'acteurs importants** – qui visent d'ailleurs un marché européen plus que national –, de surcroît déjà organisés. **Ensuite, une capacité d'innovation avérée** en matière de technologies financières, qui a déjà fait ses preuves en ce qui concerne les modes alternatifs de paiement (*crowdfunding*, paiement par *smartphone* etc.) et pourrait aujourd'hui s'étendre aux monnaies virtuelles. **Enfin, un cadre réglementaire et fiscal en construction, caractérisé par son pragmatisme**. Il convient à cet égard de

[1] *Directive 2007/64/CE du 13 novembre 2007 sur les services de paiement (DSP).*

[2] *Article L. 152-1 du code monétaire et financier (CMF). L'article 54 de la loi n°2013-1117 du 6 décembre 2013 relative à la lutte contre la fraude fiscale et la grande délinquance économique et financière a étendu la compétence de la DGDDI aux transferts sous forme de cartes prépayées, d'or et de jetons de casino.*

noter que la supervision des « services » et la qualification des « objets » ne suffiront pas à empêcher pas les détenteurs de *bitcoins* de les utiliser pour vendre ou d'acquérir des biens illégaux : **l'action des forces de l'ordre et de la justice est complémentaire de la mise en place d'un cadre réglementaire**.

Les monnaies virtuelles et les technologies qui leur sont liées ouvrent de vastes perspectives, qui ne sauraient être ignorées ou seulement rejetées : il importe, dès lors, de **poursuivre la démarche de régulation engagée, dans un esprit d'ouverture teinté de vigilance**.

SECONDE PARTIE :
ANNEXES

LETTRE DES RAPPORTEURS AU MINISTRE

SÉNAT — *République Française*

COMMISSION DES FINANCES

LE PRÉSIDENT

LE RAPPORTEUR GENERAL

SB

Paris, le 19 mars 2014

Monsieur le Ministre,

La commission des finances du Sénat a organisé le 15 janvier 2014 une audition portant sur les enjeux liés au développement des monnaies virtuelles, parmi lesquelles figure le *bitcoin*. Etaient notamment présent des représentants de la direction générale du Trésor, de la Banque de France, de TRACFIN et de la direction nationale du renseignement et des enquêtes douanières.

L'intérêt porté par les membres de la commission des finances à cette audition ainsi que les développements récents de l'actualité nous ont convaincu de poursuivre notre travail sur le sujet.

C'est pourquoi, nous vous adressons deux questionnaires, pour lesquels nous souhaiterions obtenir des réponses avant le 30 avril 2014. Le second est un questionnaire-type qui pourrait être adressé à différents services économiques régionaux.

Ces réponses sont susceptibles d'être reproduites et nous vous prions de bien vouloir nous indiquer celles qui doivent rester confidentielles.

Nous vous prions d'agréer, Monsieur le Ministre, l'expression de notre haute considération.

Philippe MARINI
Président

François MARC
Rapporteur général

Monsieur Pierre MOSCOVICI
Ministre de l'économie et des finances
139, rue de Bercy
75 572 PARIS Cedex 12

RÉPONSES DE L'ADMINISTRATION AU QUESTIONNAIRE GÉNÉRAL

Travail coordonné par la direction générale du Trésor (DGT) à la demande du président et du rapporteur général de la commission des finances du Sénat. Les informations transmises sont reproduites ci-dessous dans leur intégralité.

1) <u>Transmettre l'ensemble des documents produits par l'administration relatifs aux monnaies virtuelles (rapports, notes, circulaires, etc.).</u>

La **Banque de France** a publié le 5 décembre 2013 sur son site Internet un « Focus » sur les monnaies virtuelles[1] mettant en garde les utilisateurs des monnaies virtuelles sur les risques qu'ils encourent.

L'**Autorité de contrôle prudentiel et de résolution** a publié une position et un communiqué le 29 janvier 2014 relatifs aux opérations sur les Bitcoins en France[2].

La Direction générale du Trésor a diffusé le 7 mai 2014 un « non-paper » à l'intention du Comité des services financiers qui réunit l'ensemble des Etats membres de l'UE. Certains **services économiques** auprès des ambassades ont également produit des notes d'analyse début 2014.

La **Direction du Renseignement Douanier** (DRD) de la DGDDI a produit plusieurs analyses qui ont servi à alimenter les réflexions du groupe de travail lancé par TRACFIN (cf. ci-dessous) :

- décembre 2013 : une étude relative à l'état des lieux des monnaies virtuelles en sources ouvertes, actualisée en février en 2014,
- janvier 2014 : trois notes de tendance relatives à *Webmoney*, *BTC China* et *Mt. Gox*.

Par ailleurs, plusieurs travaux sont en cours au sein de la **Direction Nationale du Renseignement et des Enquêtes Douanières**. La division « veille et analyse stratégique » effectue une veille sur la problématique des monnaies virtuelles en tant que menace potentielle pour les activités douanières avec le soutien du groupe renseignement financier de la DSAO.

[1] *Cf.* *http://www.banque-france.fr/fileadmin/user_upload/banque_de_france/publications/Focus-10-stabilite-financiere.pdf*
[2] *Cf.* *http://acpr.banquefrance.fr/fileadmin/user_upload/acp/publications/registre-officiel/201401-Position-2014-P-01-de-l-ACPR.pdf*

Deux études seront publiées dans les mois à venir sur :

- les liens entre e-commerce et monnaies virtuelles afin d'identifier les risques et les opportunités de croissance que ces monnaies pourraient offrir pour le commerce en ligne ;
- les ouvertures prochaines d'échangeurs de monnaies virtuelles qui permettent des retraits de métaux précieux, tel que *Ripple*. En effet, avec l'augmentation des actes de blanchiment utilisant l'or, les échangeurs utilisant les métaux précieux pourraient intéresser les blanchisseurs.

Cyberdouane réalise des enquêtes sur des marchandises illégales ou illicites pouvant être acquises par le biais de monnaies virtuelles (cf. première opération d'achat en Bitcoins, qui a permis l'interpellation d'un trafiquant de stupéfiants).

Enfin, un rapport sur les monnaies virtuelles, présentant les conclusions d'un groupe de travail lancé par **Tracfin** en décembre 2013, est attendu pour l'été 2014. Ce groupe de travail inter-administrations (cf. question 2 pour une présentation détaillée) a pour objectif d'étudier les risques émanant des monnaies virtuelles ainsi que les moyens de limiter ces risques.

2) <u>Indiquer si des structures de réflexion sur ce sujet ont été mises en place au sein de ou par l'administration. Si oui, préciser leur mission, leur composition et l'échéancier de leurs travaux.</u>

Les autorités de régulation et de contrôle françaises ont engagé un certain nombre de réflexions sur le sujet des monnaies virtuelles, qui ont pris plusieurs formes.

Dans le prolongement de réflexions engagées en 2011[1], Tracfin a lancé en décembre 2013 un groupe de travail inter-administrations sur les monnaies virtuelles, associant la Direction Générale du Trésor (DGT), la Direction Générale des Douanes et des Droits Indirects (DGDDI), la Direction Générale de la Concurrence, de la Consommation et de la Répression des Fraudes (DGCCRF), la Direction des Affaires Criminelles et des Grâces (DACG), la Direction Centrale de la Police Judiciaire (DCPJ), la Direction Générale de la Gendarmerie (DGG), la Direction Générale des Finances Publiques (DGFiP), l'Autorité des Marchés Financiers (AMF), l'Autorité de Contrôle Prudentiel

[1] *Tracfin avait alors piloté un groupe de travail sur les nouveaux moyens de paiement ; la monnaie virtuelle avait fait partie des questions évoquées. Le rapport annuel 2011 de Tracfin reprend les résultats des travaux de ce groupe.*

et de Résolution (ACPR), la Banque de France ainsi que la Direction Centrale du Renseignement Intérieur (DCRI).

Ce groupe s'est réuni en décembre 2013, ainsi qu'en janvier, avril et juin 2014 afin de dresser un panorama des risques et menaces présentés par les monnaies virtuelles. Ses travaux déboucheront sur des propositions visant à limiter ces risques à l'été 2014.

Le service a également proposé qu'un appel à vigilances soit formulé à l'attention des professionnels déclarants pour les inviter à signaler particulièrement des opérations en lien avec des plates-formes internet permettant la conversion ou l'achat-revente de monnaies virtuelles. Par ailleurs, à l'occasion de ses rencontres avec les représentants des déclarants du secteur bancaire, Tracfin recommande la mise en place d'une vigilance « monnaies virtuelles ».

Des échanges réguliers ont également lieu entre la Direction générale du Trésor, l'AMF, la Banque de France et l'ACPR sur les monnaies virtuelles et les réponses réglementaires qu'il pourrait être nécessaire d'y apporter, au regard des travaux internationaux actuellement en cours dans plusieurs enceintes européennes (ESMA, BCE et EBA notamment).

3) Indiquer si la France a sollicité des prises de position sur le sujet au niveau européen (Commission européenne, BCE, EBA). Indiquer si des échanges ont lieu avec les administrations étrangères ou dans le cadre de l'Union européenne.

L'ancien ministre de l'Économie et des Finances, Pierre Moscovici, a souligné, en mars 2014, la nécessité que soit lancée une réflexion européenne sur les monnaies virtuelles (communiqué de presse du 5 mars 2014). Il a rappelé que les règles de protection des consommateurs et des investisseurs ne s'appliquaient pas efficacement aux avoirs détenus en monnaies virtuelles – notamment en *bitcoins* - et a appelé les consommateurs à la plus grande vigilance dans leur détention et leur utilisation. Il a annoncé son intention de saisir les Etats membres de l'Union européenne de la question en portant le sujet à l'examen du Conseil.

Par ailleurs, plusieurs enceintes techniques se sont déjà saisies de cette question, et les représentants français participent activement aux discussions qui s'y déroulent.

A – Au niveau européen

1. Deux groupes d'experts présidés par la DG Marché intérieur de la Commission européenne ont eu l'occasion d'aborder le sujet des monnaies virtuelles :

- le groupe de travail en matière de lutte contre le blanchiment, qui attend les résultats des travaux d'identification des risques liés aux monnaies virtuelles menés par l'Autorité bancaire européenne (EBA) et réfléchit aux approches réglementaires envisageables pour contrôler les risques identifiés.

- le groupe de travail chargé au Conseil de la négociation de la révision de la directive sur les services de paiement : une première discussion, non conclusive, a souligné les interrogations et les attentes des Etats membres quant à l'application de la règlementation en matière de paiement aux plateformes qui convertissement des monnaies virtuelles. La Commission européenne a indiqué qu'elle était favorable à une approche commune sur le sujet, et qu'il convenait également d'attendre les premières conclusions des travaux menés par l'EBA.

2. Le Comité des services financiers (ou Financial Services Committee – FSC), où la France est représentée par la direction générale du Trésor, a évoqué, lors de ses réunions du 7 mai et du 27 juin 2014, les conclusions provisoires de l'EBA au sujet des monnaies virtuelles. L'EBA a mentionné différentes options qui vont du statu quo à l'interdiction en passant par différents niveaux d'encadrement. À cette occasion, la France a proposé, par un document de position, une approche coordonnée du sujet et a suggéré que les Etats membres prennent une position sur l'opportunité de considérer que les plates-formes de conversion de monnaies virtuelles en devises ayant cours légal soient soumises à un agrément sur la base de la directive sur les services de paiement.

3. Les autorités européennes de supervision conduisent également des travaux :

- L'Autorité bancaire européenne (EBA), qui associe les superviseurs bancaires, dont l'Autorité de contrôle prudentiel et de résolution (APCR) pour la France, a conduit des travaux au cours du printemps 2014 visant à inventorier les risques liés aux monnaies virtuelles et à définir les approches réglementaires envisageables. Ces travaux ont donné lieu à la publication d'un rapport début juillet 2014.

- L'Autorité européenne des marchés financiers (ESMA), où la France est représentée par l'Autorité des marchés financiers (AMF), réfléchit avec ses homologues étrangers sur les risques posés par les monnaies virtuelles, notamment via le comité permanent chargé de l'innovation financière (*Financial Innovation Standing Committee*).

4. La BCE a réalisé un rapport en 2012 sur les monnaies virtuelles dont l'actualisation est en cours. Ce document de référence recense les risques et les questions que posent les monnaies virtuelles.

B - Au plan international

1. Le sujet est traité par le Groupe d'action financière (GAFI). La France participe aux travaux de ce groupe qui a examiné un premier document lors de sa réunion des 25-27 juin 2014. Ce document intitulé « les définitions clés et les risques potentiels en matière de lutte contre le blanchiment et le financement du terrorisme de la monnaie virtuelle » a été publié à l'issue de la réunion du GAFI. Il souligne que ces monnaies sont appelées à se développer[1] et qu'elles sont des outils puissants de circulation et de stockage de fonds illicites pour les blanchisseurs et les terroristes, hors d'atteinte des lois et de la justice.

Cette étude constitue pour le GAFI une évaluation préliminaire des risques de blanchiment et financement du terrorisme associés, tenant compte notamment des différents types de monnaies virtuelles. Ce rapport présente une série de définitions clés et constitue une base pour la production de bonnes pratiques ou de lignes directrices à l'attention des autorités compétentes et des professionnels assujettis (institutions financières, assurances, professions du chiffre et du droit, jeux, agents immobiliers, etc.).

2. A noter également, les travaux de l'Organisation Internationale des Commissions de Valeurs (OICV), en particulier son comité chargé des risques émergents (*Committee on Emerging Risks*) au sein duquel siège l'AMF, et chargé de l'analyse des risques menaçant la stabilité financière ou le bon fonctionnement des marchés.

3. La Banque des règlements internationaux (BRI) examine également le sujet des monnaies virtuelles, avec des analyses menées au sein du CPSS.

4. Une première discussion a eu lieu au sein du comité permanent sur la coopération en matière de supervision et de réglementation (*Standing Committee on supervisory and regulatory cooperation*, SCSRC) du Financial Stabilty Board (FSB) le 3 juillet 2014.

[1] *Cas d'*Alipay *ou de* Google Checkout *par exemple.*

4) Quelle est la nature juridique des monnaies virtuelles ? S'il semble admis qu'il ne s'agit pas d'une monnaie au sens du code monétaire et financier, s'agit-il : d'un bien (comme de l'or) ? d'un service ? Dans ce cas, s'agit-il d'un service régulé, comme un service de paiement ou de monnaie électronique, ou d'un service d'investissement ?

Le concept de monnaie virtuelle est généralement appréhendé sous trois angles possibles :

- monnaie privée ;
- actif physique (comme l'or) ;
- actif financier.

De très nombreuses monnaies virtuelles sont en circulation. De natures variées, les monnaies virtuelles servent à la fois de moyen de paiement et de système de paiement qui, dans certains cas, peut être également interconnecté aux réseaux financiers réguliers. Il est donc difficile de classer les monnaies virtuelles dans une même catégorie alors que leurs systèmes sont très variés.

À ce jour, la nature juridique des monnaies virtuelles n'est, en France, pas tranchée. Au plan international, certains pays se sont prononcés, de façon assez diverse sur ce point, suivant les objectifs poursuivis (lutte contre l'évasion fiscale, lutte contre le blanchiment et le financement du terrorisme…).

a) La qualification des monnaies virtuelles peut être considérée au regard de différentes branches du droit qui peuvent entrer en conflit.

Ainsi, il est permis de considérer le *bitcoin* comme une unité de mesure monétaire, sous forme électronique, qui ne permet de réaliser des paiements qu'au sein d'une communauté d'acteurs qui reconnaissent la valeur de cette unité monétaire.

Au regard du droit civil, le *bitcoin* peut être considéré comme un bien meuble incorporel valorisable, utilisé comme outil spéculatif, plus précisément d'un bien meuble par détermination de la loi car il ne peut rentrer dans la catégorie des biens immeubles définie aux articles 517 à 526 du Code civil.

Dans le même temps, au regard de certaines dispositions législatives, les monnaies virtuelles ne paraissent pas pouvoir être assimilées à une marchandise ou à une matière première. La notion de « marchandise » qui figure à l'article D. 211-1 A du code monétaire et financier (CMF) recouvre

celle de « matière première », utilisée dans la directive MIF, qui est d'application maximale et que cet article transpose, ainsi que dans le règlement européen n° 1287/2006[1]. Les matières premières au sens de la directive MIF s'entendent de « *tout bien fongible pouvant être livré, en ce compris les métaux et leurs minerais et alliages, les produits agricoles et les fournitures énergétiques, telles que l'électricité* »[2], et, aux termes du règlement européen susmentionné, « *ne devrait pas englober les services ou autres éléments qui ne sont pas des biens, tels que les monnaies ou les droits immobiliers, ou qui sont totalement incorporels* ». Dès lors, la nature incorporelle des monnaies virtuelles semble exclure celles-ci du champ des marchandises[3].

La DGDDI relève qu'il serait intéressant de considérer certaines de ces monnaies virtuelles (décentralisées, convertibles dans les deux sens et spéculatives) comme un bien similaire à l'or, ce qui permettrait à la douane d'être compétente en termes de contrôle des transferts de capitaux ou de les classer sous une même appellation d'« instrument de paiement », ce qui les ferait alors toutes entrer dans le champ de contrôle de la douane. Toutefois, cette seconde option risquerait d'entraîner une confusion avec les moyens de paiement encadrés par le code monétaire et financier.

L'émission des monnaies virtuelles ne répond aujourd'hui à aucune qualification au regard de la réglementation bancaire et financière en vigueur :

- il ne s'agit pas d'instruments de paiement au sens du c) de l'article L. 133-4 du code monétaire et financier ;
- de même, la qualification de monnaie électronique ne saurait être retenue, les monnaies virtuelles ne représentant pas une créance sur l'émetteur et n'étant pas émises contre la remise de fonds, au sens de l'article L.315-1 du code monétaire et financier ;
- ces monnaies virtuelles ne rentrent pas, enfin, dans la catégorie des instruments financiers dont la liste est définie à l'article L. 211-1 du code monétaire et financier (à cet égard, il est à noter que l'Allemagne a quant à elle rangé les monnaies virtuelles parmi les instruments financiers ; il s'agit de la seule juridiction à l'avoir fait à notre connaissance).

[1] *La doctrine n'opère pas de distinction et associe matières premières et marchandises, en relevant qu'il s'agit de biens corporels.*
[2] *Article 2 du règlement n° 1287/2006 du 10 août 2006*
[3] *On soulignera, en tout état de cause, que les dérivés de matières premières ne sont pas des instruments financiers de plein droit mais sous conditions de négociation sur un marché réglementé ou un SMN, compensation ou appels de couverture.*

Ainsi, les monnaies virtuelles pourraient être apparentées, faute de réglementation actuellement plus précise :

- à une « mesure financière » – au sens de l'article D.211-1 A 1 du code monétaire et financier[1] – pouvant servir de support à des contrats financiers ;
- à un bien assimilable à un « bien divers » au sens de l'article L.550-1 du code monétaire et financier ;
- à des « indices » au sens de l'article L. 465-2-1 du code monétaire et financier, ce qui conférerait à l'AMF une compétence en termes de sanction vis-à-vis d'éventuelles manipulations de marché ;

[1] ***Article L.211-1 du code monétaire et financier*** *:*
« I. - Les instruments financiers sont les titres financiers et les contrats financiers.
II. - Les titres financiers sont :
1. Les titres de capital émis par les sociétés par actions ;
2. Les titres de créance, à l'exclusion des effets de commerce et des bons de caisse ;
3. Les parts ou actions d'organismes de placement collectif.
III. - Les contrats financiers, également dénommés " instruments financiers à terme ", sont les contrats à terme qui figurent sur une liste fixée par décret. »
Article D.211- A du code monétaire et financier *:*
« I.- Les contrats financiers mentionnés au III de l'article L. 211-1 sont :
1. Les contrats d'option, contrats à terme fermes, contrats d'échange, accords de taux futurs et tous autres contrats à terme relatifs à des instruments financiers, des devises, des taux d'intérêt, des rendements, des indices financiers ou des mesures financières qui peuvent être réglés par une livraison physique ou en espèces ;
2. Les contrats d'option, contrats à terme fermes, contrats d'échange, accords de taux futurs et tous autres contrats à terme relatifs à des marchandises qui doivent être réglés en espèces ou peuvent être réglés en espèces à la demande d'une des parties autrement qu'en cas de défaillance ou d'autre incident conduisant à la résiliation ;
3. Les contrats d'option, contrats à terme fermes, contrats d'échange et tous autres contrats à terme relatif à des marchandises qui peuvent être réglés par livraison physique, à condition qu'ils soient négociés sur un marché réglementé ou un système multilatéral de négociation ;
4. Les contrats d'options, contrats à terme fermes, contrats d'échange et tous autres contrats à terme relatifs à des marchandises qui peuvent être réglés par livraison physique, non mentionnés par ailleurs au 3, et non destinés à des fins commerciales, qui présentent les caractéristiques d'autres instruments financiers à terme, en tenant compte de ce que, notamment, ils sont compensés et réglés par l'intermédiaire d'une chambre de compensation reconnue ou font l'objet d'appels de couvertures périodiques ;
5. Les contrats à terme servant au transfert du risque de crédit ;
6. Les contrats financiers avec paiement d'un différentiel ;
7. Les contrats d'options, contrats à terme fermes, contrats d'échanges, accords de taux futurs et tous autres contrats à terme relatifs à des variables climatiques, à des tarifs de fret, à des autorisations d'émissions ou à des taux d'inflation ou d'autres statistiques économiques officielles qui doivent être réglés en espèces ou peuvent être réglés en espèces à la demande d'une des parties autrement qu'en cas de défaillance ou d'autre incident amenant la résiliation ;
8. Tout autre contrat à terme concernant des actifs, des droits, des obligations, des indices et des mesures, non mentionné par ailleurs aux 1 à 7 ci-dessus, qui présente les caractéristiques d'autres instruments financiers à terme, en tenant compte de ce que, notamment, il est négocié sur un marché réglementé ou un système multilatéral de négociation, est compensé et réglé par l'intermédiaire d'une chambre de compensation reconnue ou fait l'objet d'appels de couvertures périodiques. »

- en termes comptables, et à défaut de qualification juridique précise, les monnaies virtuelles pourraient être considérées comme un « actif physique », et non comme un actif financier, une monnaie ou de la trésorerie[1].

b) L'ACPR estime que l'activité d'intermédiation dans l'achat-vente des monnaies virtuelles contre une monnaie ayant cours légal est celle d'un intermédiaire financier qui réalise des encaissements de fonds pour le compte de tiers[2].

L'ACPR analyse cette activité comme la fourniture de services de paiement tels que définis à l'article L. 314-1 II du code monétaire et financier : « 3° *c) exécution d'opérations de virement associées à un compte de paiement* » ; « 5° *acquisition d'ordres de paiement* »[3].

Par conséquent, les entités qui exerceront cette activité à titre habituel doivent disposer du statut de prestataire de services de paiement (PSP), et être ainsi agréées et soumises au régime prudentiel des PSP et assujetties aux dispositions relatives à la lutte contre le blanchiment de capitaux et le financement du terrorisme, sous le contrôle de l'Autorité de contrôle prudentiel et de résolution. Cette solution a été retenue par le Tribunal de commerce de Créteil, dans un jugement du 6 décembre 2011, confirmé en appel[4], opposant la société MACARAJA au CIC[5]. Toutefois, cette analyse n'est pas partagée par l'ensemble des homologues européens de l'ACPR. Une interprétation de la Commission européenne pourrait dès lors s'avérer utile.

Certains Etats membres semblent réticents à utiliser le cadre européen relatif aux services et aux moyens de paiements en estimant que cela légitime l'usage des monnaies virtuelles qui ne sont pas réglementées en tant que telles.

[1] *Le fisc américain, l'IRS, considère le* bitcoin *comme un actif et non comme une devise. A ce titre, les détenteurs de* bitcoins *sont traités comme des investisseurs boursiers.*
[2] *L'activité consiste à encaisser sur un compte ouvert au nom de l'intermédiaire, les fonds correspondant à l'achat de* bitcoins*. Ce paiement est réalisé soit par virement, soit par carte de paiement. Ensuite, les fonds sont conservés en principe jusqu'à la livraison de* bitcoins *à l'acheteur. Enfin, les fonds sont remis au vendeur par virement (déduction faite des commissions perçues).*
[3] *L'ACPR a eu à traiter des* bitcoins *dans le cadre d'une demande d'agrément de la société MACARAJA ainsi que dans le cadre d'un contrôle sur place en cours auprès d'un organisme financier.*
[4] *CA Paris du 26 septembre 2013.*
[5] *Les tribunaux français ont eu indirectement à connaître des* bitcoins *dans le cadre d'une affaire de droit au compte opposant une société MACARAJA, qui aurait assuré l'achat/vente de* bitcoins*, et l'établissement de crédit CIC, dépositaire des fonds reçus par la société MACARAJA et ne se sont prononcés jusqu'à présent que dans le cadre d'un référé. L'affaire est encore en cours d'instruction pour les volets blanchiment et exercice illégal.*

5) <u>Faut-il définir les monnaies virtuelles en droit français au niveau législatif ou réglementaire ? Est-il préférable de disposer d'une norme européenne ou internationale (traité, accord) ?</u>

Avant de s'interroger sur le niveau approprié pour l'établissement d'une norme, une réflexion préalable sur l'opportunité d'une régulation des monnaies virtuelles doit être conduite. La plupart des juridictions considèrent en effet que le fait de réguler ces monnaies renforcerait la légitimité de ces instruments aux yeux du public et accroîtraient leur diffuser en créant un sentiment de sécurité, alors qu'ils présentent des risques potentiels certains. La solution privilégiée par la plupart des autorités est d'alerter sur les risques encourus et sur le caractère non régulé des transactions, de manière à ce que les personnes qui y recourent le fassent « à leurs risques et périls ». Les limites de ce raisonnement pourraient être trouvées (i) si le développement des monnaies virtuelles dans un cadre non régulé faisait courir un risque à la stabilité (mais le consensus est clair aujourd'hui sur le fait que les volumes considérés rendent cette perspective éloignée) ; (ii) s'il donne lieu à un développement de la fraude et du blanchiment : c'est aujourd'hui le risque qui est le plus souvent mis en avant pour justifier une action publique d'assujettissement à des obligations.

Dans le cas où une définition des monnaies virtuelles serait considérée comme nécessaire, une définition découlant d'une norme européenne serait appropriée, compte tenu du caractère transnational de cette technologie et de la nécessité de disposer d'une norme la plus harmonisée possible. Il pourrait être envisagé de s'appuyer sur les textes européens existants pour élaborer cette définition mais un texte ad hoc serait sans doute préférable.

Au plan international, cette approche coordonnée du traitement des monnaies virtuelles pourrait se faire au travers le Groupe d'action financier (GAFI) qui pourrait proposer des lignes directrices servant de base à l'élaboration de normes communes dans les différentes juridictions.

Dans le cas où une définition ou un assujettissement spécifique à certaines règles des monnaies virtuelles ne serait pas considérée comme opportuns, il en résulterait que ces monnaies seraient régies par le droit commun applicable à tout bien « ordinaire », déconnecté de toute référence au droit financier. Dans une telle hypothèse, le droit commun de la protection des consommateurs pourrait trouver à s'appliquer en lien avec des dispositions pénales applicables en matière d'escroquerie ou de litiges commerciaux.

A ce stade, la France a choisi une voie moyenne : alerte sur les risques, recours à des qualifications de droit commun plutôt qu'à une catégorie spécifique, clarification de l'assujettissement aux règles du secteur régulé lorsque la monnaie virtuelle rencontre la sphère régulée (soumission des plateformes d'échange avec une monnaie ayant cours légal au statut de PSP).

En conclusion, les travaux des différents groupes évoqués aux questions n° 2 et n° 3 visent à étudier l'opportunité de définir les monnaies virtuelles avec un double objectif :

- d'une part, couvrir la grande diversité de leurs caractéristiques, afin de ne pas s'exposer au risque d'arbitrage réglementaire au vu de failles dans la régulation ;
- d'autre part, définir une position française en vue de contribuer à l'élaboration de règles harmonisées acceptée par le plus grand nombre possible de juridictions, donc de préférence internationale et a minima européenne, en réponse à certains risques sur lesquels il n'existe pas d'instruments juridiques adaptés.

6) La qualification retenue pour les monnaies virtuelles entraîne des conséquences pour l'application de régimes spécifiques. Préciser notamment ce qu'il en est :

- **En matière de traitement fiscal (ISF, TVA, plus-values) :**

Concernant l'impôt de solidarité sur la fortune (ISF) :

L'article 885 E du code général des impôts (CGI) dispose que « *l'assiette de l'impôt de solidarité sur la fortune est constituée par la valeur nette, au 1er janvier de l'année, de l'ensemble des biens, droits et valeurs imposables appartenant aux personnes visées à l'article 885 A, ainsi qu'à leurs enfants mineurs lorsqu'elles ont l'administration légale des biens de ceux-ci.*

Dans le cas de concubinage notoire, l'assiette de l'impôt est constituée par la valeur nette, au 1er janvier de l'année, de l'ensemble des biens, droits et valeurs imposables appartenant à l'un et l'autre concubin et aux enfants mineurs mentionnés au premier alinéa ».

Les *bitcoins* entrent dans l'assiette de l'ISF définie par l'article 885 E précité du CGI, et cela pour leur valeur vénale, c'est-à-dire celle résultant du jeu de l'offre et de la demande, retenue au 1er janvier de l'année d'imposition.

Ainsi, et conformément à l'article 885 A du CGI, les redevables de l'ISF ayant leur domicile fiscal en France, imposables à raison de leurs biens situés en France comme hors de France[1], doivent inclure les *bitcoins* qu'ils possèdent dans leur patrimoine imposable.

Par ailleurs, il est précisé que les transmissions à titre gratuit (DMTG) de *bitcoins* sont également, en vertu des dispositions de l'article 750 ter du CGI,

[1] *Sauf pour les redevables qui n'ont pas été domiciliés en France au cours des cinq années civiles précédant celle au cours de laquelle elles ont leur domicile fiscal en France qui ne sont imposables qu'à raison de leurs seuls biens situés en France, et cela jusqu'au 31 décembre de la cinquième année suivant celle au cours de laquelle le domicile fiscal a été établi en France.*

soumis aux droits de mutation à titre gratuit (DMTG), sous réserve de l'application de conventions internationales.

Ainsi, par exemple, en l'absence de convention fiscale, la donation de *bitcoins* par un donateur résidant en France à un donataire domicilié hors de France serait soumise aux DMTG en France.

Concernant la taxe sur la valeur ajoutée (TVA) :

Le traitement de l'émission et de la circulation des *bitcoins* au regard de la TVA relève d'une problématique communautaire dès lors que la TVA est un impôt harmonisé. Un comité de la TVA - organisme consultatif prévu à l'article 398 de la directive 2006/112 CE du 28 novembre 2006 - est prévu au mois de juin 2014 afin de fixer un cadre européen au traitement TVA des *bitcoins*.

Concernant les plus-values :

En l'absence de cédule particulière à laquelle les rattacher, les produits résultant d'opérations sur les monnaies virtuelles doivent être imposés dans la catégorie des bénéfices non commerciaux (BNC) en application de l'article 92 du CGI qui prévoit l'imposition en BNC de toutes occupations, exploitation lucratives et sources de profits ne se rattachant pas à une autre catégorie de bénéfices ou de revenus.

De plus, l'achat de biens meubles corporels ou incorporels en vue de leur revente constitue un acte de commerce au sens de l'article L. 110-1 du code de commerce. Conformément aux dispositions de l'article 34 du CGI, l'achat-revente de monnaies virtuelles exercé à titre habituel et pour son propre compte constitue une activité commerciale dont les revenus sont à déclarer dans la catégorie des bénéfices industriels et commerciaux (BIC). Ce cas devrait cependant être peu fréquent en pratique.

- **En matière de lutte anti-blanchiment et de lutte contre le terrorisme.**

Les monnaies virtuelles n'étant pas considérées comme des moyens de paiement en l'état actuel du droit, elles n'entrent pas dans le champ de réglementation française relative aux moyens de paiement qui prévoit des mesures particulières à des fin de lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT).

En revanche, les obligations relatives à la lutte contre le blanchiment de capitaux et le financement du terrorisme s'appliquent aux opérations de conversion entre monnaie virtuelle et devise officielle compte tenu de la publication d'une position et d'un communiqué de presse par l'ACPR selon lesquels les entités qui exercent à titre habituel cette activité doivent disposer du statut de prestataire de services de paiement. Cet agrément les soumet aux obligations de LCB/FT, comme les autres prestataires de service visés à l'article L. 561-2 du code monétaire et financier. L'application de ces mesures est contrôlée par l'Autorité de contrôle prudentiel et de résolution.

Suite à l'avis de l'EBA de juillet 2014, la piste retenue au niveau communautaire pourrait être, plutôt que de généraliser cette interprétation, d'assujettir les plateformes aux obligations de vigilance LCB-FT via un aménagement de la directive LAB-FT actuellement en cours de révision.

Que ce soit via l'assimilation aux PSP ou via la création d'une nouvelle catégorie d'acteur couverts par la directive LCB/FT, ces plateformes de conversion pourront donc être assujetties aux obligations de vigilances de LCB/FT à l'égard des clients et des fonds qu'elles seront appelées à convertir (identification et vérification d'identité, contrôle de l'origine des fonds, soupçons éventuels, déclaration de soupçon à TRACFIN…). Elles viendraient alors s'ajouter à la liste des assujettis existante (Banques, assurances, avocats…).

Les établissements financiers qui hébergent ces plateformes (probablement des établissements de paiement) devront surveiller leurs activités et leur appliquer les obligations de vigilance auxquelles ils sont astreints à l'égard de leurs clients.

La DGDDI a pour mission de contrôler les transports physiques de capitaux à la fois sur le plan international (import ou export) entre l'Union européenne et les autres pays tiers (Règlement (CE) n°1889/2005 du 26 octobre 2005) et au niveau communautaire[1]. Suite à la révision de la législation sur les obligations déclaratives de capitaux (le décret d'application est en cours de rédaction), la DGDDI sera prochainement compétente pour contrôler les transferts physiques de capitaux supérieurs à 10 000 euros concernant les monnaies électroniques (cartes prépayées), l'or, les jetons de casino, en plus des espèces, bons et titres au porteur, chèques et chèques de voyage.

La DGDDI pourrait être compétente pour contrôler les mouvements de monnaies virtuelles adossés à des supports physiques (cartes prépayées par exemple) si les monnaies virtuelles sont assimilés à des fonds dans la mesure où la douane est compétente en matière de lutte anti-blanchiment pour contrôler les transferts de fonds aux frontières[2].

[1] *Art 464 du code des douanes :* « Les personnes physiques qui transfèrent vers un État membre de l'UE ou en provenance d'un État membre de l'UE des sommes, titres ou valeurs, sans l'intermédiaire d'un établissement de crédit, d'un établissement de monnaie électronique, d'un établissement de paiement ou d'un organisme ou service mentionné à l'article L. 518-1 doivent en faire la déclaration dans des conditions fixées par décret. Une déclaration est établie pour chaque transfert à l'exclusion des transferts dont le montant est inférieur à 10 000 € ».

[2] *Art 415 du code des douanes :* « fait de procéder ou de tenter de procéder, par exportation, importation, transfert ou compensation, à une opération financière entre la France et l'étranger portant sur des fonds que les intéressés savaient provenir, directement ou

Les autorités de supervision devront par ailleurs s'assurer que les entités sur lesquelles elles ont compétence en matière de LBC/FT[1], et qui sont exposées aux monnaies virtuelles, respectent leurs obligations préventives et déclaratives en tenant compte d'une situation de risque élevé.

- **En matière de protection et d'information des utilisateurs, les monnaies virtuelles présentent des risques significatifs :**

Le remboursement d'une monnaie virtuelle n'est pas garanti et sa convertibilité dans une monnaie ayant cours légal non plus. Par ailleurs, il n'existe pas de dispositif de protection du consommateur adapté aux monnaies virtuelles. Elles n'entrent pas dans le périmètre juridique de la directive européenne des services de paiement et n'offrent ainsi aucune garantie en cas de fraude contrairement aux moyens de paiement traditionnels.

L'AMF est compétente en matière de protection des investisseurs, qui peuvent être exposés aux monnaies virtuelles, notamment dans les cas suivants :

1. Un investisseur peut acquérir des monnaies virtuelles directement (*mining*, transaction bilatérale avec un autre investisseur, achat d'options sur internet[2]) ou indirectement, *via* une plateforme ;
2. Des fonds ou des produits financiers peuvent être exposés aux monnaies virtuelles : des CFD sont déjà proposés au public[3] ; des ETF synthétiques et produits structurés pourraient également se développer[4] ;
3. Un investisseur peut prendre une participation qui pourrait transiter par une plateforme[5] de *crowdfunding* (financement participatif) proposant d'utiliser des monnaies virtuelles ;

indirectement, d'un délit prévu par le code des douanes ou d'une infraction à la législation sur les substances ou plantes vénéneuses classées comme stupéfiants ».

[1] *Sociétés de gestion et SGP au titre des services d'investissement qu'elles fournissent et de la commercialisation des parts ou actions d'OPC, les CIF et Euroclear.*

[2] *http://fr.anyoption.com/options-Bitcoin ou http://www.optionsdigitales.com/options-binaires/les-options/Bitcoin.*

[3] *À titre d'exemple, Plus500 (http://www.plus500.com/AllInstruments/AllInstruments.aspx), agréé par la FCA, ou encore Ava Capital Markets Ltd (http://www.avatrade.fr/trading-info/range-of-markets/Bitcoin), agréé par la banque centrale d'Irlande, permettent de traiter des CFD sur Bitcoin et Litecoin au même titre que des CFD sur actions, indices, commodities ou Forex. Plus500 classe d'ailleurs ces CFD dans la catégorie Forex.*

[4] *Un premier projet d'ETF Bitcoin aurait été présenté à la SEC à l'été 2013 et serait toujours en cours d'analyse.*

[5] *Par exemple http://coinfunder.com/ ou http://www.raiseBitcoins.com/.*

4. Sont aussi concevables :
   a. des opérations d'augmentation de capital de sociétés cotées ou non, ou le paiement de dividendes en monnaies virtuelles ;
   b. des sociétés, dont les titres font l'objet d'offres au public, pourraient exposer directement ou indirectement l'investisseur aux monnaies virtuelles.

Toutefois, les services de l'AMF n'ont, à ce jour, ni reçu de plaintes d'investisseurs ayant subi des pertes liées aux monnaies virtuelles, ni observé de fonds, de sociétés de gestion, de conseillers en investissements financiers ou de produits financiers exposés ou exposant les investisseurs à de tels risques. Selon la définition qui sera retenue et la crédibilité du cadre réglementaire proposé, les risques de réputation pesant sur les détenteurs de ces monnaies virtuels pourront être limités.

7) **Avez-vous pu constater des points de convergence ou de divergence entre les régulateurs des principaux pays concernés par les monnaies virtuelles ? Par exemple, la Banque de France et l'ACPR ont indiqué que l'échange d'une devise contre des *bitcoins* constituait une activité de service de paiement : cette position est-elle partagée par les autres ? Le droit de l'Union européenne permet-il de qualifier les monnaies virtuelles ? Quelles sont les dispositions qui pourraient le cas échéant être instituées ou modifiées pour qualifier, réguler et fiscaliser les monnaies virtuelles ? Fournir une liste complète des dispositions**

Des points de convergence parmi les principaux régulateurs concernés ont pu être constatés.

Bien qu'il soit encore difficile de définir précisément et de manière uniforme les monnaies virtuelles, les principales banques centrales (Eurosystème, Système de Réserve Fédérale des Etats-Unis, Banque Populaire de Chine, Banque du Japon) estiment que les monnaies virtuelles, n'ayant pas cours légal, ne sont pas une monnaie et ne sont donc pas régulées par les banques centrales.

En matière de stabilité financière, l'ensemble des régulateurs des principaux pays concernés s'accordent sur le fait que le développement des transactions en monnaie virtuelle en l'état actuel, ne présentent pas de risques significatifs. Les données portant sur les transactions de *bitcoins* (source : *blockchain.info*) font état en juillet 2014 d'un rythme journalier d'environ 60 000 transactions à l'échelle mondiale, correspondant à 100 000 *bitcoins* échangés par jour. Les échanges se sont intensifiés en décembre 2013, pour autant, les volumes sont restés marginaux : 100 000 transactions journalières ont été conclues en fin d'année 2013 pour 350 000 *bitcoins* échangés. À titre de

comparaison les échanges journaliers en euros via les moyens de paiement conventionnels s'établissent à 295 millions EUR.

Cependant à plus court terme, les autorités de régulation considèrent que les monnaies virtuelles présentent des risques majeurs pour les utilisateurs ainsi que des risques notoires pour le blanchiment compte tenu de l'anonymat et de l'absence d'une réelle traçabilité des transactions.

Plus précisément les utilisateurs sont potentiellement exposés à de lourdes pertes compte tenu du caractère erratique du marché, qui se traduit par une volatilité exacerbée du taux de change, un risque important de manipulation de cours, ainsi qu'un risque de liquidité notoire, notamment en cas de défiance généralisée vis-à-vis des monnaies virtuelles. En outre Les utilisateurs ne sont pas protégés dans le cas d'actes frauduleux visant les plateformes d'échange de monnaies tels que le piratage informatique susceptible de suspendre les transactions, voire de vider la plateforme des avoirs en monnaies virtuelles des consommateurs.

Face à ce constat, à l'instar de la Banque de France, de nombreuses banques centrales (Allemagne, Belgique, Pays-Bas, Israël, Chine, Inde, Russie) ont manifesté publiquement leurs inquiétudes en matière de protection des utilisateurs au regard des monnaies virtuelles :

- L'Allemagne
http://www.bundesbank.de/Redaktion/EN/Interviews/2014_01_08_thiele_handelsblatt.html

- La Belgique
http://www.bitcoin.fr/post/Avertissement-Banque-nationale-de-Belgique

- Les Pays-Bas
http://www.dnb.nl/en/news/news-and-archive/nieuws-2013/dnb300672.jsp

- L'Inde
http://rbi.org.in/scripts/BS_PressReleaseDisplay.aspx?prid=30247

- Israël
http://www.boi.org.il/en/NewsAndPublications/PressReleases/Pages/19-02-2014-BitCoin.aspx

- La Suisse
http://www.finma.ch/f/finma/publikationen/faktenblaetter/documents/fb-bitcoins-f.pdf

- Les Etats-Unis
http://investor.gov/news-alerts/investor-alerts/investor-alert-bitcoin-other-virtual-currency-related-investments

La plupart des régulateurs estiment qu'une régulation est possible mais qu'il existe toutefois un risque à légitimer cet instrument à travers l'application d'un cadre réglementaire financier existant. Plusieurs régulateurs sont néanmoins partisans d'une évolution à court terme du cadre règlementaire actuel sur le volet blanchiment/financement du terrorisme par un assujettissement des plateformes de conversion à des obligations de vigilance.

Aux Etats-Unis, le service du département du Trésor américain *Financial Crimes Enforcement Network* (FINCEN) a publié des lignes directrices le 18 mars 2013 (FIN-2013-G001) indiquant qu'un opérateur qui accepte et transmet des monnaies virtuelles convertibles entre dans la qualification de « *money transmitter* » et à ce titre entre dans le champ de la législation américaine régissant les entreprises exerçant ce type d'activité. L'initiative de l'ACPR déjà décrite est proche de cette démarche.

Si l'analyse des principaux régulateurs internationaux des risques relatifs aux monnaies virtuelles est largement concordante, certaines initiatives nationales relevées au cours des derniers mois suggèrent des différences d'appréciation :

- Fin mars 2014, le fisc américain a indiqué[1] que les monnaies virtuelles seraient considérées comme des biens (*property*) ;
- En février 2014, l'autorité de contrôle prudentiel allemande (*BaFin*) a donné au Bitcoin, en tant qu'unité de compte privée, le statut d'instrument financier et exige une autorisation préalable en cas d'utilisation commerciale (*commercial use*), d'activité de *proprietary trading*, de *broking* ou de plateforme multilatérale (*multilateral trading system*)[2] ;
- L'Autorité Monétaire de Singapour a, quant à elle, publié le 13 mars 2014 une régulation des intermédiaires effectuant des transactions en monnaie virtuelle (notamment les opérateurs de plateformes d'échange en *bitcoins*, qui ne sont pas considérés comme des valeurs mobilières), afin de limiter les risques potentiels de blanchiment de capitaux et de financement du terrorisme. En découle un devoir de vérification de l'identité des contreparties lors de réalisation de transactions en *bitcoin* et de signalement, auprès du *Suspicious Transaction Reporting Office*, de toute transaction suspecte.

[1] *http://www.irs.gov/uac/Newsroom/IRS-Virtual-Currency-Guidance*
[2] *http://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2014/fa_bj_1401_bitcoins_en.html*

8) **Le droit de l'Union européenne permet-il de qualifier les monnaies virtuelles ? Quelles sont les dispositions qui pourraient le cas échéant être instituées ou modifiées pour qualifier, réguler et fiscaliser les monnaies virtuelles ? Fournir une liste complète des dispositions**

Comme évoqué supra, les monnaies virtuelles n'ont pas aujourd'hui de définition nationale, européenne ou internationale. Toutefois, certains textes européens déjà adoptés, notamment dans le domaine de la gestion (UCITS, AIFM) et des abus de marché (MAD et MAR), ou envisagés, par exemple en matière de marchés d'instruments financiers (révision de la directive MIF) ou d'indices (benchmarks), permettraient éventuellement, selon le statut juridique qui serait appliqué aux monnaies virtuelles, de donner des responsabilités de supervision et/ou de sanction aux autorités européennes et nationales compétentes.

9) **Quelles difficultés concrètes se poseraient une fois les monnaies virtuelles qualifiées ? Comment assurer le contrôle, la régulation et la fiscalisation effective des transactions ? Des mesures particulières sont-elles envisagées ?**

L'anonymat des investisseurs, passant par internet, dans certains cas la non-traçabilité des opérations, la non-réglementation ou les différences de réglementation auxquelles sont assujetties les plateformes d'échanges et les difficultés de la coopération internationale en matière d'enquêtes ou de sanctions compromettent la maîtrise des risques associés aux monnaies virtuelles. Par ailleurs, compte tenu du réseau actuellement encore limité des monnaies virtuelles, leur utilisation dans le cadre d'activités illicites ou de blanchiment et de financement du terrorisme n'offre d'intérêt que si elles peuvent être converties *in fine* en monnaie ayant cours légal. Compte tenu de ces risques les monnaies virtuelles font l'objet d'un suivi attentif des autorités (cf. les alertes précitées lancées par la Banque de France et l'Autorité de contrôle prudentiel et de résolution).

La généralisation au niveau international de l'enregistrement des transactions, des investisseurs et des monnaies virtuelles utilisées, de même que l'agrément et la supervision des fonctions remplies par les monnaies virtuelles, notamment sur les plateformes d'échanges, constitueraient des avancées importantes. L'agrément des plateformes de conversion entraîne l'application par ces dernières de vigilances en matière de LBC/FT sous le contrôle en France de l'ACPR. Cet agrément implique également la surveillance par la Banque de France de la sécurité opérationnelle de ces plateformes (article L. 141-4 du Code Monétaire et Financier), limitant le risque de fraude au moment de l'achat ou vente de monnaies virtuelles.

Pour autant, la supervision de ces entités ne permettra pas de réglementer l'utilisation des monnaies virtuelles sur internet auprès des acteurs économiques les acceptant, notamment en cas d'utilisation pour la vente de biens ou services illicites sur internet, en particulier en situation de transactions transfrontières.

Des travaux devront donc être lancées, au niveau européen, afin que cette problématique soit suivie de manière coordonnée par les différentes autorités européennes de supervision, y compris par la Commission Européenne. En tout état de cause, l'élaboration d'une norme au niveau européen reste la condition minimale pour l'application d'une mesure efficace, même s'il est possible que les acteurs délocaliseront leurs activités vers des juridictions au cadre législatif moins contraignant.

En termes de contrôle douanier, au regard de l'obligation de déclarer les montants éventuellement transportés lors du passage d'une frontière, les contrôles sur les supports de monnaies électroniques demeurent complexes sans la coopération du titulaire du support permettant de connaître les montants en jeu. Il est à noter que des cartes de débit adossées à des monnaies virtuelles apparaissent dans différents pays. À titre d'exemple, la société *Cryptex*, basée à Hong Kong, devrait lancer prochainement une carte de paiement qui serait acceptée dans 80 pays.

10) Quand une entreprise effectue une transaction en monnaie virtuelle, quelles sont ses obligations déclaratives ? Quelles inscriptions doivent figurer dans ses comptes ?

En l'état actuel de la réglementation, l'utilisation de monnaies virtuelles pour échanger, acheter ou vendre des biens n'est pas soumise à une obligation déclarative, a l'exception toutefois de l'obligation déclarative au procureur de la république, prévue au L561-1 du Code monétaire et financier et qui s'impose à toute personne ayant connaissance, dans l'exercice de ses activités de la commission d'une infraction.

À noter que les autorités de supervision s'assurent que les professionnels sur lesquels elles ont compétence en matière de LBC/FT respectent leurs obligations préventives et déclaratives (vérification de l'identité des parties et maîtrise des autres risques afférents).

En tout état de cause, les factures accompagnant les marchandises libellées en monnaies virtuelles et non en devises officielles ne seront pas acceptées pour le dédouanement. En effet, le cadre législatif est strict : aucune facture accompagnant la marchandise à destination du territoire douanier communautaire ne pourra être libellée en monnaie virtuelle tant qu'un Etat

de l'Union européenne n'aura pas reconnu une de ces monnaies comme monnaie légale.

11) L'émergence d'un mode de paiement décentralisé est-il de nature à faire diminuer les coûts de transaction ? Quelles sont les principales failles de sécurité de ces modes de paiement ? Que faudrait-il pour les sécuriser ? Les coûts de la sécurité et de la régulation sont-ils de nature à limiter les gains identifiés par ailleurs ? Une banque centrale pourrait-elle être gestionnaire ou « assureur en dernier ressort » d'un tel mode de paiement ?

Les caractéristiques actuelles des monnaies virtuelles montrent un certain nombre de limites en terme d'efficience en raison notamment des coûts qui rendent ces instruments encore peu intéressants au regard des systèmes de paiement régulés : lenteur des transactions (parfois 10 minutes d'attente avant confirmation), coût du matériel et des logiciels informatiques, absence de mécanismes de remboursement, faible acceptation par les commerçants, prélèvement de commissions lors de transaction, consommation énergétique.

La question du coût des moyens de paiement doit être également considéré au regard du niveau de sécurité offert. Les monnaies virtuelles font peser un certain nombre de risques aux commerçants qui peuvent occasionner des coûts, notamment en raison de la volatilité des cours, qui peuvent être bien plus élevés que le coût des moyens de paiement traditionnels.

En matière de paiements en ligne, les banques françaises ont mis en place, sous l'impulsion de la Banque de France, des mécanismes d'authentification non rejouables visant à sécuriser ces opérations. À ce titre, il semble inopportun de favoriser des facilités de paiement alternatives moins coûteuses mais non sécurisées. La Banque de France considère que la sécurité, qui est un élément du coût d'un moyen de paiement, ne doit pas être un facteur concurrentiel au bénéfice des moins-disant en matière de sécurité.

12) Comment la France a-t-elle organisé la réponse à l'utilisation criminelle des monnaies virtuelles, y compris en matière de blanchiment ? Une activité de « veille » est-elle organisée autour de l'émergence des monnaies virtuelles et des plateformes d'échange ? Des autorités internationales (ex : Interpol) se sont-elles saisies de ce dossier ?

Les risques en matière de stabilité financière apparaissent faibles selon les analyses convergentes des superviseurs. Ce sont davantage des risques à court terme pour la protection des consommateurs et en matière de blanchiment qui sont constatés. En matière de lutte anti-blanchiment, la qualification des plateformes de conversion entre monnaie virtuelle et devise

officielle comme organismes assujettis aux obligations de vigilances renforcées, indépendamment de l'existence ou non d'un agrément en tant que PSP, paraît nécessaire.

Comme indiqué précédemment, Tracfin suit les risques et implications en termes de blanchiment et de financement du terrorisme des monnaies virtuelles depuis 2011. Ce suivi des risques se fait à la fois par le biais d'une veille interne et externe. Tracfin a également piloté en 2011-2012 un groupe de travail sur les nouveaux moyens de paiement et a relancé une réflexion sur la thématique en décembre 2013. Enfin, depuis janvier 2013, le SCN Tracfin a créé une cellule d'analyse stratégique, notamment en charge de l'activité de veille et de détection de nouvelles menaces, afin de diffuser une information en temps réel sur des sujets identifiés (stratégie de surveillance), de répondre au besoin de synthèse et d'analyse (études ponctuelles) et d'identifier des thèmes émergents.

La DNRED, depuis plus d'un an, élabore une veille automatisée sur cette thématique à l'image de ce qui est réalisé aujourd'hui par Europol et Interpol. Toutefois, pour pousser plus loin encore la réflexion au sein de l'Union européenne, d'identifier les nouvelles monnaies virtuelles et les risques y afférents, il pourrait être envisagé de créer une entité chargée de veiller et d'analyser au quotidien les nouvelles monnaies, les nouvelles plateformes et échangeurs, leurs caractéristiques et leurs utilisateurs par le biais de matrices d'analyse de risques.

13) Le financement de l'innovation en matière de monnaies virtuelles aurait lieu essentiellement aux États-Unis et en Asie. Comment expliquer le retard pris par l'Europe et par la France en la matière ? Faut-il s'en inquiéter ? Constate-t-on une progression des investissements dans ce secteur ? Les institutions publiques françaises (ex : BPI) seraient-elles susceptibles d'engager de tels investissements ?

L'innovation en matière de monnaies virtuelles s'inscrit dans le cadre plus large des projets innovants dans les technologies financières (*crowdfunding*, nouveaux prestataires de paiement, *bitcoin*, améliorations aux infrastructures des banques et des assurances, en matière de gestion de l'information ou d'analyse des risques, etc.). Les entreprises spécialisées dans les technologies financières (*Fintech*) élaborent et proposent des services qui peuvent être concurrents ou complémentaires de l'offre existante de services financiers.

Les « *Fintech* » représentent un segment d'entreprises innovantes assez dynamiques en France. Plus particulièrement l'industrie des paiements dans laquelle les acteurs français ont une tradition établie de longue date est devenue le champ d'un foisonnement de nouveaux moyens de paiement et de nouveaux acteurs (opérateurs télécoms, de la grande distribution et

acteurs d'Internet) favorisés par l'essor des ventes en ligne et des services mobiles, dynamisée en retour par la réaction des opérateurs historiques1. Compte tenu de l'ensemble de ces évolutions la France est en pointe en matière d'innovation sur les moyens de paiement.

Ce segment de marché, comme plus généralement les entreprises spécialisées dans le développement de technologies de pointe destinées au secteur financier sont soutenues par les pouvoirs publics. En particulier, le pôle de compétitivité Finance Innovation, lancé en 2008 par Paris Europlace participe à la structuration de l'écosystème autour de l'activité pour faciliter les transferts d'information entre les acteurs et a en particulier pour objectif de :

- encourager l'émergence de projets industriels dans les différents métiers - banque, assurance, gestion, service aux institutions financières - associant les milieux académiques et les professionnels de la finance ;
- favoriser le positionnement de l'industrie financière sur les marchés innovants ;
- développer et coordonner des projets de recherche en finance et mener des actions de promotion du pôle de recherche en finance français ;
- accélérer le développement d'entreprises financières de croissance en France.

Plus généralement, de manière plus transversale, les « *Fintech* » sont soutenues par les pouvoirs publics dans le cadre de la politique de soutien au financement de l'innovation et des nouvelles technologies en France qui facilitent le financement (de manière directe via Bpifrance ou indirecte via des incitations fiscales).

Si l'innovation strictement orientée *bitcoin* apparaît plus dynamique aux États-Unis et en Asie, la France n'est pas absente de ces problématiques sur lesquelles elle a un savoir-faire reconnu. Ces innovations bénéficient notamment de l'écosystème du pôle de compétitivité Finance Innovation ainsi que du soutien générique à l'innovation.

---

[1] *Par exemple :*
- *le « paiement sans contact » s'est mis en place progressivement tout au long de 2013. La plupart des banques fournissent aux commerçants désormais des terminaux de paiement compatibles avec le NFC* (Near Field Communication).
- Paylib *est une solution de paiement en ligne lancée en septembre 2013 par BNP Paribas, la Banque postale et Société Générale, qui est proposée gratuitement aux clients des trois groupes bancaires.*
- SEPAmail *est un service de messagerie sécurisée permettant d'effectuer de façon simple et dématérialisée des échanges liés aux paiements comme la gestion des mandats des prélèvements SEPA, les règlements de factures, des paiements sur Internet et des échanges documentaires. Six grandes banques françaises (BPCE, Crédit Mutuel, BNP Paribas, Société générale et Crédit agricole) ont récemment lancé Sepamail.eu.*

ETUDE COMPARATIVE INTERNATIONALE RÉALISÉE PAR LA DIRECTION GÉNÉRALE DU TRÉSOR

Analyse comparative dans 13 pays

Contribution des services économiques des pays suivants : Allemagne, Canada, Chine, Corée, Chypre, États-Unis, Inde, Israël, Japon, Royaume-Uni, Russie, Singapour, Thaïlande

Mai 2014

I. ALLEMAGNE

Q1/- Les monnaies virtuelles ont-elles fait l'objet de débats, de travaux (rapports, auditions publiques, etc.), de prises de position publiques ou politiques ? Avez-vous identifié des réflexions en cours sur le sujet ? Des think-tanks sont-ils actifs sur le sujet ?

Suite à une série de faillites de plateformes en ligne basées sur des monnaies virtuelles (la dernière étant la plateforme japonaise *Mt.Gox*) dont la presse allemande s'est fait l'écho ces dernières années, la Bundesbank et le superviseur allemand, la BaFin, informent sur leur site internet le consommateur sur la nature des monnaies virtuelles.

Plusieurs députés se sont emparés du sujet, notamment Frank Schäffler (député FDP sous l'ancienne législature) qui a posé une question au gouvernement l'année passée sur le traitement fiscal des *bitcoins* (cf. réponse Q6). La commission des affaires économiques du Landtag de Bavière a invité en mars dernier le membre du directoire de la Bundesbank, Carl-Ludwig Thiele, sur ce sujet. Ce dernier s'est montré très rassurant face aux questions des députés bavarois en affirmant que l'utilisation des *bitcoins* est un épiphénomène et le restera tant que « *la monnaie virtuelle ne sera pas émise par une banque centrale indépendante qui garantirait la stabilité de la valeur de la monnaie* ».

Un jeune député, Jens Zimmermann (SPD), membre de la commission des Finances, a récemment animé un groupe de travail du groupe parlementaire SPD au Bundestag sur les monnaies virtuelles où il se prononce pour une régulation de cette activité avant qu'elle ne représente un réel danger.

Commerzbank, qui a pris position en mai 2013 sur le sujet[1], réclame que le superviseur de la bourse surveille également les plateformes de monnaies virtuelles, estimant que les risques de ces nouvelles monnaies ne devaient pas être sous-estimés.

Par ailleurs, C.-L. Thiele (membre du directoire de la Bundesbank) interviendra à la fin du mois de mai sur le sujet des *bitcoins* (« Monnaie virtuelle – Bitcoin, moyen de paiement ou objet de spéculation ? ») devant un parterre d'acteurs du secteur financier allemand et de responsables politiques sur invitation de la Commerzbank.

Q2/- Les autorités publiques se sont-elles montrées plutôt favorables ou circonspectes sur les monnaies virtuelles, notamment le *bitcoin* ?

Les autorités publiques allemandes se montrent plutôt circonspectes sur les monnaies virtuelles.

[1] http://zertifikate.commerzbank.de/SiteContent/1/1/2/544/11/120_waehrungsstrategie.html.

La Bundesbank, par l'intermédiaire d'un des membres de son directoire, C.-L. Thiele, a indiqué que les monnaies virtuelles ne sont actuellement qu'un phénomène de niche, mais met clairement en garde contre les risques qu'elles représentent. Il s'est prononcé dans ce sens récemment sur les *bitcoins* en particulier : « *en réalité, le* bitcoin *est un instrument hautement spéculatif en raison des fortes et rapides variations, quasiment inexplicables, qui ne présente aucune garantie. L'épargnant peut perdre à tout moment la totalité de son investissement. La confiance dans la stabilité de la valeur de la monnaie est une condition importante pour l'utiliser en tant que moyen d'échange. Il manque donc un élément important au* bitcoin *pour jouer un rôle significatif en tant que moyen de paiement. Avec environ 70 000 transactions au niveau mondial, le* bitcoin *ne représente pas plus qu'un épiphénomène. Si l'on évoque les 60 millions de virements et prélèvements qui sont opérés tous les jours en Allemagne, on peut douter du potentiel du* bitcoin *– indépendamment de la fluctuation de sa valeur – à devenir un système de paiement significatif* »[1].

La Bundesbank rappelle en outre que les monnaies virtuelles, à la différence des monnaies classiques, ne bénéficient pas de la garantie d'un État.

De son côté, le superviseur allemand, la BaFin, qui a décidé en juillet dernier d'encadrer les activités des plateformes en ligne des monnaies virtuelles (cf. Q4), met en garde épargnants et consommateurs à l'égard des monnaies virtuelles en expliquant dans sa lettre mensuelle de janvier dernier[2] que le bitcoin, par exemple, peut être perdu ou volé comme tout autre monnaie en espèces. La BaFin signale que les coûts de transaction augmenteront probablement proportionnellement au nombre de bitcoins en circulation en raison des besoins croissants en capacité informatique pour les gérer. Le superviseur rappelle en outre que les monnaies virtuelles peuvent servir à du blanchiment d'argent, ce qui peut entraîner la fermeture d'une plateforme d'échanges et « *avoir des conséquences dommageables également pour l'utilisateur honnête* ».

Q3/- Certains acteurs des monnaies virtuelles mènent-ils un travail de *lobbying* auprès des institutions publiques (administrations, Parlement, régulateurs) ? Si oui, quels sont les arguments mis en avant ? Quelles sont leurs demandes ?

Les fédérations représentant cette activité (*Bundesverband Bitcoin e.V., Bundesverband Digitale Wirtschaft*) mènent un travail de lobbying assez peu prononcé jusqu'à présent, selon un interlocuteur du Bundestag.

[1] http://www.bundesbank.de/Redaktion/DE/Standardartikel/Presse/Gastbeitraege/2014_04_11_thiele_die_bank.html

[2] http://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2014/fa_bj_1401_bitcoins.html

Q4/- Les monnaies virtuelles font-elles l'objet d'une définition légale ? Des évolutions légales ou règlementaires sont-elles envisagées ? Si oui, préciser les principales dispositions.

Le superviseur allemand, BaFin, a qualifié en juillet 2013 dans une notice d'orientation[1] les *bitcoins* d'unités de compte (*Rechnungseinheiten*). La loi sur le secteur bancaire (*Kreditwesengesetz*, §1 Abs.11 Satz 1 n°7, KWG) classifie les unités de comptes dans la catégorie des instruments financiers (*Finanzinstrumente*), de même que les devises. Cette définition officialisée par la BaFin (il s'agit désormais d'un usage établi par l'administration, *Verwaltungspraxis*) permet au superviseur d'appliquer aux *bitcoins* les règles qu'il applique à tout instrument financier et de décider si l'activité contrôlée doit être exercée avec un agrément bancaire.

Q5/- Les régulateurs sont-ils intervenus pour encadrer l'utilisation des monnaies virtuelles ? Les plateformes dédiées à l'utilisation de ces monnaies sont-elles soumises à des obligations spécifiques ?

La BaFin, a publié, dans sa lettre mensuelle de janvier dernier, une analyse des *bitcoins* dans laquelle elle explique les cas dans lesquels l'obtention d'un agrément est obligatoire, à savoir lorsque l'échange de *bitcoins* se fait dans le cadre d'un service rémunéré (et non d'un simple achat, vente ou prospection).

Q6/- Les administrations fiscales ont-elles pris position sur la nature des monnaies virtuelles et, partant, sur les conséquences fiscales qui y sont attachées ?

Le ministère fédéral des Finances a précisé le statut fiscal des *bitcoins* en août dernier dans une réponse à une question parlementaire.

S'agissant de l'impôt sur le revenu : le BMF a indiqué le 7 août 2013 que les revenus dégagés à l'occasion de la revente de *bitcoins* sont taxables en application de l'article 23 (1) point 2 de l'EStG (loi d'imposition des revenus) au titre des plus-values privées (*Private Veräusserungsgeschäfte*).

L'article 23 de l'EStG prévoit que sont imposables au titre des plus-values privées les plus-values dégagées à l'occasion de la cession de biens immobiliers ou assimilés dans le délai de dix ans et les plus-values dégagées à l'occasion de la cession d'autres biens (ou marchandises, « *andere Wirtschaftsgüter* ») dans le délai de moins d'un an. Cette catégorie comprend notamment les bijoux, l'or, les tableaux, les pièces de collection...

[1] http://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Merkblatt/mb_111220_finanzinstrumente.html

Par ailleurs, le texte indique que si le revenu net ainsi dégagé est inférieur à 600 euros sur une période de moins d'un an, le revenu est exonéré d'impôt sur le revenu.

Les plus-values dégagées sont à déclarer en même temps que l'ensemble des revenus de l'année.

Le BMF ne s'est, en revanche, pas prononcé sur le traitement pratique des plus-values dégagées à l'occasion d'opérations successives d'achat et revente de *bitcoins* dans le délai d'un an. La réponse indique seulement que le sujet sera soumis aux plus hauts responsables des administrations fiscales allemandes à l'occasion d'une de leurs prochaines réunions. Les articles parus dans la presse indiquent que la solution qui s'impose est l'application de la méthode Fifo (First-in-first-out).

S'agissant de la TVA : le BMF s'est prononcé à deux reprises, les 7 août et 27 septembre 2013 pour clarifier l'application de l'exonération prévue pour les moyens de paiements légaux (« *gesetzliche Zahlungsmitteln* ») au § 4 Nr 8b de l'UStG (loi sur la TVA).

Dans la première réponse, le BMF estime que le *bitcoin* - ne rentrant pas dans la définition des moyens de paiements légaux - ne peut bénéficier d'une exonération au titre du paragraphe de l'UStG précité. La seconde réponse indique, qu'en revanche, le 8c du § 4 de l'UStG pourrait servir de base légale pour une telle exonération.

Q7/- Les autorités publiques ont-elles entrepris des actions d'information ou de prévention vis-à-vis des épargnants ou des consommateurs ?

La Bundesbank et la BaFin informent depuis l'année passée sur leur site internet ou lors de conférences sur les risques que représentent les monnaies virtuelles, comme mentionné dans la réponse à la question 2.

Q8/- Constate-t-on une progression des investissements (publics ou privés) en matière de monnaies virtuelles ?

Le superviseur allemand a constaté une utilisation plus répandue du *bitcoin* à partir de 2011, qui s'est traduite pour la BaFin par une montée en puissance du nombre de questions qui lui sont adressées pour exercer une activité sur la base de la monnaie virtuelle. Actuellement, le superviseur reçoit en moyenne une question par jour sur ce sujet, notamment de personnes qui souhaitent installer un distributeur automatique. Jusqu'à présent, la BaFin n'a pas délivré d'autorisation à cet effet, mais ne l'exclut pas à court ou moyen terme dans le cas où le demandeur est déjà détenteur d'un agrément. Le volume des transactions en *bitcoin* en Allemagne n'est pas connu, ni la BaFin, ni le BMF ne disposant pas de données fiables.

II. CANADA

Q1/- Les monnaies virtuelles ont-elles fait l'objet de débats, de travaux (rapports, auditions publiques, etc.), de prises de position publiques ou politiques ? Avez-vous identifié des réflexions en cours sur le sujet ? Des think-tanks sont-ils actifs sur le sujet ?

Peu de réflexions publiques ont été identifiées, hormis quelques publications relativement confidentielles. Toutefois, le Parlement du Canada a entrepris très récemment une série de consultations afin d'étudier l'utilisation de la monnaie numérique. Plus précisément, c'est le Comité sénatorial permanent des banques et du commerce qui a cherché à avoir une meilleure compréhension du sujet, ce qui englobe les risques, les menaces et les avantages liés à ces modes d'échange par voie électronique.

Six séances publiques ont été organisées et ont permis de recueillir des informations et analyses de la part des principaux acteurs du secteur :

Le 26 mars 2014, les représentants du ministère des Finances (Division du secteur financier).

Le 27 mars 2014, des représentants du monde universitaire, autour des notions de monnaie et de monnaie numérique en général (M. Warren Weber, économiste et historien de l'économie, États-Unis, et M. Joshua S. Gans, professeur-coordonnateur de gestion stratégique à la Rotman School of Management de l'Université de Toronto et titulaire de la chaire Jeffrey C. Skoll en innovation technique et en entrepreneuriat de la Rotman School).

Le 2 avril 2014, les représentants de la Banque du Canada (Gestion financière et des Opérations bancaires).

Le 3 avril 2014, un représentant du monde scientifique (M. Jeremy Clark, professeur adjoint à l'Institut d'ingénierie des systèmes d'information de l'Université Concordia, spécialisé en cryptographie appliquée, en monnaie numérique et en sécurité dans les télécommunications en réseau), puis un économiste (M. David Descôteaux, chercheur associé à l'Institut économique de Montréal).

Le 9 avril 2014, des représentants des acteurs économiques impliqués dans les crypto monnaies (M. Kyle Kemper et Mme Victoria van Eyk, Bitcoin Strategy Group sur les guichets automatiques Bitcoin; M. Joseph David, CAVirtEx, sur le rôle des plateformes d'échanges de bitcoins, M. Haseeb Awan, BitAccess, fabricant de guichet automatique).

Le 10 avril 2014, des représentants du secteur bancaire (Association des banquiers canadiens, et Banque Royale du Canada, divisions Cartes internationales et produits de paiement canadiens, et Paiements émergents).

Q2/- Les autorités publiques se sont-elles montrées plutôt favorables ou circonspectes sur les monnaies virtuelles, notamment le *bitcoin* ?

D'une façon générale, les autorités publiques font preuve d'une certaine bienveillante neutralité vis-à-vis des monnaies virtuelles, reconnaissant l'ampleur de l'innovation technologique et les gains qu'elles peuvent apporter à l'économie canadienne. Ces autorités s'accordent également sur l'absence d'un besoin d'encadrement de ces activités par les pouvoirs publics, les seules responsabilités du gouvernement étant une surveillance globale du système et une information des consommateurs.

Ainsi, le ministère des finances reconnait que « *les monnaies virtuelles constituent… une innovation susceptible de procurer certains avantages aux consommateurs et aux marchands* ». Plus généralement, le ministère relève trois perspectives sur cette monnaie. « À titre de monnaie, on est sceptique sur sa viabilité à long terme. C'est particulièrement à cause de sa volatilité et parce que son utilisation n'est pas encore généralisée. À titre de marchandise, il suscite encore de l'intérêt, mais aussi de grandes craintes de la part des investisseurs. … à titre d'innovation au chapitre des paiements, le *bitcoin* nous permet de tirer des leçons intéressantes et nous croyons qu'il y a des possibilités, ce que nous suivrons avec intérêt ». Selon lui, le Gouvernement n'a pas à donner d'approbation sur tel ou tel système de paiement. En outre, les montants actuellement en jeu sont trop faibles pour constituer un véritable enjeu, et seuls les risques de blanchiment les préoccupent.

Enfin, devant le Sénat, le ministère des finances a toutefois souligné les aspects novateurs de ces monnaies et milité pour leur promotion afin de créer une économie plus concurrentielle, allant jusqu'à déclarer aux parlementaires « que les avantages sont suffisamment nombreux pour vous dire qu'il ne faudrait pas automatiquement intervenir et réglementer cette monnaie ».

De la même façon, si la Banque du Canada reconnait ne pas être en mesure de prévoir l'orientation que prendront les nouvelles monnaies à l'avenir, elle assure continuer à surveiller attentivement leur évolution et à en évaluer les conséquences.

Pour la Banque, la question de savoir comment tirer parti de ces nouvelles monnaies tout en protégeant les consommateurs.

Mais la Banque reconnait même que « une fois que le mouvement du *bitcoin* a pris de l'ampleur, ce sont surtout les spéculateurs qui s'y sont intéressés. Il n'y a rien de mal à spéculer, et je ne crois pas que le gouvernement ait un rôle à jouer pour protéger quiconque se livre ouvertement à la spéculation ».

Enfin, concernant les aux risques économiques et systémiques, la Banque admet que le volume des transactions est beaucoup trop petit pour

que s'en inquiéter, même si les risques sont susceptibles de s'intensifier à l'avenir.

Enfin, les premières réactions des parlementaires sont également plutôt favorables. Concernant une éventuelle réglementation, certains reconnaissent que « *même si 80 % des détenteurs sont des spéculateurs, ils ont le droit de spéculer. Pourquoi faudrait-il s'en soucier ? C'est un marché pour acheteurs avertis. Les gens savent que c'est une monnaie hautement instable. Peut-être le gouvernement n'a-t-il aucun rôle à jouer, à part dire aux gens: "Faites attention et prenez vos précautions"* ». Les sénateurs reconnaissent également que « *le gouvernement ne réglemente pas d'autres commodités comme l'or et l'argent. Il y a une tonne d'autres commodités et le gouvernement n'a pas de rôle à jouer pour nous assurer que les gens ne perdront pas d'argent. Pourquoi ne pas laisser le marché dicter la suite des choses ? Oui, il y a un risque assez élevé, comme dans le cas de bien des commodités. Pourquoi s'impliquer autrement ?* ».

Q3/- Certains acteurs des monnaies virtuelles mènent-ils un travail de lobbying auprès des institutions publiques (administrations, Parlement, régulateurs) ? Si oui, quels sont les arguments mis en avant ? Quelles sont leurs demandes ?

Aucun acteur ne représente le système *Bitcoin* en lui-même. En revanche, les acteurs économiques externes qui ont suivi et participé à son développement tentent visiblement un premier travail de lobbying, dans le sens d'une plus forte réglementation.

C'est le cas des représentants des sociétés auditionnés au Sénat, tel Joseph David, président-directeur général, Canadian Virtual Exchange (*CAVirtEx*), qui « recommande que le gouvernement réglemente notre secteur comme il le fait pour les transactions en devise étrangère ». De même, Haseeb Awan, cofondateur, *BitAccess*, sous couvert des « possibilités d'évasion fiscale, de financement du terrorisme et d'autres activités illégales et frauduleuses », estime que « des lois peuvent certainement s'appliquer dans de telles situations ». Il affirme même qu' « actuellement, partout au Canada et dans le monde, on peut démarrer une entreprise d'échanges virtuels, comme celle de *CAVirtEx*, en faisant l'objet de moins de surveillance publique que si l'on ouvrait un kiosque de hot dogs. Autrement dit, il n'y a pas de réglementation, pas d'obstacles à l'entrée et pas de surveillance publique de l'accès au marché des échanges. Ce manque de surveillance a créé un environnement réglementaire où les jeunes entrepreneurs envisagent plus facilement la fraude que la possibilité de bâtir une entreprise solide et durable ».

Toutefois, ce travail de lobbying s'apparente davantage à une tentative de fermer le marché aux nouveaux entrants, sous couvert d'une démarche vertueuse. Certains parlementaires n'ont d'ailleurs pas manqué de dénoncer l'incohérence ou les doutes que soulevaient une telle démarche.

Ainsi, pour l'un d'eux, d'une part on s'éloignerait ainsi de la raison d'être initiale du *bitcoin* ou des autres formes de monnaie, fondées sur une approche libertaire, un marché libre, sans participation ni supervision du gouvernement ; d'autre part, la mise en œuvre d'une réglementation comme celle d'une banque ou celle des devises étrangères entrainerait de tels couts , qu'ils seraient « acculés à la faillite en moins d'une semaine ». Pour un autre sénateur, « tous ces éléments que vous souhaitez ajouter occasionneront des frais et réduiront l'efficacité du *bitcoin*, parce que les consommateurs devront en payer les coûts au bout du compte ».

Par ailleurs, le ministère des finances reconnaît avoir des discussions fréquentes avec les acteurs économiques, mais estime qu'il ne s'agit pas de véritable lobbying mais plutôt de séances d'information, vis-à-vis d'une technologie qui évolue très vite.

Sans être des acteurs des monnaies virtuelles, les banques engagent également un travail de lobbying. Sans surprise, elles militent pour une réglementation maximale de ce « système parallèle », rappelant au passage qu'elles n'ont « *approuvé aucune forme de monnaie numérique* ».

Les auditions au Sénat ont permis de souligner que l'adoption de crypto monnaies permettait de s'affranchir des couts bancaires, très élevés notamment lors de transferts internationaux, ce qui avait déjà soulevé l'attention des parlementaires. Dans ces conditions, le discours officiel des banques canadiennes est loin d'avoir convaincu les parlementaires. Pour l'un d'entre eux, « *cela crée l'impression que c'est la concurrence, que vous défendez votre territoire et que, par conséquent, vous allez vous compromettre et veiller à vous donner un avantage par rapport à tout concurrent* ».

De même, alors que les banques militent pour une réglementation des crypto monnaies calquée sur celle des banques, un Sénateur relève que « *C'est une option et nous devons envisager cela, mais vous savez qu'il existe une autre option. Revenu Canada, à l'instar de l'IRS, a adopté la position selon laquelle il s'agit d'une marchandise, un peu comme l'or ou l'argent, et il n'y a pas de garanties pour les négociateurs de marchandises* ».

Q4/- Les monnaies virtuelles font-elles l'objet d'une définition légale ? Des évolutions légales ou règlementaires sont-elles envisagées ? Si oui, préciser les principales dispositions.

Les monnaies virtuelles ne font l'objet d'aucune définition légale. La Loi sur la monnaie stipule que l'unité monétaire du Canada est le dollar. Les dispositions de cette loi régissent le cours légal et la monnaie d'usage et définissent la forme que prennent les pièces et les billets. Viennent ensuite la Loi sur la Monnaie royale du Canada, pour les pièces, et la Loi sur la Banque du Canada, pour les billets. Aucune de ces lois ne s'applique à l'utilisation des monnaies virtuelles au Canada, et ni une ni l'autre n'interdit d'avoir recours à ces monnaies.

Les séances de consultation organisées par le Parlement du Canada avaient pour objet, notamment, d'établir si des évolutions légales étaient nécessaires. Il est trop tôt pour anticiper ce que sera la réaction du gouvernement, mais la teneur des débats écarte pour l'instant l'idée de toute évolution juridique à court terme.

Enfin, notons que le Plan d'action 2014-2015 (budget), actuellement en discussion au Parlement, cite pour la première fois le concept de monnaies virtuelles. Il ne s'agit toutefois pas de leur donner une définition légale, mais uniquement de les intégrer dans la lutte contre le blanchiment.

Q5/- Les régulateurs sont-ils intervenus pour encadrer l'utilisation des monnaies virtuelles ? Les plateformes dédiées à l'utilisation de ces monnaies sont-elles soumises à des obligations spécifiques ?

Aucune intervention des régulateurs n'encadre l'utilisation des monnaies virtuelles, et les plateformes dédiées ne sont soumises à aucune obligation spécifique. Concernant les banques, le Bureau du surintendant des institutions financières (BSIF) n'a publié aucune consigne sur les opérations en monnaie virtuelle et ne règlemente ni n'interdit l'utilisation de cette forme de monnaie.

À l'issue du plan d'action évoqué supra, des instructions (règlements) seront éventuellement adoptés, mais là-encore, uniquement dans le cadre du blanchiment.

Q6/- Les administrations fiscales ont-elles pris position sur la nature des monnaies virtuelles et, partant, sur les conséquences fiscales qui y sont attachées ?

En ce qui concerne la fiscalité, l'Agence du revenu du Canada met des renseignements à la disposition du public pour l'informer du traitement réservé aux monnaies virtuelles aux termes de la Loi de l'impôt sur le revenu. L'utilisation de ce type de monnaie pour l'achat de biens et de services est perçue comme du troc et elle est, à ce titre, imposable.

Ainsi, d'après un document d'information de l'Agence du revenu du Canada du 5 novembre 2013, les règles en matière de troc s'appliquent lorsqu'une monnaie virtuelle est employée pour payer un bien ou un service. Par conséquent, la juste valeur marchande des biens et des services achetés doit être ajoutée au revenu du vendeur aux fins de l'impôt. Si aucun bien ou service n'est acheté, mais qu'une monnaie virtuelle est vendue, tous gains ou pertes sont assujettis à l'impôt sur les gains en capital.

Q7/- Les autorités publiques ont-elles entrepris des actions d'information ou de prévention vis-à-vis des épargnants ou des consommateurs ?

D'une façon générale, les autorités publiques sont encore prudentes vis-à-vis du phénomène et n'ont pas encore entrepris d'action d'information à grande échelle. Seule l'Agence de la consommation en matière financière du Canada propose sur son site web des informations ainsi que des mises en garde relatives aux monnaies virtuelles. Par ailleurs, certains organismes de réglementation des valeurs mobilières provinciaux commencent à examiner ces questions. Au Québec, l'Autorité des marchés financiers a émis une mise en garde en février au sujet des *bitcoins*. La mise en garde fait état des risques de fraude, et rappelle que les monnaies virtuelles ne sont pas couvertes par le fonds d'indemnisation des services financiers de la province ou par son fonds d'assurance-dépôts.

À l'inverse, les banques ont déjà engagé des actions d'information, invitant leurs clients à la plus grande prudence vis-à-vis des crypto-monnaies.

Q8/- Constate-t-on une progression des investissements (publics ou privés) en matière de monnaies virtuelles ?

Par définition, les monnaies virtuelles sont sans frontières et sont échangées en ligne. Lorsque l'on examine une transaction donnée, il n'est pas possible de connaître le pays où la transaction a été effectuée, ni la nationalité des parties. Par conséquent, il est difficile d'avoir une idée précise du montant de devises virtuelles échangées au Canada.

L'Association canadienne des paiements a dû extrapoler des données à partir de la part canadienne du marché mondial des paiements et estime qu'en moyenne, entre 1 000 et 2 000 opérations en *bitcoins* sont effectuées par jour. Le volume d'opérations réalisées en *bitcoins* au Canada ne représente que 1 % du total des opérations au pays.

Il existe environ 100 bourses à l'échelle mondiale, dont près de 10 au Canada. Le premier guichet automatique de *bitcoin* au monde a été inauguré à Vancouver en novembre 2013 (ce guichet a enregistré des transactions d'environ 1 million de dollars durant son premier mois de service). Depuis, d'autres villes canadiennes ont emboîté le pas. À l'échelle mondiale, environ 1 500 marchands sont prêts à faire des transactions en *bitcoins*, dont près de 200 au Canada. Cette monnaie est surtout utilisée pour le jeu en ligne, mais elle est populaire auprès des détaillants en ligne, en particulier chez les détaillants de secteur de la technologie.

Dans tous les cas, si des données précises sont difficiles à établir, la tendance à un accroissement dans l'usage des monnaies virtuelles est clairement avérée. Pour beaucoup d'acteurs, à défaut de la monnaie *bitcoin*

proprement dite, pour laquelle les perspectives sont totalement incertaines, le système de paiement *Bitcoin* est là pour rester. Pour certains, *Bitcoin* peut être vu comme une technologie perturbatrice dans le système de paiements, mais il semble avoir réglé un des grands défis qui s'offrent à la monnaie numérique décentralisée, soit l'authentification entre les parties à l'opération sans l'intervention d'un tiers de confiance. Ces produits, bien que perturbateurs, pourraient très bien se répandre organiquement dans l'ensemble du système de paiements.

III. CHINE

Q1/- Les monnaies virtuelles ont-elles fait l'objet de débats, de travaux (rapports, auditions publiques, etc.), de prises de position publiques ou politiques ? Avez-vous identifié des réflexions en cours sur le sujet ? Des think-tanks sont-ils actifs sur le sujet ?

Les monnaies virtuelles et le *bitcoin* ont fait l'objet de publications par des chercheurs et des professionnels. D'une manière générale, ces études concluent au faible potentiel de ces dispositifs en Chine.

La presse chinoise a fait état de l'arrestation par la police chinoise en décembre 2013 de trois individus suspectés d'être les opérateurs de la plateforme *Bitcoin GL*. Enregistrée à Hong Kong, mais vraisemblablement gérée depuis la Chine continentale, cette plateforme avait soudainement fermé le 26 octobre 2013. Les utilisateurs du système avaient subi une perte estimée à 25 millions CNY (4,1 millions USD).

Q2/- Les autorités publiques se sont-elles montrées plutôt favorables ou circonspectes sur les monnaies virtuelles, notamment le *bitcoin* ?

Les autorités publiques se montrent plutôt conciliantes à l'égard de l'utilisation des monnaies virtuelles dans les jeux internet. En revanche, leur attitude à l'égard du *bitcoin* est empreinte de beaucoup plus de prudence.

Q3/- Certains acteurs des monnaies virtuelles mènent-ils un travail de lobbying auprès des institutions publiques (administrations, Parlement, régulateurs) ? Si oui, quels sont les arguments mis en avant ? Quelles sont leurs demandes ?

Aucun travail de lobbying n'est identifié.

Q4/- Les monnaies virtuelles font-elles l'objet d'une définition légale ? Des évolutions légales ou règlementaires sont-elles envisagées ? Si oui, préciser les principales dispositions.

Dès juin 2009, une circulaire commune du ministère de la culture et du ministère du commerce a précisé les conditions d'utilisation de la monnaie virtuelle dans les jeux en ligne. La circulaire définit la monnaie virtuelle dans les jeux en ligne comme « un instrument virtuel d'échange émis par les opérateurs de jeux en ligne, achetés par les utilisateurs des jeux en utilisant une monnaie ayant cours légal, stocké en dehors du programme du jeu, enregistré sur un serveur, représentatif d'un certain nombre d'unités ».

Par ailleurs, la Banque centrale chinoise (*People's Bank of China – PBoC*) a publié le 5 décembre 2013 une circulaire sur le *bitcoin* rédigée conjointement avec quatre autres institutions (*Ministry of Industry and Information Technology*, *China Banking Regulatory Commission*, *China Securities Regulatory Commission*, *China Insurance Regulatory Commission*). Le *bitcoin* y est qualifié de marchandise virtuelle et non de monnaie virtuelle. Le gouverneur de la PBoC, ZHOU Xiaochuan, a comparé le *bitcoin* à des timbres échangés par les philatélistes.

Q5/- Les régulateurs sont-ils intervenus pour encadrer l'utilisation des monnaies virtuelles ? Les plateformes dédiées à l'utilisation de ces monnaies sont-elles soumises à des obligations spécifiques ?

La circulaire de juin 2009 établit l'obligation d'une demande préalable au ministère de la culture pour émettre une monnaie virtuelle. Elle distingue l'activité d'émetteur de celle de plateforme d'échange en interdisant le cumul de ces deux activités au sein d'une même entreprise. Les monnaies virtuelles ne peuvent être utilisées que dans les jeux internet.

La circulaire du 5 décembre 2013 interdit aux institutions financières tout usage du *bitcoin* et notamment : l'échange de *bitcoins* contre des CNY ou des devises étrangères, les opérations de paiement en *bitcoin*, le développement de produits financiers en *bitcoins*, ou encore l'utilisation du *bitcoin* comme unité de compte. La circulaire justifie ces interdictions par les risques inhérents au *bitcoin* : spéculation et volatilité, utilisation à des fins de blanchiment, utilisation pour des transactions illégales, risque opérationnel des plateformes. L'utilisation de *bitcoins* reste toutefois autorisée dans le cadre de la loi sur les télécommunications et la circulaire précise que les détenteurs de *bitcoins* sont libres d'échanger cette « marchandise virtuelle » entre eux. Les plateformes d'échange de *bitcoins* doivent s'enregistrer auprès de l'autorité de contrôle des télécommunications. Ces plateformes ont également pour obligation de recueillir des pièces justifiant de l'identité des utilisateurs. Enfin, il leur est demandé de mettre en place un dispositif de détection des opérations suspectes et de coopérer avec le Bureau chargé de la lutte anti-blanchiment au sein de la PBoC. La circulaire publiée le 5 décembre ne visait pas expressément les fournisseurs de services de paiement sur internet. Mais la presse chinoise a fait état d'interventions gouvernementales auprès de ces fournisseurs pour qu'ils cessent de traiter des transactions d'échange de *bitcoins*.

Q6/- Les administrations fiscales ont-elles pris position sur la nature des monnaies virtuelles et, partant, sur les conséquences fiscales qui y sont attachées ?

En 2008, l'administration fiscale (*State Administration of Taxation – SAT*) a publié une réglementation qui précise que les gains tirés de

transactions sur des monnaies virtuelles sont imposables au titre de l'impôt sur le revenu. Les monnaies virtuelles sur internet peuvent en effet être vendues entre joueurs.

Q7/- Les autorités publiques ont-elles entrepris des actions d'information ou de prévention vis-à-vis des épargnants ou des consommateurs ?

La circulaire du 5 décembre 2013 insiste sur la nécessité de renforcer l'information du public sur le risque lié à l'investissement en *bitcoins*. La PboC a adressé plusieurs mises en garde au public, en insistant sur la volatilité de la valeur du *bitcoin*.

Q8/- Constate-t-on une progression des investissements (publics ou privés) en matière de monnaies virtuelles ?

Il n'existe pas d'instrument de mesure de progression des investissements.

IV. CHYPRE

Q1/- Les monnaies virtuelles ont-elles fait l'objet de débats, de travaux (rapports, auditions publiques, etc.), de prises de position publiques ou politiques ? Avez-vous identifié des réflexions en cours sur le sujet ? Des think-tanks sont-ils actifs sur le sujet ?

Les monnaies virtuelles ont fait l'objet de débats, malgré tout limités, dernier en date, celui au sein de la commission du commerce du Parlement chypriote, en présence de différentes institutions et acteurs économiques (Banque Centrale de Chypre, Autorité des marchés, etc.) invités à présenter leurs analyses et positions sur le sujet. Si ces débats dans l'ensemble, ont permis de lancer la réflexion et mis en exergue les réserves de l'ensemble des participants à l'égard de l'utilisation des monnaies virtuelles, il n'en demeure pas moins qu'aucune décision n'a été prise à ce stade quant au traitement qui doit être réservé aux monnaies virtuelles à Chypre.

L'intérêt d'introduire l'utilisation des monnaies virtuelles a été au cœur de l'actualité journalistique durant le 1e trimestre 2014, au moment où battait son plein une importante campagne de presse lancée par un développeur de plateformes venant de s'installer à Chypre (cf. ci-après). Depuis, le sujet est tombé en désuétude et les débats se sont estompés, voire arrêtés.

À noter qu'il n'y a pas de think-tanks actifs sur le sujet.

Q2/- Les autorités publiques se sont-elles montrées plutôt favorables ou circonspectes sur les monnaies virtuelles, notamment le *bitcoin* ?

Attitude circonspecte des autorités publiques. La Banque Centrale de Chypre ainsi que le Ministère des Finances se montrent très réservés à l'égard de l'utilisation des monnaies virtuelles.

Q3/- Certains acteurs des monnaies virtuelles mènent-ils un travail de lobbying auprès des institutions publiques (administrations, Parlement, régulateurs) ? Si oui, quels sont les arguments mis en avant ? Quelles sont leurs demandes ?

Une grande campagne publicitaire a eu lieu durant le 1e trimestre 2014 par la société *Neo & Bee – LMB Subsidiaries Limited*, important développeur de support électronique de monnaies virtuelles créée fin 2013 et ayant son siège social à Chypre. À travers cette campagne de promotion de l'utilisation du *bitcoin* à Chypre (principalement à travers l'instauration d'un portefeuille électronique pour l'achat de biens et services auprès de commerçants formant un réseau), *Neo & Bee* a surtout souhaité sensibiliser la presse (qui a favorablement accueilli le concept) à travers l'organisation de

conférence de presse, le sponsoring d'évènements sociaux, l'organisation de déjeuners de travail avec les rédactions économiques de la presse chypriote etc.

La Banque Centrale de Chypre, sollicitée par *Neo & Bee*, a toujours refusé d'établir des contacts avec l'entreprise.

En mars 2014, alors que le lancement des activités de *Neo & Bee* était attendu, la presse a annoncé la fuite de Chypre du créateur de l'entreprise et DG, laissant derrière lui des dettes (loyers, dépenses publicitaires, salariés non payés etc.). Un mandat d'arrêt international a été lancé à son encontre.

Q4/- Les monnaies virtuelles font-elles l'objet d'une définition légale ? Des évolutions légales ou règlementaires sont-elles envisagées ? Si oui, préciser les principales dispositions.

Pas de définition légale à ce stade. Les autorités souhaitent mettre en place les dispositions nécessaires mais en l'absence d'expérience et de savoir-faire au niveau national, les dispositifs mis en place par les autres états membres de l'Union Européenne constitueraient des sources d'inspiration et d'expertise à mettre à profit localement. La Banque Centrale de Chypre est demandeuse d'expertise en la matière.

Q5/- Les régulateurs sont-ils intervenus pour encadrer l'utilisation des monnaies virtuelles ? Les plateformes dédiées à l'utilisation de ces monnaies sont-elles soumises à des obligations spécifiques

Pas d'intervention pour encadrer l'utilisation des monnaies virtuelles. Pas d'obligations spécifiques pour les plateformes.

Q6/- Les administrations fiscales ont-elles pris position sur la nature des monnaies virtuelles et, partant, sur les conséquences fiscales qui y sont attachées ?

Sans objet.

Q7/- Les autorités publiques ont-elles entrepris des actions d'information ou de prévention vis-à-vis des épargnants ou des consommateurs ?

La Banque Centrale de Chypre, le Ministère des Finances et le Ministère de l'Énergie de l'Industrie, du Commerce et du Tourisme ont publié sur leurs sites internet respectifs, une annonce conjointe adressée aux consommateurs alertant des risques et dangers sous-jacents (y compris le blanchiment d'argent) à l'utilisation des monnaies virtuelles, indiquant que

celles-ci ne constituent ni de la monnaie en circulation, ni un moyen économique et financier.

L'annonce indique que la monnaie virtuelle est un type de monnaie numérique non régulée qui n'est pas émise par la Banque Centrale.

Les autorités appellent les consommateurs à examiner tous les paramètres relatifs à l'usage des monnaies virtuelles afin d'appréhender les risques sous-jacents.

Q8/- Constate-t-on une progression des investissements (publics ou privés) en matière de monnaies virtuelles ?

L'Université de Nicosie (établissement d'enseignement supérieur privé) est active en matière de monnaies virtuelles à travers deux types d'actions :

-elle a officiellement lancé en décembre 2013, l'acceptation du paiement des frais de scolarité en *bitcoin*, en premier lieu pour les étudiants étrangers (notamment du continent africain) qui suivent les cours à distance. Sur son site internet ((http://www.unic.ac.cy/digitalcurrency) l'Université se félicite d'être le premier établissement universitaire au monde (!) à pouvoir effectuer des transactions en monnaie virtuelle ;

-elle propose un Master nommé *Msc in digital currencies* http://digitalcurrency.unic.ac.cy/about-the-program/degree-overview, qui ne semble pas attirer l'intérêt de grand nombre d'étudiants.

V. CORÉE DU SUD

Q1/- Les monnaies virtuelles ont-elles fait l'objet de débats, de travaux (rapports, auditions publiques, etc.), de prises de position publiques ou politiques ? Avez-vous identifié des réflexions en cours sur le sujet ? Des think-tanks sont-ils actifs sur le sujet ?

La BOK (*The Bank of Korea*) a publié un rapport d'étude sur le *bitcoin* en décembre 2013. Depuis, aucun autre document des autorités compétentes coréennes sur cette monnaie virtuelle n'a été publié. La presse coréanophone continue à évoquer le sujet mais la perception du public de la notion du *bitcoin* reste relativement faible. Le marché domestique du *bitcoin* est très peu développé en Corée.

Le *Korea Institute of Finance* a publié un article court sur le sujet et prépare un rapport sur le *bitcoin* et les monnaies virtuelles en s'intéressant aux aspects techniques, légaux et financiers. Ce rapport devrait recommander une supervision attentive afin de prévenir toute activité illégale et de protéger les intérêts des consommateurs. Il devrait également souligner les difficultés du *bitcoin* liées au fait qu'il ne peut pas y avoir un cours légal et qu'il est difficile d'en faire une monnaie alternative, l'anonymat des transactions ne permettant pas de fournir les informations nécessaires au fonctionnement des marchés financiers, sans compter les risques de « hacking ».

Q2/- Les autorités publiques se sont-elles montrées plutôt favorables ou circonspectes sur les monnaies virtuelles, notamment le *bitcoin* ?

Les autorités publiques ont une vision plutôt négative du phénomène *bitcoin*, surtout depuis la faillite de *Mt. Gox*, une des plus importantes plateformes d'échange de *bitcoins*. Pour les autorités coréennes, la supervision des monnaies virtuelles est complexe, faisant craindre une utilisation elles peuvent être utilisées de manière frauduleuse (le blanchiment d'argent est la principale crainte).

Selon son rapport de 2013, la BOK estime que le *bitcoin* présente un potentiel en qualité de moyen de paiement alternatif mais seulement à terme, compte tenu des risques de cette monnaie virtuelle (échanges illégaux, risques pour les utilisateurs lors des transactions). Il est nécessaire de prendre des mesures réglementaires afin d'encadrer les activités commerciales et les secteurs concernés par l'utilisation possible du *bitcoin*

Q3/- Certains acteurs des monnaies virtuelles mènent-ils un travail de *lobbying* auprès des institutions publiques (administrations, Parlement,

régulateurs) ? Si oui, quels sont les arguments mis en avant ? Quelles sont leurs demandes ?

Pas de lobbying auprès du gouvernement ou au parlement sur les monnaies virtuelles n'a été identifié à ce jour.

Q4/- Les monnaies virtuelles font-elles l'objet d'une définition légale ? Des évolutions légales ou règlementaires sont-elles envisagées ? Si oui, préciser les principales dispositions.

En Corée, le *bitcoin* est considéré comme un bien numérique (digital good), par exemple, comme un fichier mp3. La Corée n'a pas préparé de loi-cadre d'encadrement des monnaies virtuelles. Les textes législatifs existants ne prennent pas encore en compte les produits issus de nouvelles technologies, tels que le bitcoin.

Les plateformes d'échanges de *bitcoin* sont déclarées dans le secteur de télémarketing auprès des administrations comme des portails de vente en ligne (*G-market*, *Interpark*, etc.) et ne font pas l'objet de contrôle ni par la banque centrale, ni par le MOSF (*Ministry of Strategy and Finance*), ni par la FSC (*Financial Services Commission*).

Selon les autorités, quand le marché sera plus développé avec un nombre d'échanges plus important, il sera nécessaire de clarifier le statut légal du *bitcoin* et de renforcer les mesures préventives ainsi que les dispositifs de contrôle.

Q5/- Les régulateurs sont-ils intervenus pour encadrer l'utilisation des monnaies virtuelles ? Les plateformes dédiées à l'utilisation de ces monnaies sont-elles soumises à des obligations spécifiques ?

Les régulateurs coréens du secteur financier ne mènent pas d'action concrète pour contrôler les monnaies virtuelles. L'ouverture des marchés boursiers du *bitcoin* ainsi que les activités commerciales ne requièrent pas de condition spécifique. Les commerçants doivent seulement faire une déclaration auprès des administrations pour commencer leurs activités selon la loi « *Act on the consumer protection in the electronic commerce transaction, etc.* ».

Q6/- Les administrations fiscales ont-elles pris position sur la nature des monnaies virtuelles et, partant, sur les conséquences fiscales qui y sont attachées ?

Selon le NTS (*Nation Tax Service*) qui est l'autorité fiscale coréenne, les monnaies virtuelles pouvant être utilisées comme un moyen de paiement, dont le *bitcoin*, ne sont pas imposables en Corée. Le NTS explique que cette

prise de position de la Corée sur le *bitcoin* a également été adoptée par plusieurs pays, excepté le Royaume-Uni qui prévoit de fiscaliser le *bitcoin*.

Le NTS distingue ces monnaies virtuelles non imposables du « *game money* » (l'argent du jeu virtuel), dont l'usage est restreint (il ne s'utilise que sur certains sites internet), mais qui donne lieu à des échanges beaucoup plus importants que ceux du *bitcoin*. Suite à un contentieux entre un particulier et le trésor public, la Cour Suprême a jugé en avril 2012 que les gains issus des jeux virtuels seraient dorénavant soumis à l'imposition. . En pratique, le NTS peine à fiscaliser le « *game money* » car les échanges en ligne sont très difficilement contrôlables. Le NTS craint que cette situation ne se reproduise avec le *bitcoin*.

Q7/- Les autorités publiques ont-elles entrepris des actions d'information ou de prévention vis-à-vis des épargnants ou des consommateurs ?

Aucune prise de position officielle des autorités politiques coréennes n'a été annoncée à ce stade. Les autorités n'ont pas encore publié de document pour sensibiliser ou informer les consommateurs et les investisseurs.

Q8/- Constate-t-on une progression des investissements (publics ou privés) en matière de monnaies virtuelles ?

Le marché du *bitcoin* en Corée repose sur quelques initiatives privées et ne suscite pas un grand intérêt du public. *Korbit*, la première plateforme d'échanges du *bitcoin* coréenne, établie en juillet 2013, a recueilli 450 000 USD d'investissements en janvier 2014 de la part de la Silicon Valley. Parmi les actionnaires coréens de *Korbit*, il y a *SK Planet* et *Banks Foundation for Young Entrepreneurs* mais leur participation relève plus d'un soutien à des start-up innovantes que d'un réel investissement dans les monnaies virtuelles.

Coinplug, une autre plateforme d'échanges, créée en janvier 2014 par de jeunes ingénieurs coréens, a élaboré un système de point de vente (POS) de *bitcoin* et a mis au point un distributeur automatique (ATM) en collaboration avec Hyosung, une entreprise coréenne. Ce premier distributeur a été installé en Corée en mars 2014. Là encore, il s'agit plutôt d'initiatives ponctuelles d'investisseurs privés.

Commentaires éventuels :

Compte tenu du développement technologique en Corée du Sud, l'utilisation des monnaies virtuelles devrait avoir un potentiel important. L'intérêt a été grandissant tout au long de l'année dernière mais la faillite de *Mt. Gox* a mis en lumière les possibles failles du système, et freiné l'intérêt des acteurs financiers et du grand public pour les monnaies virtuelles.

VI. ÉTATS-UNIS

Q1/- Les monnaies virtuelles ont-elles fait l'objet de débats, de travaux (rapports, auditions publiques, etc.), de prises de position publiques ou politiques ? Avez-vous identifié des réflexions en cours sur le sujet ? Des think-tanks sont-ils actifs sur le sujet ?

En raison des volumes de transaction et des nombreux acteurs présents sur le territoire américain, les monnaies virtuelles sont l'objet de beaucoup d'attention aux États-Unis. Des dizaines de blogs y sont consacrés et la plupart des médias nationaux traitent de l'actualité du *bitcoin*. Les monnaies virtuelles ont également fait l'objet de nombreuses prises de position publique. Parmi les prises de position publique, de nombreux investisseurs (*venture capital*) se sont déclarés en faveur du *bitcoin* (Mike Novogratz, Marc Andreessen, Winklevoss Twins, Steve Forbes). Toutefois Paul Krugman a qualifié dans une tribune décriée du *New York Times*[1] le *bitcoin* de « diable » et Warren Buffet de « mirage ».

Les autorités publiques en revanche accordent une attention croissance aux risques qui leur sont associés comme la forte volatilité, le financement d'activités illégales et notamment le blanchiment d'argent. Le *Department of Justice* a ainsi déjà fermé plusieurs plateformes d'échange de monnaies virtuelles utilisées pour financer des activités criminelles en s'appuyant sur les lois pénales en vigueur. La fermeture de *Silk Road*, plateforme permettant notamment l'achat et la vente de stupéfiants, qui utilisait le *bitcoin* comme monnaie d'échange a été très largement relayée dans les médias. Elle est notamment à l'origine d'une série d'audition menée par la commission du Sénat sur la sécurité intérieure (*Senate Committee on Homeland Security and Governmental Affairs*) sur les dangers liés au développement des monnaies virtuelles (*Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies*) en novembre dernier. Plusieurs représentants d'autorités publiques ainsi été invités à s'exprimer (*Department of Justice*, *Department of Treasury*, FBI).

De nombreux think-tanks se focalisent exclusivement sur la promotion des monnaies virtuelles, le plus connu d'entre eux est *The Bitcoin Foundation*, dont le Président a été appelé à témoigner lors de l'audition à la commission sur la sécurité intérieure du Sénat. La *Bitcoin Foundation* a été créée en septembre 2012 et regroupe plusieurs personnalités liées au *bitcoin* dont le créateur Satoshi Nakamoto[2].

Malgré les dizaines de monnaies virtuelles existantes, seule le *bitcoin* et à la marge, quelques autres (*Litecoin*, *Ripple*), font l'objet d'une attention particulière de la part des médias, des think-tanks, des autorités publiques.

[1] http://krugman.blogs.nytimes.com/2013/12/28/bitcoin-is-evil/.

Q2/- Les autorités publiques se sont-elles montrées plutôt favorables ou circonspectes sur les monnaies virtuelles, notamment le *bitcoin* ?

Les autorités publiques en charge de la régulation se sont montrées dans l'ensemble favorables aux monnaies virtuelles, certaines d'entre elles – la Fed et le FBI notamment[1] - soulignant à l'occasion de l'audition au Sénat, le potentiel des monnaies virtuelles à rendre les échanges plus efficients, sécurisés et rapides.

Néanmoins les autorités publiques en charge de la sécurité intérieure se sont montrées davantage circonspectes face au développement du *bitcoin* : très récemment, le ministère de la Défense (*Department of Defense*) a dédié une partie de ses activités aux risques que représentent ces monnaies pour le développement des activités terroristes.

Certains régulateurs des États fédérés, comme la *North American Securities Administrators Association* (NASAA) par exemple le 29 avril dernier, ont mis en garde les utilisateurs du *bitcoin* contre sa volatilité.

Q3/- Certains acteurs des monnaies virtuelles mènent-ils un travail de lobbying auprès des institutions publiques (administrations, Parlement, régulateurs) ? Si oui, quels sont les arguments mis en avant ? Quelles sont leurs demandes ?

Plusieurs associations soutiennent le développement du *bitcoin*, dont la plus connue est *The Bitcoin Foundation* (cf. Q1), une organisation à but non lucratif représentant les intérêts des investisseurs du secteur[2] et œuvrant pour la promotion du *bitcoin* auprès des institutions publiques[3]. De manière générale, les lobbys encouragent les institutions publiques à adapter et préciser le cadre législatif au *bitcoin* sans prendre de nouvelles dispositions. Ils mettent en avant le potentiel des monnaies virtuelles à révolutionner le transfert d'argent et proposer une solution alternative aux moyens de paiement traditionnels, plus couteux. Ils insistent également sur le caractère nouveau, prometteur et attaché à l'idéal de liberté de cette nouvelle technologie.

Ces points ont été développés lors de l'audition à la Commission du Sénat en novembre dernier du Président de *The Bitcoin Foundation* qui a eu notamment l'occasion de mettre en avant : (i) le caractère transnational et sûr

[1] *Selon Ben Bernanke, alors président de la Fed,* « these innovations may hold long-term promise, particularly if they promote a faster, more secure and more efficient payment system ». *Le FBI ajoute :* « our approach is guided by recognition that online payment systems, centralized and decentralized, offer legitimate financial services ».
[2] *Notamment,* Lightspeed Venture Partners *ou* Bitcoin Investment Trust.
[3] *L'organisation a d'ailleurs récemment embauché Amy Weiss, ancienne adjointe au service presse de la Maison Blanche et Jim Harper, ancien conseiller au Sénat et à la U.S. House.*

du *bitcoin* comme réserve de valeur, notamment dans les pays où la monnaie officielle est vulnérable (ii) les innovations apportées par le *bitcoin*, nouveau moyen de paiement plus rapide, et (iii) la création d'emplois dans divers secteurs. Selon lui, les États-Unis auraient par conséquent intérêt à se positionner en tant que leader dans la promotion et le développement de cette monnaie.

Par ailleurs, seul le *bitcoin* fait l'objet d'un lobbying de la part d'associations dédiées, les autres monnaies virtuelles n'ayant pas la même résonance.

Q4/- Les monnaies virtuelles font-elles l'objet d'une définition légale ? Des évolutions légales ou règlementaires sont-elles envisagées ? Si oui, préciser les principales dispositions.

Les autorités américaines ne se sont pas entendues pour donner une définition légale commune des monnaies virtuelles et un tel projet ne semble pas envisagé à court-terme. Néanmoins, le *Governement Accountability Office* (GAO) a proposé la définition suivante : « une monnaie virtuelle est une unité digitale d'échange qui n'est pas soutenue par l'État ». Selon le *FinCEN*, il s'agit d'un moyen d'échange qui opère comme une monnaie dans certains environnements sans pour autant en présenter tous les attributs.

Q5/- Les régulateurs sont-ils intervenus pour encadrer l'utilisation des monnaies virtuelles ? Les plateformes dédiées à l'utilisation de ces monnaies sont-elles soumises à des obligations spécifiques ?

Il n'y a pas de réglementation globale des monnaies virtuelles, les autorités de régulation traitant les monnaies virtuelles selon leurs prérogatives.

La *Federal Reserve*, par le biais de sa Président, Janet Yellen, a déclaré que la réglementation du *bitcoin* n'était pas de son ressort.

La *FinCen* a publié une directive concernant les modalités du *Bank Secrecy Act* en ce qui concerne les monnaies virtuelles. Le *FinCEN* assimile les plateformes de conversion dollar/*bitcoin* à des Money Service Businesses et les contraint à s'enregistrer à ce titre auprès de lui, et à se conformer à l'obligation d'identification de leurs clients (*Know Your Client*), réduisant de fait l'anonymat d'une partie des utilisateurs de cette monnaie virtuelle. Par ailleurs, ces plateformes de conversion sont depuis mars 2013 soumises à des mesures anti-blanchiment qui leur imposent (i) de tenir des registres de l'ensemble des transactions effectuées, (ii) de reporter au gouvernement toutes transactions de plus de 10 000$ et (iii) de prévenir le *FinCEN* de toute suspicion de fraude. Le *FinCEN* a ensuite précisé explicitement en janvier 2014 que les « mineurs » et investisseurs en *bitcoin*s pour compte propre ne

sont pas soumis à ces contraintes. La FinCen a rappelé cette dernière disposition dans une note publiée le 29 avril[1].

La SEC s'estime en mesure de se saisir de toute transaction où des intérêts seraient versés à partir d'actifs liés à une monnaie virtuelle, et un ETF (*Exchange Traded Fund*) en *bitcoins* s'est inscrit en octobre 2013 auprès de l'agence.

La CFTC estime que tout produit dérivé ayant pour sous-jacent une monnaie virtuelle ou un actif libellé en monnaie virtuelle se situe sous sa juridiction et devrait ainsi publier une directive sur la réglementation des dérivés en *bitcoin* à moyen-terme.

Les régulateurs des États fédérés pourraient également émettre une réglementation du *bitcoin*. L'État de New-York a notamment mené, courant janvier, des auditions destinées à déterminer l'opportunité et les modalités d'une « *BitLicense* », et prévoit la définition courant 2014 d'un cadre réglementaire pour les monnaies virtuelles. L'État de Californie a pour sa part envoyé mi-2013 plusieurs mises en demeures à des entreprises soupçonnées d'opérer sans licence en tant que Money Transmission Services en *bitcoins*. Un projet de loi est par ailleurs à l'étude au Sénat de l'État de Californie pour fournir au *bitcoin* un cadre pleinement légal.

Q6/- Les administrations fiscales ont-elles pris position sur la nature des monnaies virtuelles et, partant, sur les conséquences fiscales qui y sont attachées ?

L'*Internal Revenue Service* (IRS), le service des impôts américain, a récemment publié une notice sur le sujet (n° 2014-21 en date du 25 mars 2014). Il attribue, dans ce document, le statut de titre de propriété au *bitcoin* plutôt que celui de monnaie. Cette classification a de nombreuses implications sur le régime de taxation du *bitcoin* : (i) les détenteurs de la monnaie devront déclarer leurs gains /pertes en tant que gains/pertes en capital plutôt qu'en monnaie étrangère. Cette taxation vaut également lorsqu'un *bitcoin* est utilisé pour régler un achat. (ii) Les mineurs de *bitcoin* seront considérés comme des travailleurs indépendants et devront déclarer les gains réalisés en dollar par leur activité (le cours de référence étant le cours du *bitcoin* à la date du minage). Cette nouvelle réglementation devrait avoir des répercussions sur l'usage de la crypto-monnaie, notamment comme valeur d'échange.

Q7/- Les autorités publiques ont-elles entrepris des actions d'information ou de prévention vis-à-vis des épargnants ou des consommateurs ?

[1] http://www.fincen.gov/news_room/rp/rulings/html/FIN-2014-R007.html

Plusieurs autorités publiques au niveau fédéral ont publié des notices de mise en garde des consommateurs sur les dangers du *bitcoin*.

La SEC a publié une mise en garde concernant les schémas de Ponzi utilisant la monnaie virtuelle[1].

Les régulateurs de plusieurs États ont également publié des notices de mise en garde contre l'utilisation des monnaies virtuelles à travers la NASAA, un organisme qui regroupe différents régulateurs d'États nord-américains. En mars 2014, le *Washington State Department of Financial Institutions* a également publié une alerte sur les risques liés aux monnaies virtuelles.

La FINRA, un association d'autorégulation des marchés, a publié une notice[2] visant à rappeler les dangers d'une forte volatilité des cours et les risques inhérents aux plateformes de *trading* (symbolisés par *Mt. Gox*).

Q8/- Constate-t-on une progression des investissements (publics ou privés) en matière de monnaies virtuelles ?

De nombreux fonds d'investissement (venture-capital) ont investis des sommes très importantes sur le *bitcoin* ou sur des projets qui y sont liés. Ainsi 98,6 millions de dollars ont été levés depuis la création du *bitcoin* en 2009 pour être injecté dans 19 startups nord-américaines[3]. Le fonds *Fortress Investment Group* (62 milliards de dollars d'actifs sous gestion) a investi dans Patera Capital Management, un *hedge fund* se concentrant uniquement sur l'univers *bitcoin*.

Par ailleurs de plus en plus d'incubateurs aident les startups spécialisées dans les monnaies virtuelles à se financer et se développer. Récemment, Seedcoin, le premier incubateur spécialisé dans les startups *bitcoin* a levé 2 000 *bitcoins* à l'occasion de son second round, et l'incubateur californien 500Startups a lancé un consortium d'investisseurs qui se concentrera sur le *bitcoin* et les technologies financières.

Enfin, les plateformes d'échanges de monnaies virtuelles - permettant d'échanger des dollars contre des *bitcoin* ou autres monnaies virtuelles et de les stocker dans un portefeuille virtuel – ne cessent de s'accroitre. Ces plateformes permettent au grand public et aux professionnelles d'échanger facilement de la monnaie virtuelle.

[1] www.sec.gov/investor/alerts/ia_virtualcurrencies.pdf
[2] http://www.finra.org/Investors/ProtectYourself/InvestorAlerts/FraudsAndScams/P456458
[3] *Selon une étude menée par le cabinet* Aite Group.

VII. INDE

Q1/- Les monnaies virtuelles ont-elles fait l'objet de débats, de travaux (rapports, auditions publiques, etc.), de prises de position publiques ou politiques ? Avez-vous identifié des réflexions en cours sur le sujet ? Des think-tanks sont-ils actifs sur le sujet ?

En Inde, il existe des débats sur les monnaies virtuelles, en dépit de leur faible pénétration sur le marché local (en particulier, l'Inde représenterait à ce jour 1 % du marché mondial du *bitcoin* ; de 30 000 à 50 000 Indiens seraient en possession de cette monnaie virtuelle).

Ces débats ont surtout émergé à la suite des forts mouvements de baisse du « cours » du *bitcoin* par rapport au dollar, depuis la fin de l'année 2013. En décembre dernier, la banque centrale indienne (la RBI) a mis en garde les utilisateurs de monnaies virtuelles contre les risques qu'ils encourent.

Le gouvernement indien, qui, comme la RBI, est sensible à la question de la protection du consommateur, s'est également publiquement interrogé sur le rôle actuel ou potentiel des monnaies virtuelles dans le financement d'activités illégales voire criminelles. Dans le cas du *bitcoin* en particulier, en raison du caractère anonyme des transactions (les utilisateurs sont repérés par une adresse électronique composée de 34 caractères et non par leur identités civiles), cette monnaie virtuelle peut être utilisée pour contourner les règles relatives à la lutte contre le blanchiment de capitaux et le financement du terrorisme. Une enquête serait en cours sur deux plateformes (*BuySellBitCo.in* et *Rbitco.in*), depuis décembre 2013.

Des conférences sont organisées de façon sporadique à travers le pays, souvent à l'initiative des plateformes d'échanges.

Q2/- Les autorités publiques se sont-elles montrées plutôt favorables ou circonspectes sur les monnaies virtuelles, notamment le *bitcoin* ?

L'approche des autorités est ambivalente, qu'il s'agisse des autorités monétaires ou budgétaires.

La RBI, soucieuse de protéger le consommateur, a insisté sur les risques liés à la détention de *bitcoins*, mais n'a pas interdit ou limité les échanges.

De son côté, le gouvernement, qui s'est inquiété des risques de financement d'activités criminelles (cf. supra), a, dans le même temps, regretté le manque à gagner pour les finances publiques de la non taxation des transactions réalisées en monnaies virtuelles, et, en particulier, en *bitcoins*.

Q3/- Certains acteurs des monnaies virtuelles mènent-ils un travail de lobbying auprès des institutions publiques (administrations, Parlement, régulateurs) ? Si oui, quels sont les arguments mis en avant ? Quelles sont leurs demandes ?

L'organisation à but non lucratif « *Bitcoin Alliance India* » s'est donnée trois objectifs : mettre fin aux incompréhensions concernant la monnaie, aider les entrepreneurs à développer la monnaie cryptographique et, enfin, proposer un cadre de régulation de la monnaie. Cette organisation a été fondée en janvier 2014, dans le sillage de la conférence tenue en décembre dernier à Bangalore (« *Global Bitcoin Conference* ») à l'initiative de la plateforme *Coinmonk*.

C'est à notre connaissance la seule structure susceptible de représenter la « communauté » des utilisateurs de *bitcoins*. Trop jeune, elle ne disposerait que de très peu de relais auprès des administrations, du Parlement ou des régulateurs.

Cette structure ne met pas en avant de motivations spécifiques indiennes pour justifier de l'utilisation du *bitcoin*. Pour Philippe Herlin, professeur de finance au CNAM et auteur de « *La révolution du* bitcoin *et des monnaies complémentaires, une solution pour échapper au système bancaire et à l'euro ?* », l'Inde pourrait devenir une place forte du *bitcoin* dans les prochaines années : en plus de présenter des « avantages » bien connus d'interopérabilité des opérations de paiements et d'absence de taxes ou de commissions sur les opérations d'achat ou de revente, le *bitcoin* pourrait devenir une valeur refuge en Inde, au même titre que l'or, dans un contexte local marqué par la dépréciation de la roupie et par une inflation élevée.

Q4/- Les monnaies virtuelles font-elles l'objet d'une définition légale ? Des évolutions légales ou règlementaires sont-elles envisagées ? Si oui, préciser les principales dispositions.

Les monnaies virtuelles ne font pas l'objet d'une définition légale en Inde.

Q5/- Les régulateurs sont-ils intervenus pour encadrer l'utilisation des monnaies virtuelles ? Les plateformes dédiées à l'utilisation de ces monnaies sont-elles soumises à des obligations spécifiques ?

L'utilisation des monnaies virtuelles n'est pas encadrée. Mais les questionnements tant de la RBI que Ministère des Finances ont suffi à produire des effets visibles sur le « marché » :

BuySellBitCo.in, la principale plateforme indienne de transactions de la monnaie virtuelle, a suspendu ses activités le 27 décembre 2013. Cette

plateforme, dirigée par Mahim Gupta, est surveillée par les services du gouvernement en raison d'importantes transactions suspectes (quelques 1000 transactions impliquant 400 individus, pour un total de plusieurs centaines de milliers de dollars). Officiellement, la plateforme a annoncé qu'elle souhaitait protéger ses utilisateurs « *tant que le cadre réglementaire des monnaies virtuelles ne sera pas défini plus clairement en Inde* ». Jusqu'à sa fermeture, elle enregistrait presque 200 000 dollars de transactions par mois.

Le lancement du *Laxmicoin*, une monnaie virtuelle proprement indienne (Laxmi est la déesse de la fortune chez les Hindous), a été retardé depuis les mises en garde de la Banque centrale. Son créateur, Mitts Daki, a lui aussi déclaré être dans l'attente d'un éclaircissement concernant la réglementation de la devise et son approbation par la RBI. La différence entre le *Laxmicoin* et le *bitcoin* est floue à ce stade.

Q6/- Les administrations fiscales ont-elles pris position sur la nature des monnaies virtuelles et, partant, sur les conséquences fiscales qui y sont attachées ?

L'*Income Tax Department* envisagerait de taxer les échanges réalisés à partir de ce type de monnaies. Selon cette direction du Ministère des Finances, cette taxe permettrait de limiter l'évasion fiscale. Pour évaluer l'impact d'une telle mesure, des bases de données sur les transactions effectuées en *bitcoins* ont été récupérées par l'administration fiscale indienne (notamment auprès de la start-up *CoinMonk Ventures*). Un tel projet nécessite cependant au préalable une reconnaissance juridique de la devise (à l'instar de ce qui existerait en Allemagne).

Q7/- Les autorités publiques ont-elles entrepris des actions d'information ou de prévention vis-à-vis des épargnants ou des consommateurs ?

À l'exception de la communication de la RBI, aucune action n'a été entreprise.

Q8/- Constate-t-on une progression des investissements (publics ou privés) en matière de monnaies virtuelles ?

Aucun n'investissement significatif en matière de monnaies virtuelles n'a été relevé en dehors de la création de sites de commerce en ligne. À titre d'illustrations, HighKart.com accepte uniquement les *bitcoins* comme moyen de paiements. Ce site propose l'achat de nombreux biens marchands dans différents secteurs (habillement, biens électroménagers, biens électroniques, bijouterie). Sa rentabilité n'est pas connue.

Commentaires éventuels :

Le gouvernement indien semble se pencher vers une réglementation calquée sur celle des États-Unis, réglementation qui accepte le *bitcoin* comme moyen de paiement mais qui s'attache en parallèle à combattre l'utilisation du réseau à des fins criminelles (blanchiment d'argent, trafic de stupéfiants).

VIII. ISRAËL

Q1/- Les monnaies virtuelles ont-elles fait l'objet de débats, de travaux (rapports, auditions publiques, etc.), de prises de position publiques ou politiques ? Avez-vous identifié des réflexions en cours sur le sujet ? Des think-tanks sont-ils actifs sur le sujet ?

L'activité liée aux monnaies virtuelles est relativement importante en Israël. Véritable « économie de l'innovation », le pays est un leader en matière d'électronique, de cyber-sécurité, et des technologies associées à la finance, ce qui a contribué à l'émergence de start-ups spécialisées dans les monnaies virtuelles. Israël compte notamment cinq plateformes d'échanges de *bitcoins*, des sociétés spécialisées dans le développement de microprocesseurs pour « minage » parmi les plus performants au monde, ainsi que des associations actives cherchant à promouvoir l'utilisation de *bitcoins*. Plusieurs dizaines de commerces israéliens, notamment des restaurants, acceptent le paiement en *bitcoins*. Une monnaie virtuelle locale, *Isracoin*, a également été créée.

Ces monnaies font l'objet de débats publics réguliers dans le pays. L'association israélienne des *bitcoins*, fondée en 2011 par des entrepreneurs du secteur, organise deux fois par mois des conférences sur les monnaies virtuelles. Le plus grand rassemblement, organisé en juillet 2013, a réuni plus de 300 participants. Le débat est également animé par l'association sur internet : diffusion d'articles et vidéos, forums, groupe Facebook qui compte plus de 3000 membres.

Le phénomène a suscité l'intérêt de la presse israélienne. Une dizaine d'articles consacrés aux monnaies virtuelles ont été publiés par les principaux quotidiens économiques du pays ces dernières années.

Pour l'heure l'utilisation des monnaies virtuelles n'a pas donné lieu à des prises de positions politiques affirmées, à l'exception de quelques rares interventions dans la presse d'hommes politiques plutôt favorables à leur développement. En revanche, une déclaration officielle des autorités financières visant à souligner les risques liés à ces monnaies a été publiée en février 2014 (cf. question 7).

Q2/- Les autorités publiques se sont-elles montrées plutôt favorables ou circonspectes sur les monnaies virtuelles, notamment le *bitcoin* ?

Les autorités publiques ont clairement souligné les risques liés à l'utilisation des *bitcoins* mais ne se sont pas prononcées clairement contre leur utilisation et se sont engagées à étudier la question (cf. question 7). Elles consentent par ailleurs à la certification des sociétés gérant des plateformes d'échanges comme bureaux de change tout en ne reconnaissant pas le *bitcoin* comme une véritable monnaie.

La *Tax Authority*, l'agence chargée de la lutte contre le blanchiment d'argent et la police se montrent favorables à un dialogue régulier avec les associations et entrepreneurs du secteur.

Q3/- Certains acteurs des monnaies virtuelles mènent-ils un travail de lobbying auprès des institutions publiques (administrations, Parlement, régulateurs) ? Si oui, quels sont les arguments mis en avant ? Quelles sont leurs demandes ?

Des associations regroupant les acteurs des monnaies virtuelles mènent un travail de lobbying. Pour promouvoir leurs vues elles rencontrent régulièrement les administrations fiscales et financières ainsi que des hommes politiques et leurs équipes.

Les principaux entrepreneurs israéliens actifs dans ce secteur mettent en avant la nécessité pour les autorités publiques de réguler l'utilisation des monnaies virtuelles et d'établir des normes claires à suivre pour éviter le blanchiment d'argent par le biais de plateformes d'échanges. Ils estiment en effet que tout en servant l'intérêt de l'État, un cadre juridique rassurerait les utilisateurs et renforcerait l'usage des monnaies virtuelles.

Certaines plateformes d'échanges ont adopté de leur propre initiative, sans que les autorités les y obligent à ce stade, des mesures visant à éviter le blanchiment d'argent. Elles s'inspirent des règles applicables à l'échange de monnaies reconnues. Au-delà de certaines sommes échangées ces sociétés demandent la présentation d'une ou plusieurs cartes d'identités. Elles affirment également soumettre des rapports réguliers sur l'ensemble des transactions effectuées aux autorités en charge de la lutte contre le blanchiment d'argent. En l'absence de réglementation et contrôle en la matière, la portée réelle de ces mesures n'est cependant pas démontrée.

Q4/- Les monnaies virtuelles font-elles l'objet d'une définition légale ? Des évolutions légales ou règlementaires sont-elles envisagées ? Si oui, préciser les principales dispositions.

Les monnaies virtuelles ne font pas l'objet d'une définition légale. Aucune évolution n'est pour le moment envisagée, les autorités adoptant une position attentiste.

Q5/- Les régulateurs sont-ils intervenus pour encadrer l'utilisation des monnaies virtuelles ? Les plateformes dédiées à l'utilisation de ces monnaies sont-elles soumises à des obligations spécifiques ?

A ce jour les régulateurs ne sont pas intervenus pour encadrer l'utilisation de ces monnaies, qui ne sont soumises à aucune obligation spécifique.

Q6/- Les administrations fiscales ont-elles pris position sur la nature des monnaies virtuelles et, partant, sur les conséquences fiscales qui y sont attachées ?

Non, les autorités fiscales n'ont pas pris position sur la nature des monnaies virtuelles.

Q7/- Les autorités publiques ont-elles entrepris des actions d'information ou de prévention vis-à-vis des épargnants ou des consommateurs ?

En février 2014 la Banque centrale d'Israël, le département des marchés de capitaux, des assurances et de l'épargne du Ministère des Finances, la *Tax Authority*, l'Autorité des valeurs mobilières, et l'Autorité de lutte contre le blanchiment d'argent et le financement du terrorisme ont publié une déclaration commune pour avertir des risques liés aux monnaies virtuelles. Ces autorités ne déconseillent pas formellement l'utilisation des monnaies virtuelles mais appellent à la vigilance.

La déclaration fait état de huit risques principaux :

- la valeur de ces monnaies n'est garantie par aucune banque centrale ;

- la gestion du risque lié à ces monnaies est difficile car elles peuvent être échangées de manière anonyme hors des circuits de contrôle traditionnels des institutions financières ;

- elles peuvent constituer un terreau fertile aux activités financières frauduleuses (système de Ponzi par exemple) ;

- la valeur des monnaies virtuelles est très volatile ;

- échangées de manière anonyme ces monnaies peuvent être utilisées à des fins de blanchiment d'argent et de financement du terrorisme ;

- elles peuvent être volées par le biais de piratages informatiques ;

- des plateformes d'échanges peuvent fermer et les monnaies détenues par leur intermédiaire disparaître ;

- l'échange de monnaies virtuelles n'est pas supervisé par les autorités israéliennes.

Q8/- Constate-t-on une progression des investissements (publics ou privés) en matière de monnaies virtuelles ?

L'évolution de l'achat de *bitcoins* par les utilisateurs privés est très volatile et suit les tendances constatées dans le reste du monde Les acteurs du secteur évaluent à moins de dix millions d'euros le montant total des *bitcoins* achetés en Israël à ce jour.

IX. JAPON

Q1/- Les monnaies virtuelles ont-elles fait l'objet de débats, de travaux (rapports, auditions publiques, etc.), de prises de position publiques ou politiques ? Avez-vous identifié des réflexions en cours sur le sujet ? Des think-tanks sont-ils actifs sur le sujet ?

Le sujet de la monnaie virtuelle ne suscite que peu d'engouement au Japon, en dehors de l'affaire « *Mt. Gox* » de février dernier (voir également la note du SER de Tokyo « *La faillite de* Mt. Gox *: quelle régulation et supervision japonaises pour le Bitcoin* » de mars 2014) :

L'importance des monnaies virtuelles est en réalité limitée dans le pays (seulement 15 magasins acceptaient les paiements en *bitcoins* fin 2013 sur tout le territoire). Il est clairement apparu que *Mt. Gox* n'avait que peu de clients japonais (au mieux quelques milliers) et que son lien avec le Japon était surtout sa localisation géographique à Tokyo.

De fait, l'écho médiatique de la faillite de la plateforme *Mt. Gox* a surtout été provoqué par les suites judiciaires engagées en Amérique du nord et, au Japon, par les attaques d'un parlementaire de l'opposition, Tsutomu Okubo. Ancien vice-ministre des finances et très impliqué sur ce sujet, celui-ci a interrogé à plusieurs reprises le gouvernement, l'obligeant ainsi à prendre publiquement position. En réponse, le gouvernement a officiellement déclaré le 7 mars qu'il considère que le bitcoin n'est pas une monnaie, mais que les transactions en bitcoin peuvent être taxées dans le cadre réglementaire actuel (taxe sur la consommation et impôt sur le revenu et sur les sociétés). Le débat public n'a pas davantage été soutenu, les autorités restant factuelles et prudentes, signalant simplement qu'elles « se penchaient » sur la question.

Aucun think tank n'est actuellement actif sur la monnaie virtuelle : sa faible importance économique et sociale dans le pays ne justifie pas l'intérêt des centres de recherche. Koji Sakuma, *chief economist* du centre de recherche de la Bank of Tokyo-Mitsubishi UFJ (la plus importante banque du pays), auteur d'un récent rapport sur le *bitcoin*, nous confie que la parution de son rapport peu de temps avant l'affaire *Mt. Gox* n'est qu'un concours de circonstance et qu'il n'envisage pas de poursuivre davantage ses travaux sur le sujet (« *this was my first and probably last report on bitcoins* »).

Q2/- Les autorités publiques se sont-elles montrées plutôt favorables ou circonspectes sur les monnaies virtuelles, notamment le *bitcoin* ?

Avant même le coup de projecteur très défavorable provoqué par la faillite de *Mt. Gox*, les autorités se sont toujours montrées réservées à l'égard du *bitcoin*. Selon M. Sakuma, cette méfiance s'explique d'abord par le rôle potentiel des monnaies virtuelles dans le blanchiment et le financement

occulte[1]. M. Sakuma explique que l'inconvénient principal du *bitcoin* comme moyen de paiement est, d'une part sa forte volatilité contre cours légal (cotation sur les plateformes d'échange type *Mt. Gox*), et d'autre part sa faible liquidité compte tenu de la fréquence des transactions (à peine 50 par minute, contre plus de 1000 pour le système Visa).

En définitive, les autorités ont donc une approche plutôt conservatrice. Elles n'envisagent pas la monnaie virtuelle comme un catalyseur possible du développement des marchés et de l'économie japonaise en général, et se satisfont du faible engouement de la population en la matière.

Q3/- Certains acteurs des monnaies virtuelles mènent-ils un travail de lobbying auprès des institutions publiques (administrations, Parlement, régulateurs) ? Si oui, quels sont les arguments mis en avant ? Quelles sont leurs demandes ?

Il n'y a aucun travail de lobbying.

Q4/- Les monnaies virtuelles font-elles l'objet d'une définition légale ? Des évolutions légales ou règlementaires sont-elles envisagées ? Si oui, préciser les principales dispositions.

La position des autorités est très claire : ce n'est pas de la monnaie et elles n'ont aucune définition légale.

Aucune évolution légale ou règlementaire n'est envisagée à ce stade, ni vers davantage de restriction, ni vers davantage de souplesse. Les autorités veulent surtout garder leurs distances en espérant que le sujet restera marginal (selon M. Sakuma et des contacts à la BOJ).

Q5/- Les régulateurs sont-ils intervenus pour encadrer l'utilisation des monnaies virtuelles ? Les plateformes dédiées à l'utilisation de ces monnaies sont-elles soumises à des obligations spécifiques ?

La loi bancaire japonaise interdit aux établissements de prendre en dépôts ou effectuer des transactions par l'intermédiaire de *bitcoins*.

Les autorités seraient officiellement en train d'approfondir le sujet (« *fact finding* »), mais des contacts au sein de l'administration nous confirment leur réticence de principe à réguler (et donc reconnaître) la monnaie virtuelle. Le sous-gouverneur de la Banque du Japon, Hiroshi Nakaso, nous confie qu'il estime que la monnaie virtuelle serait impossible à superviser si elle venait à être régulée. Dès lors il préfère chercher à rendre le

[1] *Le sous-gouverneur de la Banque du Japon, Hiroshi Nakaso, estime pour sa part que le* bitcoin *est avant tout une menace pour le système de paiement classique.*

système de paiement classique plus « compétitif » [en réduisant les coûts de transactions notamment] afin de prévenir le développement des monnaies virtuelles, plutôt que de chercher à les réguler.

Q6/- Les administrations fiscales ont-elles pris position sur la nature des monnaies virtuelles et, partant, sur les conséquences fiscales qui y sont attachées ?

Oui. Compte tenu des textes actuels, l'administration fiscale estime que les transactions en *bitcoins* sont taxables en théorie (taxe à la consommation et impôt sur le revenu et sur les sociétés).

Leur approche est néanmoins passive dans la mesure où cette imposition reste sur des bases déclaratives (déclaration des transactions en *bitcoins* par les contribuables) : la *National Tax Agency* n'a ainsi pas montré d'appétence particulière pour la recherche active de ces transactions (dans la pratique difficiles à tracer) en vue de leur taxation. Les efforts à fournir ne seraient pas en adéquation avec le faible volume de ces transactions.

Q7/- Les autorités publiques ont-elles entrepris des actions d'information ou de prévention vis-à-vis des épargnants ou des consommateurs ?

Aucune campagne proactive n'a été entreprise.

Q8/- Constate-t-on une progression des investissements (publics ou privés) en matière de monnaies virtuelles ?

Aucune progression significative n'a été observée : la demande reste faible.

Commentaires éventuels :

La « menace » du *bitcoin* évoquée par le sous-gouverneur Nakaso reste largement virtuelle : la forte intégration financière du pays (plus de 96 % de la population de plus de 15 ans dispose d'un compte bancaire[1]) et l'efficacité de son système de paiement (en particulier sur les transactions transfrontalières) réduisent grandement l'attractivité de la monnaie virtuelle. Même si le nombre de commerces à accepter les *bitcoins* venaient à se multiplier, il est probable que le nombre de transactions effectives en *bitcoins* resterait très limité. C'est une différence notable avec la Chine. On notera d'ailleurs qu'un quart de la quinzaine d'établissements commerciaux à accepter des *bitcoins* au Japon sont en fait des écoles de langue chinoises d'après M. Sakuma.

[1] *Source : Banque Mondiale, 2011 : http://datatopics.worldbank.org/financialinclusion/.*

X. ROYAUME-UNI

Q1/- Les monnaies virtuelles ont-elles fait l'objet de débats, de travaux (rapports, auditions publiques, etc.), de prises de position publiques ou politiques ? Avez-vous identifié des réflexions en cours sur le sujet ? Des think-tanks sont-ils actifs sur le sujet ?

Les monnaies virtuelles, notamment les *bitcoins*, ont fait l'objet d'une couverture importante dans les médias, mais il n'y a pas eu pour le moment de rapport ou d'auditions parlementaires sur le sujet.

Les prises de position des autorités sont pour l'instant rares :

- HMRC a pris une décision sur le traitement fiscal des monnaies virtuelles (cf. note jointe) ;

- La Banque d'Angleterre considère que « *les* bitcoins *ne devraient pas avoir un impact significatif à court terme sur [ses] objectifs en matière de politique monétaire et de maintien de la stabilité financière, compte tenu de la faible importance des transactions à ce stade* ». Elle indique qu'elle continue à « *suivre attentivement l'évolution de l'activité liée aux monnaies virtuelles et [sa] position à l'avenir dépendra de ses développements* » ;

- Chris Salmon, à l'époque *Chief Cashier* de la Banque d'Angleterre, a souligné lors d'un colloque en novembre 2013 le caractère innovant des *bitcoins*, mais estimé qu'ils pourraient être remplacés par une monnaie virtuelle technologiquement plus avancée. Il a en outre estimé que la probabilité qu'une banque centrale émette des monnaies virtuelles dans la décennie à venir était à son avis proche de zéro (« *exceedingly unlikely* »).

Q2/- Les autorités publiques se sont-elles montrées plutôt favorables ou circonspectes sur les monnaies virtuelles, notamment le *bitcoin* ?

Il est difficile de trancher compte tenu de la rareté des prises de position publiques des autorités.

HMRC (direction des impôts) a pris rapidement une position sur le traitement fiscal des monnaies virtuelles, dans un sens qui apparaît favorable à leur usage (exonération de TVA pour l'échange de monnaies virtuelles contre des devises, en particulier) ;

Côté Banque d'Angleterre, l'attitude à notre sens semble plutôt être celle d'une neutralité bienveillante, comme le montrent les déclarations de Chris Salmon.

Q3/- Certains acteurs des monnaies virtuelles mènent-ils un travail de lobbying auprès des institutions publiques (administrations, Parlement, régulateurs) ? Si oui, quels sont les arguments mis en avant ? Quelles sont leurs demandes ?

Oui. Les acteurs de l'industrie souhaiteraient être régulés, afin d'obtenir le « sceau » du régulateur qui permettrait de convaincre le grand public de leur solidité et de leur sérieux.

Q4/- Les monnaies virtuelles font-elles l'objet d'une définition légale ? Des évolutions légales ou règlementaires sont-elles envisagées ? Si oui, préciser les principales dispositions.

Non, il n'y a pas de définition légale à ce stade, hormis celle qui serait implicite dans la décision de HMRC (cf. note jointe).

La *Prudential Regulation Authority* pourrait avoir à prendre position si une entité affirmant recevoir des dépôts en *bitcoins* cherchait à obtenir une licence bancaire.

Q5/- Les régulateurs sont-ils intervenus pour encadrer l'utilisation des monnaies virtuelles ? Les plateformes dédiées à l'utilisation de ces monnaies sont-elles soumises à des obligations spécifiques ?

Non, les régulateurs ne sont pas intervenus (hormis HMRC) et aucune obligation supplémentaire spécifique n'est mise en place à ce stade (mai 2014).

Q6/- Les administrations fiscales ont-elles pris position sur la nature des monnaies virtuelles et, partant, sur les conséquences fiscales qui y sont attachées ?

Cf. note jointe pour la position prise le 3 mars 2014 par HRMC.

Q7/- Les autorités publiques ont-elles entrepris des actions d'information ou de prévention vis-à-vis des épargnants ou des consommateurs ?

Non, aucune pour le moment (mai 2014).

Q8/- Constate-t-on une progression des investissements (publics ou privés) en matière de monnaies virtuelles ?

Pour l'instant les investissements sont faibles, même si l'on constate le développement aux Etats-Unis (mais pas au Royaume-Uni pour l'instant) de plusieurs plateformes d'*Exchange Traded Funds* permettant d'investir en

bitcoins (notamment *Winklevoss Bitcoin ETF*, qui a fait l'objet d'une demande d'agrément auprès de la SEC).

ANNEXE

NOTE

OBJET : règles fiscales applicables aux *bitcoins* au Royaume-Uni.

Les autorités britanniques ont publié le 3 mars 2014[1] des commentaires concernant les règles applicables aux *bitcoins* en matière de TVA, d'impôt sur les sociétés, d'impôt sur le revenu et de plus-values. Elles indiquent par ailleurs qu'un certain nombre de commerçants, tels que les opérateurs du commerce électronique, les pubs ou encore les restaurants utiliseraient déjà les *bitcoins* comme moyens de paiement. Ces commentaires, notamment en ce qu'ils font référence à la notion de monnaies virtuelles (« *cryptocurrencies* ») n'ont pas vocation à s'appliquer en dehors du domaine de la fiscalité.

1- TVA

Comme le rappelle l'administration fiscale (HMRC), les règles de TVA étant régies au niveau européen, le traitement des opérations portant sur les *bitcoins* adopté par le Royaume-Uni doit être cohérent avec celui qui pourrait éventuellement être mis en œuvre au niveau de l'Union européenne.

Dans cette attente, la position exprimée par ces commentaires n'a qu'un caractère provisoire :

- l'activité de création de *bitcoins* (« *bitcoin mining* ») est placée hors du champ de la taxe, dès lors que cette activité ne constitue pas une activité économique au sens de la TVA ;

- en revanche, les prestations de services qui seraient rendues dans le cadre d'autres activités par les créateurs de *bitcoins* (« *miners* »), telles que pour la fourniture de services dans le cadre de la vérification de transactions spécifiques pour lesquels des frais sont facturés, seront exonérés de la TVA en vertu de l'Article 135-1(d) de la directive TVA 2006/112/CE dès lors que ces opérations doivent être considérées comme répondant à la définition des opérations qui sont visées par ces dispositions à savoir, « *les opérations, y compris la négociation, concernant les dépôts de fonds, comptes courants, paiements, virements, créances, chèques et autres effets de commerce* » ;

- lorsque les *bitcoins* sont échangés contre des livres sterling ou d'autres monnaies étrangères (comme les euros ou les dollars), aucune TVA n'est due sur la valeur des *bitcoins* eux-mêmes ;

[1] http://www.hmrc.gov.uk/briefs/vat/brief0914.htm

- les frais facturés en sus de la valeur des *bitcoins* en vue de négocier ou d'effectuer toute transaction concernant les *bitcoins* sont exonérés de la TVA en application des dispositions de l'article 135-1 (d) de la directive précitée.

En revanche, dans tous les cas, la TVA est due de façon normale sur les biens ou les services qui sont vendus en échange de *bitcoins* ou de toute autre monnaie virtuelle identique (« *cryptocurrency* »). La valeur du bien ou du service sur lequel la TVA est due correspond à la contrevaleur des *bitcoins* exprimée en livres au moment où la transaction a lieu.

2- Impôts directs

Comme pour toute autre activité professionnelle, les produits et les charges constatés à raison d'activités qui seraient en lien avec les *bitcoins* ou d'autres monnaies virtuelles doivent être soumis aux règles applicables en matière d'impôt sur les sociétés, d'impôt sur le revenu et de plus-values.

La question de savoir si un profit imposable ou si une perte déductible doivent être constatés dépend des circonstances de chaque espèce.

Les autorités britanniques notent toutefois qu'une opération, en raison de son caractère hautement hypothétique (« *speculative* »), pourrait ne pas être taxable (ou engendrés des pertes déductibles), à l'instar des gains sur les jeux et paris qui ne sont pas taxables et dont les pertes ne peuvent venir en déduction d'autres profits imposables[1].

Pour les entreprises qui acceptent d'être payés en *bitcoins*, il n'y a aucune modification engendrée dans la façon de déterminer leurs profits imposables.

La taxation des opérations portant sur les *bitcoins* résulte à ce stade de l'application des règles de droit commun en matière d'impôts directs, tant pour les entreprises que pour les particuliers.

Impôts sur les sociétés

Les profits et les pertes constatés sur des opérations de change entre monnaies sont habituellement à prendre en compte pour la détermination du résultat imposable.

[1] *Selon HMRC, en principe, les gains sur les paris et les jeux ne sont pas imposables au niveau du joueur, sauf si ce dernier est un joueur professionnel qui exerce de façon habituelle cette activité dans un but commercial, en vue d'en retirer des profits. Il en va de même des personnes (bookmakers) qui sont impliqués dans l'organisation des jeux et des paris.*

Ce principe n'est pas remis en cause en cas d'opération de change entre *bitcoins* et une autre monnaie (celle notamment dans laquelle la comptabilité de l'entreprise est retracée).

Les règles de droit commun applicables en matière de monnaies étrangères[1] et de relations de prêt[2] sont par conséquent applicables en cas d'utilisation de monnaies virtuelles tels que les *bitcoins*.

Impôt sur le revenu

Les profits et les pertes d'une entreprise engendrés à raison de transactions portant sur les *bitcoins* doivent être retracés en comptabilité et sont soumis aux règles de droit commun applicables en matière d'impôt sur le revenu.

Plus-values imposables (*capital gains tax* ou « CGT » et impôt sur les sociétés)

Les autorités britanniques estiment que les règles actuelles en matière de plus-values, tant pour les particuliers que pour les professionnels (« *capital gains tax* » pour les personnes physiques ou « *chargeable gains* » pour les entreprises soumises à l'impôt sur les sociétés) permettent d'appréhender les gains réalisés sur les cessions de *bitcoins*.

Plus-values des professionnels

En principe, si un profit ou une perte à raison des transactions portant sur les *bitcoins* n'entraient pas dans la détermination du résultat courant de l'entreprise ou n'étaient pas dégagés dans le cadre d'une opération de prêts, ce profit ou cette perte auraient vocation soit à être soumis à l'impôt sur les sociétés en tant que plus-value ou moins-value[3], soit à être soumis à la « CGT » pour les entreprises individuelles (modalités identiques à celles applicables au particulier décrites ci-après, avec possibilité d'une taxation réduite à 10% notamment en cas de cession ou cessation d'activité[4].

Plus-values des particuliers

Rappel : l'imposition des plus-values des particuliers fait l'objet d'une imposition forfaitaire spécifique au taux de 28 % (ce taux est ramené à 18 % pour les personnes qui ne sont pas imposées à un taux supérieur au taux de base[5] de l'impôt sur le revenu).

[1] http://www.hmrc.gov.uk/manuals/cfmmanual/CFM61030.htm
[2] http://www.hmrc.gov.uk/manuals/cfmmanual/cfm30170.htm
[3] http://www.hmrc.gov.uk/ct/managing/company-tax-return/returns/chargeable-gain.htm#3
[4] http://www.hmrc.gov.uk/helpsheets/hs275.pdf
[5] *Pour un exemple de calcul :* http://www.hmrc.gov.uk/rates/cgt.htm.

Les gains nets ne sont soumis effectivement à l'impôt que pour la fraction de la plus-value qui excède 10 900 £ (5 450 £ pour les trustees qui ne sont pas en charge de personnes handicapées).

Par ailleurs, les cessions de biens personnels, en principe soumis à la « CGT », ne sont pas imposables lorsque leur valeur unitaire est inférieure à 6 000 £ [1].

[1] http://www.hmrc.gov.uk/cgt/possessions/basics.htm.

XI. RUSSIE

Q1/- Les monnaies virtuelles ont-elles fait l'objet de débats, de travaux (rapports, auditions publiques, etc.), de prises de position publiques ou politiques ? Avez-vous identifié des réflexions en cours sur le sujet ? Des think-tanks sont-ils actifs sur le sujet ?

Il n'y a pas de débats publics fournis, ni de publications d'envergure de think-tanks sur le sujet. Le *bitcoin* a fait l'objet de quelques articles de presse et de blog en début d'année 2014 en écho à la mise en avant du sujet au niveau mondial. Une conférence organisée par des acteurs de l'industrie des monnaies virtuelles et réunissant spécialistes russes et étrangers des monnaies virtuelles s'est tenue le 23 avril 2014 à Moscou devant une assemblée limitée (170 auditeurs).

Le sujet des monnaies virtuelles, notamment le *bitcoin*, fait surtout l'objet de réflexions au sein des organes régulateurs russes : Banque centrale de Russie (BCR), Ministère des Finances, Parquet général et organes de sécurité intérieure (FSB). Ces derniers échangent sur le sujet dans le cadre des réunions du « Groupe de travail interinstitutionnel pour la lutte contre les crimes économiques ».

Q2/- Les autorités publiques se sont-elles montrées plutôt favorables ou circonspectes sur les monnaies virtuelles, notamment le *bitcoin* ?

Les autorités publiques se sont montrées clairement circonspectes sur les monnaies virtuelles, notamment le *bitcoin*, concentrant leur analyse sur la possibilité d'utiliser ces dernières dans le cadre d'opérations illégales, notamment de blanchiment d'argent sale et de financement du terrorisme. Les autorités russes n'ont toutefois pas formellement interdit l'utilisation des monnaies virtuelles anonymes, en particulier le *bitcoin*, dans le pays.

Q3/- Certains acteurs des monnaies virtuelles mènent-ils un travail de lobbying auprès des institutions publiques (administrations, Parlement, régulateurs) ? Si oui, quels sont les arguments mis en avant ? Quelles sont leurs demandes ?

Il n'existe pas à notre connaissance de lobbying intensif auprès des institutions publiques de la part des acteurs des monnaies virtuelles.

Q4/- Les monnaies virtuelles font-elles l'objet d'une définition légale ? Des évolutions légales ou règlementaires sont-elles envisagées ? Si oui, préciser les principales dispositions.

Il n'existe pas de définition précise des monnaies virtuelles dans la législation russe. Cette dernière privilégie le terme assez vague de « moyens de paiement électroniques anonymes ».

La Banque centrale de Russie (BCR), le Parquet général, le Ministère des Finances et le FSB travaillent actuellement au renforcement i) de la définition du statut juridique des monnaies virtuelles, ii) de la réglementation concernant leur utilisation et iii) de la répression des infractions commises avec des monnaies virtuelles sans plus de précision (probable modification du Code Pénal).

Q5/- Les régulateurs sont-ils intervenus pour encadrer l'utilisation des monnaies virtuelles ? Les plateformes dédiées à l'utilisation de ces monnaies sont-elles soumises à des obligations spécifiques ?

Dans un communiqué publié le 27 janvier 2014, la Banque centrale de Russie (BCR) a indiqué que les personnes physiques et morales russes fournissant des services permettant l'utilisation de monnaies virtuelles pour les échanges de biens, de services ou d'argent (roubles et devises étrangères) seraient considérées comme « participants potentiels à des opérations illégales, notamment de blanchiment d'argent et de financement du terrorisme ».

La BCR a de plus rappelé que conformément à l'article 27 de la loi fédérale « *Sur la Banque Centrale de la Fédération de Russie* », l'émission de substituts monétaires est interdite sur le territoire de la Fédération de Russie. À l'issue d'une réunion le 6 février 2014, le Parquet général a à son tour rappelé qu'en vertu de la législation en vigueur « le rouble était la seule monnaie officielle en Russie et que l'émission d'autres unités monétaires ou de substituts était illégale ». Le Parquet général a en outre indiqué que « les moyens de paiement anonymes et les monnaies virtuelles, dont la plus célèbre d'entre elles, le *bitcoin*, étaient des substituts monétaires et ne pouvaient donc pas être utilisés par les personnes physiques ou morales ».

Q6/- Les administrations fiscales ont-elles pris position sur la nature des monnaies virtuelles et, partant, sur les conséquences fiscales qui y sont attachées ?

Pas à notre connaissance.

Q7/- Les autorités publiques ont-elles entrepris des actions d'information ou de prévention vis-à-vis des épargnants ou des consommateurs ?

Dans un communiqué publié le 27 janvier 2014, la Banque centrale de Russie (BCR) a condamné le caractère spéculatif des monnaies virtuelles, en particulier le *bitcoin*, et mis en garde les citoyens et les personnes morales russes, notamment les établissements de crédits, contre les risques liés à leur utilisation dans le cadre « *d'échanges de biens, de services ou d'argent (roubles et devises étrangères)* ». Au-delà des risques de pertes financières, la BCR a insisté sur la possibilité pour les personnes physiques et morales russes d'être, même involontairement, impliquées dans des opérations illégales, notamment de blanchiment d'argent et de financement du terrorisme.

Q8/- Constate-t-on une progression des investissements (publics ou privés) en matière de monnaies virtuelles ?

Il n'existe pas de statistiques fiables concernant l'utilisation de monnaies virtuelles, notamment le *bitcoin*, en Russie. Selon la presse, la Russie se classerait au 5e rang mondial en termes d'utilisateurs de *bitcoin* (près de 205 000).

XII. SINGAPOUR

Les autorités singapouriennes ne régulent pas les transactions en monnaie virtuelle en elles-mêmes, mais suivent avec intérêt l'évolution des transactions utilisant ce support et le développement des moyens d'échanges. À cet égard, l'administration fiscale (IRAS – *Inland Revenue Authority of Singapore*) a fourni en janvier dernier les clarifications nécessaires sur les règles de taxation des opérations impliquant des monnaies virtuelles. L'autorité monétaire de Singapour (MAS) a également annoncé en mars dernier qu'elle allait introduire des régulations sur les transactions en monnaie virtuelle afin de limiter les risques en termes de blanchiment et de financement du terrorisme. Bien que le statut juridique de ces nouveaux produits demeure flou, les autorités singapouriennes adoptent plutôt une attitude de laisser-faire vis-à-vis d'un marché qui pourrait croître rapidement dans la cité-État, tout en mettant en garde les utilisateurs face aux dangers potentiels de l'utilisation des monnaies virtuelles et en les incitant à la prudence.

Q1/- Les monnaies virtuelles ont-elles fait l'objet de débats, de travaux (rapports, auditions publiques, etc.), de prises de position publiques ou politiques ? Avez-vous identifié des réflexions en cours sur le sujet ? Des think-tanks sont-ils actifs sur le sujet ?

Les monnaies virtuelles ont fait l'objet d'une attention mesurée, en témoigne le peu de publications dans la presse singapourienne (à l'exception des récentes mesures annoncées par la MAS, voir Q5). Les évolutions qu'elles connaissent suscitent néanmoins des inquiétudes : ainsi, les parlementaires se sont interrogés sur l'environnement juridique des transactions en monnaie virtuelle et ont interrogé en février dernier l'autorité monétaire sur la nécessité de futures règlementations relatives à l'utilisation des monnaies virtuelles par les consommateurs singapouriens et les entreprises basées dans la cité-État. Ils ont également demandé à l'autorité monétaire de sensibiliser les Singapouriens aux risques liés aux échanges et aux investissements en monnaie virtuelle.

Q2/- Les autorités publiques se sont-elles montrées plutôt favorables ou circonspectes sur les monnaies virtuelles, notamment le *bitcoin* ?

Les autorités, si elles ne semblent pas particulièrement favorables au développement du *bitcoin*, hésitent encore entre laisser-faire et volonté de mieux contrôler les risques associés à ce marché par nature mal maitrisé. Si les autorités se sont engagées à ne pas règlementer pour le moment les transactions en monnaies virtuelles, elles envisagent de traiter l'aspect anti-blanchiment afin de préserver la réputation de la place financière de

Singapour. La MAS a indiqué en décembre dernier qu'elle n'interdirait pas aux commerçants d'accepter des paiements en monnaie virtuelles, mais elle semble surveiller de près les évolutions du marché. Reflétant cette volonté de laisser-faire, les autorités ne se sont pas opposées à l'installation des deux premiers distributeurs de *bitcoins* en Asie en février dernier (financées par la plateforme d'échange de *Bitcoin* Exchange).

Q3/- Certains acteurs des monnaies virtuelles mènent-ils un travail de lobbying auprès des institutions publiques (administrations, Parlement, régulateurs) ? Si oui, quels sont les arguments mis en avant ? Quelles sont leurs demandes ?

Pas à notre connaissance.

Q4/- Les monnaies virtuelles font-elles l'objet d'une définition légale ? Des évolutions légales ou règlementaires sont-elles envisagées ? Si oui, préciser les principales dispositions.

Le statut juridique des monnaies virtuelles demeure flou, même si les décisions récentes des autorités sont venues apporter quelques clarifications. L'autorité monétaire définit les monnaies virtuelles comme « des représentations numériques de la valeur qui peuvent être commercialisées sur internet et fonctionnent comme un moyen d'échange » ; .les monnaies virtuelles n'ont pas cours légal –leur acceptation en tant que moyen de paiement n'est donc pas garantie-, et ne sont pas considérées comme des actifs financiers (et donc ne rentrent pas dans le cadre juridique du *Securities and Futures Act*). De son côté, l'administration fiscale assimile les transactions en monnaies virtuelles à un échange de service.

Q5/- Les régulateurs sont-ils intervenus pour encadrer l'utilisation des monnaies virtuelles ? Les plateformes dédiées à l'utilisation de ces monnaies sont-elles soumises à des obligations spécifiques ?

L'autorité monétaire a annoncé en mars dernier son intention de réguler les intermédiaires permettant les transactions en monnaie virtuelle à Singapour, afin de limiter les risques liés au blanchiment d'argent et au financement du terrorisme. Si le détail des règles n'est pas encore connu, l'idée est d'imposer aux intermédiaires de monnaies virtuelles qui achètent, vendent ou facilitent l'échange contre des monnaies légales de vérifier l'identité de leurs clients et de signaler les transactions suspectes, sur le modèles des règles applicables aux bureaux de change. La MAS cite explicitement, parmi ces intermédiaires, les opérateurs de plateformes d'échange et de machines de ventes de *bitcoin*. En revanche, les points de vente qui acceptent des monnaies virtuelles en paiement de biens ou de services seront exclus du champ de cette régulation.

Q6/- Les administrations fiscales ont-elles pris position sur la nature des monnaies virtuelles et, partant, sur les conséquences fiscales qui y sont attachées ?

L'administration fiscale a clarifié en janvier dernier les règles de taxation des opérations impliquant les monnaies virtuelles. Elle assimile les monnaies virtuelles à une fourniture de service, et non une monnaie, ce qui se traduit notamment par les traitements suivants :

Pour l'application de la TVA (*Goods and Services Tax*) pour les entreprises qui y sont soumises[1] : l'utilisation par les entreprises de monnaies virtuelles pour l'achat d'un bien ou d'un service est considérée comme du troc, la transaction pouvant alors être taxée pour les deux biens échangés si les monnaies virtuelles sont utilisées pour payer un fournisseur local. La vente de monnaies virtuelles est considérée comme une vente de service, et est donc soumise à la TVA, sur la totalité de la transaction si l'entreprise vend/achète directement des monnaies virtuelles ou sur la commission uniquement si elle n'agit qu'en tant qu'intermédiaire (comme le font les plateformes d'échange). Les ventes de monnaies virtuelles à destination d'acteurs basés hors de Singapour ne sont pas soumises à la TVA locale.

Concernant l'imposition des sociétés (*Income tax*), les entreprises qui vendent/achètent des monnaies virtuelles sont imposées sur la base des gains réalisés, à l'exception notable des monnaies virtuelles acquises ou vendues à des fins d'investissement[2].

Q7/- Les autorités publiques ont-elles entrepris des actions d'information ou de prévention vis-à-vis des épargnants ou des consommateurs ?

L'organisme gouvernemental *MoneySENSE* a publié une alerte à destination des consommateurs sur les risques liés à l'utilisation des monnaies virtuelles. Les informations disponibles sur ce site internet s'accordent avec les déclarations de l'autorité monétaire, précisant que :

- les investissements en monnaie virtuelle ne sont pas garantis par les lois *Securities and Futures Act et Financial Advisers Act* ;

- les avoirs en monnaie virtuelle des consommateurs utilisant des opérateurs de plateforme d'échange (telles que *Liberty Reserve*, *WebMonay*, *Perfect Money*) ne sont pas protégés en cas de fermeture des plateformes ;

[1] *Obligatoire uniquement si le chiffre d'affaires est supérieur à 1 M SGD (environ 575 000 EUR).*
[2] *Dans ce cas, le bénéfice de la vente est considéré comme une plus-value et n'est donc pas imposés à Singapour, le pays n'avant pas de taxe sur les plus-values*

- les consommateurs ne sont pas en mesure d'obtenir un remboursement de leurs avoirs si le régime de monnaie virtuelle cessait de fonctionner.

Les utilisateurs doivent être conscients que la valeur des unités de monnaie virtuelle peut fluctuer de façon imprévisible dans un court laps de temps (par exemple la valeur du *bitcoin* aurait chuté de plus de 50 % en quelques heures au début du mois d'avril 2013).

Q8/- Constate-t-on une progression des investissements (publics ou privés) en matière de monnaies virtuelles ?

La plateforme d'échange en ligne *FYB*-SG, première plateforme de la sorte à Singapour, permet d'échanger de la monnaie virtuelle contre des SGD. Plus de 440 000 dollars de *bitcoin* ont été traités depuis sa mise en service en janvier 2013 et les investissements devraient progresser rapidement avec l'augmentation du nombre de commerçants de biens et services, encore marginaux dans la cité-État, acceptant d'être rémunérés avec ce moyen de paiement. À noter également que les infrastructures de marché se renforcent, avec la création depuis début 2013 de plusieurs plateformes d'échange, et l'installation récente des premiers distributeurs de *bitcoins*.

XIII. THAÏLANDE

Q1/- Les monnaies virtuelles ont-elles fait l'objet de débats, de travaux (rapports, auditions publiques, etc.), de prises de position publiques ou politiques ? Avez-vous identifié des réflexions en cours sur le sujet ? Des think-tanks sont-ils actifs sur le sujet ?

Ces dernières années en Thaïlande, l'intérêt porté par les médias et le public aux monnaies virtuelles, et le *bitcoin* en particulier, a été assez fluctuant. Un regain est apparu après la faillite et la fermeture, en février 2014, de *Mt. Gox*, la première plateforme mondiale de transaction et de stockage de *bitcoin*.

Quelques banques ont publié des travaux de recherche sur les monnaies virtuelles dans le but d'éduquer le grand public et de prévenir des risques associés.

En juillet 2013, la Banque de Thaïlande a déclaré que l'absence de régulation et de cadre juridique rendait la vente et l'achat de *bitcoins* illégaux, obligeant ainsi *Bitcoin Co. Ltd*, la première plateforme d'échange de *bitcoins* en Thaïlande, à suspendre ses activités en juillet 2013. En août 2013, *Bitcoin Co. Ltd* s'est transformée en site de minage.

Fin janvier 2014, la Banque de Thaïlande a statué que finalement, les opérations d'échange de *bitcoins* ne dépendaient pas des régulations du ministère des Finances, sauf dans le cas où des devises étrangères pouvaient être échangées. N'opérant qu'en baths, *Bitcoin Co. Ltd* a pu reprendre ses activités sur le territoire thaïlandais en février 2014.

Actuellement, le *bitcoin* ne peut donc être échangé qu'en devise locale (THB). L'échange en devises étrangères est interdit.

Le 18 mars 2014, la Banque centrale thaïlandaise a fait une déclaration précisant que les monnaies virtuelles n'ont pas cours légal dans ce pays.
En avril 2014, le comité des Finances, de la Fiscalité et de la Banque du Sénat a sollicité une consultation à la Banque centrale afin de débattre des monnaies virtuelles, leurs préoccupations concernant principalement la protection du consommateur.

Après plusieurs mois d'inactivité et une période de tests, la première plateforme d'échange de *bitcoins* en Thaïlande est à nouveau active (depuis le 20 mai 2014). Elle permet le transfert de bahts depuis des comptes basés en Thaïlande, ainsi que l'échange de plusieurs autres monnaies virtuelles (*litecoin*, *dogecoin*, *peercoin*, *feathercoin* et *zetacoin*).

Une seconde plateforme d'échange, *Coins (Thailand) Co. Ltd*, a également été légalisée le 20 juin dernier.

Il existe donc aujourd'hui en Thaïlande deux plateformes d'échange légales et réglementées, et au moins quatre plateformes d'échange non réglementées (qui ne sont pas gérées par des entreprises déclarées au registre du commerce) permettant l'achat et la vente de *bitcoins*.

Le *bitcoin* conserve le statut de « *commodity* » et non de monnaie ; les commerçants ne sont donc pas contraints de l'accepter comme moyen de paiement.

Pour information, *Bitcoin Co. Ltd* organise le 27 septembre 2014 la « *Thailand Bitcoin Conference 2014* » (http://bitcoin2014.in.th/)

Q2/- Les autorités publiques se sont-elles montrées plutôt favorables ou circonspectes sur les monnaies virtuelles, notamment le *bitcoin* ?

Les préoccupations de la Banque de Thaïlande sont liées principalement à la protection du consommateur.

Étant donné que les monnaies virtuelles ne sont pas largement utilisées en Thaïlande, une déclaration d'information et de mise en garde auprès de la population est, d'après la Banque de Thaïlande, suffisante et appropriée à ce stade. Cependant, elle n'exclut pas d'imposer ultérieurement, si nécessaire, une réglementation.

Le 30 avril 2014, le Bureau de lutte contre le blanchiment d'argent (*Anti Money Laundering Office*) a publié une circulaire destinée aux institutions financières pour réaffirmer leur obligation à strictement se conformer à la législation AML/CFT (*Anti-Money Laundering / Combating the Financing of Terrorism*) lorsqu'elles traitent avec des sociétés d'échange de *bitcoins*.

Ce bureau a également tenu une conférence de presse le 8 mai 2014 pour avertir le public des risques liés aux monnaies virtuelles.

Les autres autorités publiques n'ont pas encore manifesté d'intérêt particulier.

Q3/- Certains acteurs des monnaies virtuelles mènent-ils un travail de lobbying auprès des institutions publiques (administrations, Parlement, régulateurs) ? Si oui, quels sont les arguments mis en avant ? Quelles sont leurs demandes ?

La Banque de Thaïlande n'est pas informée de telles actions.

Q4/- Les monnaies virtuelles font-elles l'objet d'une définition légale ? Des évolutions légales ou règlementaires sont-elles envisagées ? Si oui, préciser les principales dispositions.

Les monnaies virtuelles n'ont, comme expliqué précédemment, pas cours légal en Thaïlande. Le *bitcoin* conserve le statut de « *commodity* » et non de monnaie.

Actuellement, étant donné le très faible développement des monnaies virtuelles en Thaïlande, la Banque centrale ne met pas en œuvre de régulation. Cependant, elle n'exclut pas d'imposer ultérieurement, si nécessaire, une réglementation.

Q5/- Les régulateurs sont-ils intervenus pour encadrer l'utilisation des monnaies virtuelles ? Les plateformes dédiées à l'utilisation de ces monnaies sont-elles soumises à des obligations spécifiques ?

Il n'y a pas de régulations particulières ou d'obligations pour ces monnaies en Thaïlande à ce jour mis à part le fait que le *bitcoin* ne peut être échangé qu'en devise locale (THB).

Q6/- Les administrations fiscales ont-elles pris position sur la nature des monnaies virtuelles et, partant, sur les conséquences fiscales qui y sont attachées ?

Comme indiqué précédemment, le *bitcoin* conserve en Thaïlande le statut de « *commodity* » et non de monnaie.

Q7/- Les autorités publiques ont-elles entrepris des actions d'information ou de prévention vis-à-vis des épargnants ou des consommateurs ?

Voir réponses 1 et 2.

Q8/- Constate-t-on une progression des investissements (publics ou privés) en matière de monnaies virtuelles ?

Comme développé dans la question 1, il existe seulement quelques sociétés en Thaïlande liées à l'achat, à la vente et à la création (minage) de *bitcoins* dont :

- 2 plateformes d'échange légales et réglementées ;

- au moins 4 plateformes d'échange de *bitcoins* non réglementées permettant l'achat et la vente de *bitcoins*, mais qui ne sont pas gérées par des entreprises enregistrées au registre du commerce.

- uniquement quelques commerçants, localisés majoritairement dans les zones touristiques, acceptent cette monnaie comme moyen de paiement.

La Banque de Thaïlande considère que pour l'instant, le nombre d'utilisateurs de ces monnaies est limité en Thaïlande.

AUDITION CONJOINTE DU 15 JANVIER 2014 SUR LES MONNAIES VIRTUELLES ET LE BITCOIN

Réunie le 15 janvier 2014 sous la présidence de M. Philippe Marini, président, la commission a procédé à l'audition conjointe de Mme Delphine d'Amarzit, chef du service du financement de l'économie de la direction générale du Trésor, MM. Denis Beau, directeur général des opérations à la Banque de France, Jean-Baptiste Carpentier, directeur du service Traitement du renseignement et action contre les circuits financiers clandestins (TRACFIN), Jean-Michel Cornu, directeur scientifique de la fondation Internet nouvelle génération (FING), Jean-Paul Garcia, directeur national du renseignement et des enquêtes douanières (DNRED), et Gonzague Grandval, président de Paymium SAS, sur les enjeux liés au développement des monnaies virtuelles de type *bitcoin*.

M. Philippe Marini, président. – Certains ont pu être surpris que nous décidions d'organiser l'audition de ce matin, mais il n'y a pas lieu de l'être : la commission des finances du Sénat, depuis 2008-2009, s'efforce d'approfondir sa compréhension des changements, souvent de très grande portée, liés à l'irruption du numérique dans la vie économique et financière. Nous avons pris ce sujet par différents angles, notamment fiscal. Nous avons ainsi été la première instance parlementaire à missionner un cabinet indépendant pour mieux comprendre les enjeux en matière de fiscalité des entreprises multinationales du numérique. Naturellement, la fiscalité n'est pas tout. Les considérations relatives à la politique monétaire, à la protection des opérateurs et des épargnants, à la sécurité du système financier sont également, parmi d'autres, des préoccupations qui peuvent être bousculées par l'évolution spontanée des technologies et des pratiques.

Nous pensons être dans notre rôle lorsque nous nous efforçons de creuser ce sillon. C'est ce que nous avons fait avec deux de nos collègues ici présents, Albéric de Montgolfier et Philippe Dallier, rapporteurs spéciaux de la mission « Gestion des finances publiques et des ressources humaines », qui nous ont présenté un rapport très concret, nourri de leurs contrôles sur pièces et sur place, sur le rôle des douanes dans la lutte contre la fraude sur Internet. Nous avons pu observer que, en la matière, ce n'est pas une petite faille, c'est un énorme fossé qui est en train de se créer. Tout ceci appelle des réponses à la fois organisationnelles et normatives au plan national et européen. De fait, ces problématiques liées à l'essor de l'économie numérique ont pour caractéristique de ne pas pouvoir être enfermées dans l'hexagone mais de devoir être traitées en conformité avec le droit communautaire, qui lui-même n'a qu'une vision partielle des choses.

Pour cette audition conjointe, j'ai le plaisir d'accueillir six intervenants :

- Mme Delphine d'Amarzit, chef du service du financement de l'économie de la direction générale du Trésor ;

- M. Denis Beau, directeur général des opérations à la Banque de France ;

- M. Jean-Baptiste Carpentier, directeur du service Traitement du renseignement et action contre les circuits financiers clandestins (TRACFIN) ;

- M. Jean-Michel Cornu, directeur scientifique de la fondation Internet nouvelle génération (FING) ;

- M. Jean-Paul Garcia, directeur national du renseignement et des enquêtes douanières (DNRED) ;

- M. Gonzague Grandval, président de Paymium SAS.

Pour lancer le débat, je me bornerais à citer un document adressé au Sénat américain en novembre 2013, dans lequel Ben Bernanke estime que les monnaies virtuelles sont « prometteuses à long terme pour autant qu'elles deviennent plus sécurisées ». C'est une formule très équilibrée, qui ne veut pas apparaître hostile à l'innovation mais qui reste soucieuse de sécurité !

Êtes-vous d'accord avec cette analyse ? Pensez-vous que l'essor des monnaies virtuelles est inéluctable ou bien qu'il s'agit d'une simple expérience qui n'a pas vocation à prendre de l'ampleur ?

En d'autres termes, il faut nous aider à nous situer dans ce monde nouveau. Nous ne pouvons plus faire semblant de gérer seulement les choses qui ne nous posent pas de problème conceptuel, alors que la réalité contourne les réglementations, la fiscalité et les régulations financières. La course est sans fin, sinon entre les gendarmes et les voleurs, du moins entre les entreprises et les autorités publiques.

M. Denis Beau, directeur général des opérations à la Banque de France. – Je soulignerai en introduction que le terme de « monnaie » ou « de moyen de paiement », appliqué aux *bitcoins* est largement un abus de langage pour des raisons à la fois économiques et juridiques.

En effet, selon une définition économique généralement admise, la monnaie est un actif qui remplit trois fonctions : unité de compte, instrument d'échange, réserve de valeur. Les *bitcoins* et autres dispositifs similaires ne répondent que très partiellement et imparfaitement à cette définition de la monnaie.

S'ils fournissent une unité de compte, leur fonction d'échange est limitée aux seuls commerçants, principalement sur Internet, ayant pris volontairement l'engagement, qu'ils peuvent remettre en cause à n'importe quel moment, d'accepter les *bitcoins* en règlement de biens et services.

Leur fonction de réserve de valeur est pour le moins incertaine : leur convertibilité en monnaie légale est aléatoire et leur valeur très fortement variable.

En outre, l'émission et la gestion de *bitcoin* ne relèvent pas du champ des moyens de paiement reconnus par notre code monétaire et financier, et en particulier de la monnaie électronique à laquelle on pourrait être tenté de les assimiler, car ils ne sont pas émis contre la remise de fonds. Ils ne bénéficient pas de ce fait d'une garantie de remboursement au pair dans la monnaie qui a cours légal, c'est-à-dire l'euro émis par les banques centrales de l'Eurosystème, ou dans les monnaies de banque qui lui sont strictement liées, c'est-à-dire celles émises par les institutions bénéficiant d'un statut d'établissement de crédit ou d'émetteur de monnaie électronique.

Du fait de l'apparition de plateformes permettant l'achat et la vente des unités de compte virtuelles comme le *bitcoin* contre de la monnaie ayant cours légal ou relié à elle, un nombre croissant d'utilisateurs peuvent acquérir ces unités de compte virtuelles. De plus, du fait de la faiblesse du coût d'utilisation de ces unités de compte virtuelles, certains pourraient être tentés d'y voir une alternative attractive aux monnaies et moyens de paiement dont l'émission et la gestion est régulée, en particulier pour régler des transactions sur Internet.

Une telle perspective ne peut laisser indifférent une banque centrale comme la Banque de France, chargée par le législateur de s'assurer de la sécurité des systèmes et des moyens de paiement, car elle pourrait conduire à une fragilisation de notre système de paiement du fait du développement des dispositifs les moins disant en matière de sécurité, source de risques pour leurs utilisateurs et pour notre économie de façon plus générale.

La sensibilisation des utilisateurs de monnaies virtuelles comme les *bitcoins* aux dangers associés à leur utilisation est donc particulièrement nécessaire et importante. C'est pourquoi la Banque de France a, comme d'autres banques centrales et autorités publiques en Europe, en Asie et aux Etats-Unis, publié le 5 décembre 2013 un document dans lequel elle souligne en particulier deux de ces dangers.

De par leur caractère anonyme, les monnaies virtuelles comme le *bitcoins* peuvent être utilisés pour contourner les règles relatives à la lutte contre le blanchiment des capitaux et le financement du terrorisme. Je laisserai sur ce point le soin aux intervenants suivants de développer cette problématique.

Les monnaies virtuelles comme le bitcoin font peser un risque financier fort sur les acteurs qui les détiennent. En effet, aucune autorité ne veille à la mise en place des conditions nécessaires pour assurer la sécurité des « coffres forts » électroniques qui permettent le stockage des unités de compte virtuelles tel que les *bitcoins*. Dans ce contexte, les détenteurs n'ont aucun recours en cas de vol de ces unités de compte par des pirates

informatiques, les « hackers ». En outre, leur convertibilité en monnaie ayant cours légal, nécessaire pour tirer les bénéfices d'une spéculation sur l'évolution de leur valeur, n'est pas garantie. Ainsi, les investisseurs ne peuvent récupérer leurs gains que si d'autres utilisateurs désirent acquérir les unités de compte virtuelles. Le système peut donc à tout moment s'effondrer lorsque les investisseurs veulent dénouer leurs positions mais se trouvent détenteurs d'avoirs devenus illiquides.

De ce fait, un commerçant ne pourra pas accepter de manière significative les paiements en unités de compte virtuelles sans s'exposer à des risques substantiels Il s'agit d'abord d'un risque de liquidité lié à la faible profondeur du « marché » d'achat/vente de ces unités de comptes en monnaie virtuelle contre une monnaie ayant cours légal ou liée strictement à celle-ci ; ensuite d'un risque financier lié à la volatilité du cours des monnaies virtuelles ; enfin, d'un risque opérationnel lié notamment à l'absence de garantie financière en cas de fraude.

Il en est de même pour les consommateurs. Ces derniers, qui disposent en réglant leurs transactions en euro des garanties associées aux moyens de paiement couverts par la directive concernant les services de paiement, notamment de remboursement en cas de paiement non autorisé, ne peuvent bien évidemment se prévaloir d'aucune garantie équivalente dans le cas d'utilisation de monnaies virtuelles.

Cette prise de conscience des caractéristiques et dangers liés à l'utilisation des monnaies virtuelles, qui n'en font pas de parfaits substituts à la monnaie légale et aux moyens de paiement scripturaux apparaît d'autant plus nécessaire qu'il existe aujourd'hui des solutions non seulement sûres mais également efficaces de paiement sur Internet. Je rappellerai à ce titre les efforts entrepris en France pour renforcer la sécurité des paiements par carte sur Internet par la mise en œuvre de dispositifs d'authentification renforcée (code unique bien souvent reçu par SMS pour valider le paiement), sous l'impulsion notamment de l'Observatoire de la sécurité des cartes de paiement, et désormais reconnue au niveau européen par le projet de révision de la directive sur les services de paiement et les recommandations du Forum européen sur la sécurité des moyens de paiement « Secure Pay ».

M. Philippe Marini, président. – Je vous poserais une question très simple : le *bitcoin* est-il de la fausse monnaie ?

M. Denis Beau. – Ce n'est pas une monnaie.

M. Gonzague Grandval, président de Paymium SAS. – Effectivement *bitcoin* n'est pas une monnaie, c'est avant tout une technologie, qui est libre et qui existe depuis plus de cinq ans. Elle a été spécifiée en 2008 et mise en activité en janvier 2009.

Plus précisément, c'est un protocole technique. C'est un réseau de transactions sur Internet complétement décentralisé, pair-à-pair (*peer-to-peer*)

et « *open source* ». C'est également une unité de compte qui circule sur ce réseau.

Parler de *bitcoin* en ne parlant que de l'unité de compte, c'est oublier la moitié du sujet, qui est le réseau de transactions électroniques. Il a d'ailleurs toujours été défini comme un système de paiement électronique et non comme une monnaie.

Ce système a de la valeur pour deux raisons. D'une part, il existe avec un nombre d'utilisateurs important, avec une puissance de calcul informatique également très importante, avec une résilience forte et une sécurité qui s'accroît de jour en jour. D'autre part, l'une des caractéristiques de l'unité de compte *bitcoin* est d'être émise en quantité limitée. Le *bitcoin* est donc rare et pourrait être assimilé à une action du réseau *bitcoin*. C'est un statut un peu hybride.

Les paiements électroniques peuvent être opérés de trois manières différentes. Le système classique, par carte bancaire, met en présence quatre acteurs : le marchand et l'acheteur, ainsi que leurs deux banques. Ce système de paiement est fondé sur le prélèvement du montant à payer sur le compte de l'acheteur. Il est susceptible de générer des fraudes puisque l'acheteur est obligé de révéler l'ensemble des informations bancaires pour procéder aussi bien à un paiement de 5 euros que de 1 000 euros.

Il existe également un système à trois acteurs, privatif, de type American Express, où l'intermédiaire financier est à la fois le prestataire du marchand et de l'acheteur.

Enfin, on trouve les systèmes de pair-à-pair : le marchand est directement en relation avec l'acheteur. *Bitcoin* est le premier véritable réseau de pair-à-pair sans tiers de confiance au milieu. La confiance est distribuée à l'ensemble des participants au réseau.

Je voudrais souligner que le protocole *bitcoin* étant libre, l'ensemble de la technologie appliquée est auditable par tout le monde et cela depuis cinq ans. On peut donc dire que la technologie est extrêmement sûre et fiable. Je ne m'attarde pas sur ces aspects techniques.

En tant que technologie innovante, nous, *Paymium*, assimilons *bitcoin* à Internet, le courriel ou encore la voix sur IP. En leur temps, ces technologies, libres, ont été beaucoup décriées et ont bouleversé de nombreuses habitudes. *Bitcoin* est le premier protocole libre en matière de paiement électronique. Ce doit être un élément suffisant pour considérer que cette technologie est à l'origine d'opportunités importantes dans le domaine du paiement, comme le courriel l'a été dans le domaine des télécommunications.

Il existe aujourd'hui plusieurs moyens de paiement électroniques, tels que *Paypal*, *Paylib*, *Buyster*, etc. qui ont un point en commun, à savoir celui d'être privatifs. Si vous êtes porteur d'un moyen de paiement *Paypal* ou

Buyster, vous ne pouvez pas payer sur un moyen différent de celui que vous possédez. Et pourtant, vous parlez de la même monnaie, vous êtes dans le même pays et vous disposez des mêmes banques. Dès lors, l'accès à ces moyens de paiement est limité et leur développement semble voué à l'échec.

Il y a trente ans, en France, a été créé le Groupement Carte Bancaire, qui a eu un mérite, unique dans le monde entier, celui de développer l'usage de la carte bancaire grâce à l'interbancarité. On ne se pose pas la question de savoir si, en tant que client d'une banque, on peut payer chez un marchand dont le compte est ouvert dans une autre banque. Réaliser un tel groupement dans le cadre des paiements électroniques serait un effort insurmontable pour le concrétiser à l'échelle au moins européenne.

Pour promouvoir l'interopérabilité des moyens de paiement, il faut s'adosser à des technologies libres pour que tout le monde soit d'accord sur la technologie utilisée. *Bitcoin* peut être cette technologie et nous le considérons comme une passerelle et comme un moyen d'interopérabilité entre les moyens de paiement au bénéfice des porteurs et des marchands, mais aussi des banques et des tiers de confiance qui vont pouvoir construire des solutions adossées à ce protocole.

Pour finir, je voudrais parler de *Bitcoin-Central*, qui est le cœur de l'activité de *Paymium*. Il s'agit d'une place de marché sur laquelle des acheteurs et des vendeurs peuvent acquérir ou vendre des *bitcoins* contre des euros, ou inversement. Elle fonctionne en partenariat avec un établissement de paiement, organisme agréé par la Banque de France, autorisé à effectuer des activités de paiements électroniques. Il réalise la tenue de compte de nos clients, en euros, dans le respect des règles prudentielles de connaissance des clients, et ce dès le premier centime d'euro sur chacune des transactions.

La sécurité, chez *Bitcoin-Central*, est un point majeur et nous pratiquons un stockage des *bitcoins* de nos clients totalement en dehors du réseau. Notre territoire, c'est l'Europe car il n'existe pas de marché français. Le marché est majoritairement américain puis nord-européen. En France, il est le moins développé des pays européens. Il est de notre devoir de faire croître notre activité partout en Europe pour créer un acteur majeur dans le domaine du paiement électronique, qui s'appuierait sur une réglementation française et européenne depuis l'origine.

M. Philippe Marini, président. – A-t-on une idée du volume des transactions annuelles en France sur cet instrument ?

M. Gonzague Grandval. – Les utilisateurs français de *bitcoins* ne sont pas cantonnés à la France. En tant qu'opérateur, nous avons une idée de l'activité sur notre place de marché. En revanche, il est difficile d'estimer le volume d'activité en France à proprement parler. Il me paraît néanmoins important de souligner que les utilisateurs français de *bitcoins* ne cantonnent pas un tel usage à la France. Au contraire, actuellement, ils l'utilisent

majoritairement dans des pays étrangers. Toutefois, on assiste à un intérêt croissant des marchands français pour le *bitcoin*.

M. Philippe Marini, président. – Vous nous parlez de *Bitcoin-Central*, de l'architecture du système, du réseau. Il y a sans doute des moyens puissants permettant à tout cela de fonctionner. À qui cela appartient-il ? À qui cela rapporte-t-il ?

M. Gonzague Grandval. – Le système lui-même n'appartient à personne d'autre qu'à ses utilisateurs. La valeur du réseau est uniquement fondée sur le nombre d'utilisateurs et l'usage qu'ils font de ce réseau.

M. Philippe Marini, président. – Vous dites que cela n'appartient à personne mais les profits appartiennent aux grands opérateurs internationaux qui utilisent ces canaux. Ce n'est pas du bénévolat !

M. Gonzague Grandval. – Les profits liés au réseau *bitcoin* à proprement parler viennent uniquement servir les processeurs du réseau *bitcoin*, c'est-à-dire des pairs dans le réseau de pair-à-pair. Ce sont des profits internes au réseau. En revanche, sur ce réseau se constituent des activités commerciales comme la nôtre, qui ont effectivement vocation à générer des profits.

M. Jean-Michel Cornu, directeur scientifique de la fondation Internet nouvelle génération. – Depuis trois ans, ma fondation a réalisé des travaux sur l'innovation monétaire, avec l'aide d'une centaine de personnes : des banquiers, des économistes, des innovateurs ou de simples citoyens. Nous avons cherché à comprendre quelles en sont les opportunités et les risques. On crée actuellement de la valeur par l'innovation. Il existe plusieurs types d'innovations, et l'innovation technologique n'est pas suffisante aujourd'hui. Dans ce contexte, l'innovation économique, dont fait partie l'innovation des mécanismes de type monétaire, présente des opportunités pour développer d'autres types d'innovations, mais également des risques.

Par rapport à cette problématique générale, je pense qu'il convient de distinguer plusieurs catégories et je vais m'efforcer d'élargir quelque peu le propos, au-delà du *bitcoin* et des monnaies virtuelles. En effet, il existe en réalité un certain nombre de monnaies dites complémentaires : il y a tout d'abord les monnaies non économiques, tels que les fameux systèmes d'échanges locaux (SEL), qui posent un certain nombre de questions déjà abordées dans le cadre de plusieurs instances ; il y a, ensuite, les monnaies de réputation (*twollar*, *exploracœur*), qui facilitent le fonctionnement des réseaux sociaux et ont donc un impact monétaire limité. Dans cette catégorie, je citerai également, plus récemment, les « donnaies », qui sont destinés à faciliter les dons.

Ce qui nous intéresse ici, ce sont les mécanismes monétaires ayant trait aux échanges, notamment commerciaux : on peut citer à cet égard les monnaies locales complémentaires, dont le champ d'échange est limité à un

territoire (Sol-Violette à Toulouse, Heol à Brest), ou les monnaies affectées, qui, elles, ne se restreignent pas au territoire mais à l'usage que l'on en fait. Ainsi, à Curitiba, au Brésil, il existe une monnaie que l'on ne peut gagner qu'en triant ses déchets, et qu'on ne peut dépenser qu'en prenant les transports en commun. Cette petite monnaie, qui représente l'équivalent d'une masse monétaire insignifiante, a permis la réalisation de transformations énormes et d'économies gigantesques au point que Curitiba est devenue la capitale verte du Brésil. Cet exemple démontre que l'impact de ce type de monnaies ne relève pas seulement de la masse monétaire.

Enfin, il y a les monnaies alternatives, qui ne se limitent pas seulement à l'échange, mais revêtent des aspects économiques comme investir, prêter ou spéculer. Dans cette catégorie, on peut citer des monnaies anciennes comme le *wir* suisse, monnaie qui permet de maintenir les échanges en période de crise. Elle existe depuis 1933 et représente 25 % des PME suisses, soit 90 000 PME. On dit que c'est une monnaie facile à gagner, mais plus difficile à dépenser. Par exemple, aujourd'hui, vous pouvez acheter votre maison en *wir*, avec une particularité : il n'y a pas de conversion possible, contrairement au *bitcoin*. Un *wir* égale un franc suisse, mais il est absolument impossible de le convertir : il s'agit donc d'un système monétaire totalement autonome. On peut, à cet égard, citer d'autres systèmes : le SCEC en Italie ou le *solidario* en Argentine. Cette dernière monnaie a eu un impact assez marginal jusqu'à la crise, au cours de laquelle elle a permis à de nombreuses personnes de survivre, avant de redevenir, par la suite, un épiphénomène.

Le caractère virtuel a permis de faciliter le développement de ce type de monnaies, certaines étant plus nouvelles, intéressantes et innovantes comme le *bitcoin* ou *OpenUDC*.

Je vais vous proposer trois critères pour essayer d'analyser et d'apprécier les risques et opportunités associés à l'innovation monétaire. Ces trois critères sont :

- le poids de la masse monétaire : par exemple, si l'on interdit ces monnaies, il n'y aura pas d'innovation, mais cela pose-t-il un problème du point de vue de la politique monétaire ?

- la transparence, au-delà de la question du blanchiment, c'est-à-dire la question de la taxation et du financement de la collectivité : sans transparence, on rencontrera des difficultés pour financer la collectivité. Quel est le niveau de transparence adéquat ?

- la dérive spéculative : la spéculation est une bonne chose – spéculer veut dire prévoir – mais lorsque la spéculation sur la monnaie devient supérieure à celle sur les biens, on peut avoir des problèmes, qui concernent aussi bien les monnaies virtuelles que les monnaies classiques. L'autre aspect de la dérive spéculative tient à la question du change et de l'instabilité qui peut exister entre les différentes monnaies.

S'agissant plus particulièrement du *bitcoin*, monnaie virtuelle et décentralisée, la masse monétaire doit être limitée, à terme, à 21 millions de *bitcoins*. Les quatre premières années, il y avait 2,6 millions de *bitcoins* créés par an. À partir de cette année, seuls 1,3 million de *bitcoins* seront créés par an, pour les quatre ans à venir. Concrètement, quelle valeur représente le *bitcoin* ? Actuellement, début janvier 2014, il y a environ 12 millions de *bitcoins* en circulation, pour une valeur de l'ordre de 7 milliards d'euros au cours actuel sur l'ensemble de la planète, soit 0,3 pour mille du PIB français. C'est à la fois beaucoup et peu.

La deuxième question qui se pose tient au fait que cette valeur de masse change en fonction du cours du *bitcoin*. Le cours d'introduction du *bitcoin*, en 2009, était de 80 millions d'euros. On estime que, fin 2014, il atteindra 10 milliards d'euros. Mais il est difficile de connaître sa valeur en 2040, date à laquelle plus aucun nouveau *bitcoin* ne sera créé. Au total, l'impact du *bitcoin* sur le poids de la masse monétaire demeure encore insignifiant mais pourrait ne plus l'être et doit donc être surveillé.

En ce qui concerne la transparence, l'échange de pair-à-pair crypté concerne les utilisateurs qui achètent et vendent des *bitcoins*. Mais les transactions elles-mêmes sont actuellement transparentes et ouvertes. En conséquence, du point de vue du blanchiment, se pose la question de savoir qui émet la monnaie et qui la reçoit. En termes de taxation et de financement de la collectivité, ne connaissant pas les destinataires, on ne peut savoir dans quel pays instaurer la taxation. C'est une difficulté à laquelle on se heurte de plus en souvent dans le monde de l'Internet : la taxation est nationale, tandis que les outils, protocoles et innovations sont de plus en plus internationaux.

Sur la dérive spéculative, j'insisterai sur deux points : d'une part, dans la mesure où l'on produit de moins en moins de *bitcoins*, c'est une monnaie rare. En 2009, au moment de sa création, il y avait toutes les dix minutes 50 *bitcoins* affectés, au hasard, à celui dont l'ordinateur faisait le calcul pour les autres. Désormais, on ne reçoit plus que 25 *bitcoins* toutes les dix minutes. Les premiers entrants sont donc favorisés par rapport aux nouveaux entrants. Il y a un débat actuellement pour savoir s'il s'agit d'une chaîne de Ponzi ou non, à savoir un montage financier frauduleux qui consiste à rémunérer les investissements des clients essentiellement par les fonds procurés par les nouveaux entrants.

Le second point important à retenir est que le *bitcoin* n'est pas un système fermé sur lui-même, mais un système qui permet la convertibilité. Il y a donc des bourses et des places de marché et l'on peut effectuer des virements sécurisés.

Enfin, pour terminer, je citerai un chiffre : l'inflation de la valeur du *bitcoin* par rapport à l'euro est de 900 % en 2013 ou de 610 % entre le 17 septembre 2013 et le 14 janvier 2014. On constate donc que la valeur du *bitcoin* augmente par rapport à l'euro, tandis que le nombre de *bitcoins*

diminue dans le temps. Il faut garder à l'esprit ces aspects du point de vue de l'analyse du risque de dérive spéculative.

En conclusion, j'estime que nous avons absolument besoin d'innovation, mais que l'innovation technologique ne suffit plus ; de même, l'innovation de services est nécessaire mais il faut aller plus loin. L'innovation économique, à travers les nouveaux modes de financement comme le financement par la foule, ou les mécanismes monétaires innovants, est donc elle aussi indispensable, mais il nous faut des critères, tels que ceux que j'ai proposés, pour analyser les meilleures innovations.

M. François Marc, rapporteur général. – Le sujet des monnaies virtuelles est d'une extrême importance. Gonzague Grandval a évoqué tout à l'heure le développement des cartes bancaires, il y a de cela plus de trente ans. Quiconque se penchant sur ce sujet constatera qu'il y avait, à l'époque, de grandes réticences à l'utilisation élargie et systématisée des cartes bancaires, voire des résistances. Dans notre pays, beaucoup de commerçants refusaient les paiements par carte bancaire. Cet exemple montre que l'innovation liée aux actes de paiement pose assez naturellement des problèmes. Ceci est conforté aujourd'hui par l'existence de dérives et de spéculations.

Malgré ces interrogations, j'ai le sentiment que cette innovation apporte une réponse positive. La théorie économique nous enseigne en effet que la diminution des coûts de transaction tend à créer une dynamique économique porteuse d'avenir.

Toutefois, certains estiment que le *bitcoin* serait « la monnaie des mafias ». Dès lors, les trois intervenants qui vont suivre pourraient nous éclairer : pourquoi et comment cette technologie est utilisée pour le blanchiment d'argent ou pour les transactions de drogue ou d'armes ? Le *bitcoin* a-t-il permis le développement des trafics ou bien s'est-il substitué aux monnaies que nous connaissons ? Outre le *bitcoin*, il existe d'autres monnaies virtuelles, plus confidentielles, spécialement développées dans le but de servir au blanchiment ou à des activités criminelles ; le *bitcoin* est-il l'arbre qui cache la forêt ?

Le Trésor pourrait-il nous éclairer sur les réflexions en cours sur le sujet du *bitcoin* en France et en Europe ? Nous constatons en effet que les Etats ont adopté des attitudes fort différentes vis-à-vis du bitcoin : la Chine a mis en place un contrôle très étroit de l'utilisation de cet outil, la Thaïlande l'a interdit et l'Allemagne lui a reconnu un statut légal.

En définitive, comment la législation française – en particulier la législation fiscale et financière – peut-elle évoluer ? Par exemple, doit-on déclarer ses *bitcoins* au titre de l'impôt sur la fortune (ISF) ? En cas de vente d'un objet contre *bitcoin*, faut-il lui appliquer la TVA ? Si une start-up pratique le change *bitcoin* contre euro, doit-elle adopter le statut d'agent de change ?

Il est donc nécessaire d'avoir une meilleure compréhension des ressorts de ces nouveaux dispositifs, afin d'estimer comment la régulation doit opérer dans ce domaine.

M. Philippe Marini, président. – Je partage totalement les interrogations du rapporteur général. Je rappelle que, selon la Banque de France, une action judiciaire conduite par le *Federal Bureau of Investigation* (FBI) a été engagée contre des fournisseurs de plateforme de conversion soupçonnés de blanchiment d'argent et de fraude fiscale. Le 2 octobre 2013, les autorités américaines ont ainsi fermé le site Internet « *Silk Road* » – site d'acquisition de produits narcotiques en ligne – sur lequel s'échangeait une importante partie des *bitcoins* en circulation.

M. Jean-Paul Garcia, directeur national du renseignement et des enquêtes douanières. – Je vous remercie, monsieur le président, d'avoir introduit mon propos en citant l'affaire « *Silk Road* ». En décembre 2013, une affaire analogue – même si elle impliquait un service infiniment plus petit et une cible infiniment plus humble – s'est fait jour en France. La cellule « Cyberdouane », placée au sein de la direction nationale du renseignement et des enquêtes douanières (DNRED), a procédé – avec l'assistance de *Paymium* – à l'arrestation d'un trafiquant de stupéfiants sur Internet, qui se faisait payer en *bitcoins*. Concrètement, la DNRED a acheté des *bitcoins* et a procédé ensuite à l'achat d'une petite quantité de stupéfiant ; ce moyen de paiement nous a ensuite permis de tracer la marchandise afin d'intervenir dans les locaux de ce trafiquant, qui était un excellent « geek ». Il avait ainsi perçu tout l'intérêt de travailler de cette manière avec du *bitcoin*. Aujourd'hui, cette personne est mise en examen et le relais est passé à la police judiciaire.

Toutefois, du point de vue de la DNRED, le principal risque porte aujourd'hui sur les trafics de monnaie en espèces. Le sujet des monnaies virtuelles, et spécialement le *bitcoin,* relève, selon moi, de l'avenir et de l'anticipation. La volatilité de ces monnaies présente un risque trop important pour les dirigeants de grandes opérations de fraude – qui ne sont pas encore familiarisés avec ces technologies. Mais il est important de mieux anticiper sur ce sujet. Dans ce but, nous investissons beaucoup dans la connaissance des monnaies virtuelles. A cet égard, nous ne pourrons entrer dans ces dispositifs que par le biais d' « échangeurs » tel que *Paymium*, qui permettent d'échanger, de stocker et de fournir ces *bitcoins*.

M. Philippe Marini, président. – Comme vous le savez, le Sénat a très largement joué son rôle en ce qui concerne les moyens d'enquête et d'investigation, notamment dans le cadre de la dernière loi de finances rectificative. Nous sommes très conscients de la nécessité de ne pas désarmer l'Etat au moment où les risques sont particulièrement préoccupants.

M. Jean-Baptiste Carpentier, directeur du service Traitement du renseignement et action contre les circuits financiers clandestins (TRACFIN). – Je vais avoir sur le sujet un propos prudent et – je ne le

dissimule pas – légèrement inquiet. Il est difficile de parler des monnaies virtuelles en général : la problématique du *bitcoin* n'est pas la problématique du « *liberty reserve* », ni celle des systèmes d'échanges locaux. Il y a toutefois une caractéristique commune : ce sont des systèmes qui se sont inscrits en parallèle du monopole de fait de la monnaie légale, qui est émise par les autorités centrales. Ces systèmes parallèles étaient souvent des épiphénomènes limités, qui ne soulevaient pas de difficulté et qui étaient parfois même très sympathiques, à l'instar des monnaies locales ; ces systèmes sont souvent nés dans les communautés de *gamers*, de joueurs de jeux vidéo. Mais depuis plusieurs années, nous voyons émerger de véritables monnaies virtuelles, au-delà de ces cercles fermés de ces communautés virtuelles. TRACFIN a été parmi les premiers services à s'intéresser à ces questions : je vous renvoie à notre rapport annuel 2011, où nous avons appelé l'attention des différentes autorités sur ces problématiques. Nous animons actuellement un groupe de travail qui réunit les pouvoirs publics concernés, afin d'en comprendre les évolutions – qui sont extrêmement rapides.

Nous sommes relativement inquiets. Depuis 1990, l'ensemble des pouvoirs publics internationaux, sous l'égide notamment du Groupe d'action financière (GAFI), a mis en place un ensemble extrêmement complet de règles de contrôle et de normes et transparence des opérations financières, qui s'imposent aux fournisseurs de services de paiement. L'idée générale était celle d'une surveillance accrue des flux de capitaux, en contrepartie de leur libéralisation. Or l'émergence des monnaies virtuelles fait aujourd'hui apparaître un « trou noir » dans cette régulation : nous ne sommes pas dans l'illégal, mais dans l'*a-légal*. Les problématiques vont au-delà de la lutte contre le blanchiment. Vous avez notamment évoqué les problématiques fiscales : quel est le statut d'un compte en *bitcoins* ? Cela a-t-il le moindre sens de parler d'un compte détenu à l'étranger ? Quel est le statut de l'impôt sur la fortune (ISF) et de la TVA ? Comment enregistre-t-on en comptabilité une transaction en *bitcoins* ou en « *liberty reserve* » ? Quelles sont les obligations de vigilance des établissements et les questions que le banquier devra poser ? Comment assurer l'équité concurrentielle avec les acteurs soumis à la régulation, qui supportent de ce fait un certain nombre de coûts ? Peut-on envisager qu'un monde *a-régulé* puisse se dispenser de ces coûts ? Ce sont des questions auxquelles je ne me permets pas de répondre – c'est là le rôle des autorités ministérielles et du Parlement.

C'est un monde dans lequel nous voyons extrêmement peu de choses. Le dispositif de contrôle des flux financiers fonctionne comme le contrôle de la vitesse sur les routes, avec des radars fixes et des radars mobiles : nous avons des radars sur certaines routes, mais il existe des routes parallèles sur lesquelles nous n'en avons pas. Je suis incapable de vous dire s'il y a ou pas des excès de vitesse. De temps en temps, nous avons tout de même eu à connaître de sujets qui touchent, directement ou indirectement, à la monnaie virtuelle. Ces sujets sont en cours d'examen par TRACFIN et

certains ont été transmis à l'autorité judiciaire. Par ailleurs, nous sommes en lien assez étroit avec nos homologues étrangers, qui sont pour certains en avance sur nous, et commencent à manifester une réelle inquiétude sur cette « économie ignorée » des monnaies virtuelles – laquelle a probablement dépassé le stade seulement anecdotique où nous nous trouvions encore il y a quelques mois… mais sans pour autant porter des enjeux macroéconomiques.

M. Philippe Marini, président. – Nous espérons toutefois pouvoir aller un peu plus loin que le stade des questions. La synthèse est délicate : soit l'on apparaît comme hostile à l'innovation, et l'on est alors voué aux gémonies du monde d'aujourd'hui, soit l'on adopte une approche libérale, mais au risque de tomber dans tous les travers qui ont été évoqués.

Mme Delphine d'Amarzit, chef du service du financement de l'économie de la direction générale du Trésor. – L'une des questions non tranchées est la suivante : y a-t-il un intérêt spécifique des monnaies virtuelles en termes de coûts de transaction ? Elles imposent de moindres frais de transaction, mais en contrepartie les utilisateurs doivent supporter d'autres types de coûts, notamment en matière de sécurité informatique. Le développement du marché nous dira s'il existe un véritable risque de concurrence avec les moyens de paiements traditionnels au sens du code monétaire et financier, ceux que les commerçants ne peuvent pas refuser. Au-delà de l'aspect libertarien des monnaies virtuelles, il existe aussi un intérêt pour les personnes qui auraient des choses à cacher.

Ensuite, le caractère spéculatif du *bitcoin*, lié à sa rareté et au déséquilibre entre l'offre et la demande, limite en fait son développement. C'est le paradoxe : c'est en partie à cause de sa volatilité que le *bitcoin* n'est pas une menace pour la stabilité financière aujourd'hui, parce que son développement est limité.

Du point de vue des pouvoirs publics, le développement des monnaies virtuelles implique de faire comprendre aux utilisateurs les risques inhérents à leur volatilité, à leur non-convertibilité, à leur exposition au piratage, *etc.* Une sensibilisation a déjà été menée par l'Autorité bancaire européenne (ABE), notamment par une alerte en décembre 2013. Mais c'est un autre paradoxe : plus nous allons clarifier et avertir, plus nous allons permettre la diffusion de ces monnaies virtuelles.

Une interdiction absolue est difficile à concevoir en tant que telle, dans la mesure où elle viserait une activité relevant du troc entre personnes privées et selon des modalités libres. En revanche, il est possible d'imposer des obligations, notamment au niveau du « lieu de rencontre » entre ces monnaies virtuelles et la monnaie légale. Ainsi, une décision de justice a récemment confirmé que les plateformes proposant de convertir des monnaies virtuelles en euros sont tenues d'avoir la qualité de prestataires de services de paiement. Cela ne permet toutefois pas de couvrir l'intégralité

des transactions en *bitcoins*, certaines pouvant être réalisées de gré à gré, sans l'intervention d'un tiers et sans conversion.

Enfin se pose la question du risque de blanchiment. Les techniciens pensent que la traçabilité des transactions en *bitcoins* est possible. Mais quelle est l'utilité de la traçabilité des flux si l'on ne connaît pas l'identité des personnes qui en sont à l'origine ? Là encore, l'intervention des prestataires de services de paiement et des établissements teneurs de compte constitue une piste.

Ces questions sont débattues au niveau international. Les lignes directrices du GAFI mériteraient probablement d'être repensées. Au niveau national, le Trésor participe au groupe de travail mentionné par Jean-Baptiste Carpentier. Sur le plan fiscal, des travaux sont en cours en lien avec la direction de la législation fiscale (DLF). J'y ajouterai d'ailleurs la question du revenu des « mineurs », qui génèrent les *bitcoins* en contribuant au fonctionnement du système et à la sécurité des transactions.

M. Albéric de Montgolfier. – Nous avons avec Philippe Dallier produit un rapport sur le rôle des douanes dans la fiscalité du commerce électronique. Nous nous sommes notamment rendus à la cellule de veille sur Internet « Cyberdouane », où nous avons vu le fonctionnement du logiciel Tor, qui permet d'accéder à des plateformes illégales de type « *Silk Road* », où l'on trouve des rubriques « drogue », « armes » ou encore « assassinats ». Tous les paiements s'y faisaient en *bitcoins*, ce qui nous a fait douter du caractère vertueux de cette monnaie… Une autre question porte sur le nombre d'utilisateurs du *bitcoin* : pouvez-vous confirmer que seulement 500 personnes physiques, soit un très petit nombre de personnes, détiennent la moitié des *bitcoins* en circulation ?

M. Richard Yung. – Rejoignant le rapporteur général, je considère qu'il faut souhaiter la bienvenue à l'innovation. Il s'agit d'un secteur nouveau qu'il nous faut mieux comprendre. À cet égard, la France semble en retard, ce qui n'est pas nouveau : *Paypal*, par exemple, n'est pas installé en France, même si des initiatives récentes des banques françaises essaient de s'en inspirer. Il ne faut pas rater les nouvelles possibilités, surtout si cela permet de diminuer les coûts de transaction.

S'agissant des activités illégales, elles existent mais ne sont pas liées à la nature du produit : elles sont malheureusement présentes pour tout moyen de paiement, qu'il s'agisse du chèque ou, bien sûr, du liquide.

Vous parlez d'un système *a-légal*. Ce n'est pas nouveau : on en voit un exemple dans le monde bancaire et financier avec le système financier parallèle qui, sans être illégal, échappe à la régulation. Pour éviter les abus, il faut fournir un encadrement. C'est pourquoi je voudrais savoir quels sont vos besoins de réglementation, car le Sénat a toujours répondu présent lorsqu'il s'est agi de fournir des outils de régulation financière.

Par ailleurs, pourquoi la France est-elle, selon vous, aussi peu active dans ce domaine et en retard par rapport aux autres pays de l'Union européenne, où il n'y a d'ailleurs pas d'approche commune ?

M. Jacques Chiron. – Vous avez souligné la rareté du produit, puisque seuls 50 *bitcoins* sont émis toutes les dix minutes, et seulement 25 à compter de cette année. Sont-ce les programmateurs, à l'origine du produit, qui organisent cette rareté ? Quelle spéculation cette rareté organisée permet-elle, surtout s'il y a un nombre limité de mineurs ?

M. Philippe Adnot. – Je voudrais connaître le nombre de mineurs qui participent au réseau. Pour que l'Allemagne taxe les plus-values, je suppose qu'il faut qu'elle ait connaissance des transactions et des volumes.

M. François Marc, rapporteur général. – Je constate que les intervenants eux-mêmes posent beaucoup de questions, sans avoir nécessairement toutes les réponses à ce stade. Je suis curieux de connaître les réactions de Gonzague Grandval qui est appelé à la défense de ce système. J'ai le sentiment, quant à moi, que nous sommes au début d'un processus et que l'innovation peut être porteuse d'avenir ; dans le même temps, le souci de régulation, que porte le Parlement, est évident dès lors que le système est *a-légal*.

Grâce aux radars routiers, le nombre de morts sur la route a été divisé par cinq en quinze ans : de même, comment assurer une surveillance des transactions, et à quel coût, pour des systèmes aussi décentralisés ?

Par ailleurs, existe-t-il un acteur, je pense par exemple à la *Bitcoin Foundation* aux Etats-Unis, qui serve ou puisse servir de référent aux autorités ? Y a-t-il un pilote dans le système *bitcoin* ?

Enfin, ne devrait-on pas donner rapidement un statut légal à certaines monnaies virtuelles, dont le *bitcoin*, afin de mieux de les réguler ?

M. Philippe Marini, président. – Pourquoi l'Union européenne, si féconde en réglementation, n'est-elle pas en train d'élaborer des règles du jeu sur ce sujet ?

Par ailleurs, comment un système aussi décentralisé peut-il avoir un seul cours ? Qui fixe le cours, et comment ? Y a-t-il un référent, ou une connexion entre les différentes plateformes de change, ou y a-t-il des écarts entre ces plateformes donnant lieu à des possibilités d'arbitrage ?

M. Gonzague Grandval. – Le réseau Tor est un système d'anonymisation du trafic sur Internet. Comme toute technologie, c'est à la fois une opportunité, notamment pour les journalistes ou les dissidents dans les pays où leur parole est bannie, mais aussi un risque pour les possibilités de blanchiment. Tor est déconnecté de *bitcoin*. La plateforme « *Silk Road* » est un exemple intéressant : lors de sa fermeture par le FBI, il y a eu d'abord un frémissement à la baisse du cours du *bitcoin* – qui est considéré, à tort, comme le symbole de sa vitalité. Mais, rapidement, le cours a repris sa

hausse. On constate qu'en réalité, « *Silk Road* » représentait seulement 1 % des transactions en bitcoin. Bitcoin n'est donc pas porté par « *Silk Road* » et le blanchiment, mais, de plus en plus, par des commerçants, qui sont déjà plusieurs dizaines de milliers aux Etats-Unis.

Les activités illégales fondées sur des transactions en bitcoin existent et doivent être combattues par les services de l'Etat ; nous les y aidons autant que possible. Mais il faut également que ces autorités de régulation se saisissent de l'objet « *bitcoin* », montent en compétence, pour anticiper son développement, car on ne pourra pas interdire ou supprimer ces évolutions technologiques.

S'agissant des détenteurs, il est vrai, en effet, que les premiers développeurs détiennent un stock important de *bitcoin*, mais cela me semble normal que les créateurs et les premiers acteurs du système aient un avantage, puisqu'ils s'analysent comme des entrepreneurs, à l'instar d'un Mark Zuckerberg ou d'un Steve Jobs.

M. Philippe Marini, président. – Comment sont-ils rémunérés ? Par une redevance ? Un droit de propriété industrielle ou intellectuelle ?

M. Gonzague Grandval. – La particularité de *bitcoin* est que la rémunération se fonde sur le travail de calcul opéré par les processeurs du réseau. Au début, l'exécution d'une seule transaction permettait d'obtenir un nombre important de *bitcoin* ; aujourd'hui, avec une forte compétition entre processeurs du réseau, qui est d'ailleurs vertueuse puisqu'elle sécurise le réseau, la rémunération par transaction exécutée est plus faible.

M. Philippe Marini, président. – Et que font-ils de leurs *bitcoins* ? Comment liquider ses positions ?

M. Gonzague Grandval. – Vous pouvez les vendre, les conserver, les utiliser pour acheter des biens ou des services ! Le système n'impose pas une utilisation des *bitcoins* ainsi reçus. Au début, le *bitcoin* était surtout utilisée comme moyen d'épargne, comme réserve de valeur. Maintenant, aux Etats-Unis notamment, on peut de plus en plus effectuer des transactions commerciales en *bitcoin*.

M. Philippe Marini, président. – Existe-t-il un marché d'options sur *bitcoin* ?

M. Gonzague Grandval. – Je crois qu'en effet des opérateurs commencent à développer ce type de produits.

S'agissant du retard de la France, je le regrette également. Les pays en avance sont les Etats-Unis, l'Europe du Nord, notamment l'Allemagne, Israël et l'Asie. Il s'agit des pays dont les autorités de régulation ont pris position en faveur d'un accompagnement de ce mouvement – sans l'encourager, mais en lui fournissant le cadre de réglementation dont il a besoin. A cet égard, il est important que la régulation soit européenne. Nous avons des concurrents en Europe qui ont parfois une croissance florissante

car, en l'absence de régulation, ils ne s'imposent pas les règles auxquelles nous nous sommes, quant à nous, astreints volontairement, d'un point de vue fiscal comme d'un point de vue financier. Il faut une régulation harmonisée, sinon l'activité continuera de se développer hors de France.

M. Philippe Marini, président. – Si l'activité n'est pas très importante en France, la France ne risque donc rien ?

M. Gonzague Grandval. – Elle ne risque rien, mais elle risque tout ! Elle doit prendre une position innovante pour capter ces compétences et ces activités, qui sont génératrices d'emplois dans le domaine du paiement électronique.

S'agissant du nombre de mineurs, on estime à environ 100 000 le nombre de processeurs sur le réseau, qui sont souvent regroupés dans des « *pools* » de minage. Ce réseau se densifie, en volume comme en valeur, car la puissance de calcul s'accroît constamment. On constate que des systèmes « *hardware* » sont développés qui ont pour seule fonction de traiter les transactions du réseau *bitcoin*.

Pour ce qui est de l'existence ou non d'un « pilote » du système *bitcoin*, il existe une Fondation *bitcoin* aux Etats-Unis. Nous voulons créer, avec d'autres partenaires, une association « *Bitcoin Europe* ».

Je suis également favorable à un statut légal, comme en Allemagne ou aux Pays-Bas : dès lors qu'une position officielle a été prise par les régulateurs, il est plus simple de lancer une activité car cela rassure les développeurs et facilite leurs activités. Nous sommes en attente de régulation, que je considère comme une assurance et un soutien à mon activité. Je serais par exemple prêt à confier à la Banque de France une partie des dépôts de mes clients en réserve pour qu'elle en assure la sécurité. S'il y avait des organismes qui ont les moyens d'assurer des données numériques comme les nôtres, des acteurs comme nous serions ravis !

M. Philippe Marini, président. – Moyennant une redevance pour service rendu ?

M. Gonzague Grandval. – Absolument. C'est une activité risquée, complexe, technique mais dont certains ont fait leur activité commerciale.

M. Philippe Marini, président. – Il est intéressant, dans vos propos, de voir que vous êtes en attente de régulation ; celle-ci peut être un facteur de compétitivité pour le territoire français.

M. Gonzague Grandval. – En effet, sans quoi la France va rater ce train comme elle a manqué celui de *Paypal*.

M. Jean-Michel Cornu. – Certaines questions sont effectivement liées et je vais y répondre, plus ou moins rapidement selon mon propre domaine de compétences, en procédant à un certain nombre de distinctions.

Tout d'abord, concernant la « centralisation » de *bitcoin*, on dénombre aujourd'hui 12 millions de *bitcoins* pour 100 000 processeurs, ce qui ne signifie pas autant d'utilisateurs puisqu'une technique consiste à multiplier le nombre d'ordinateurs pour être davantage rémunéré. En effet, le détenteur de l'ordinateur est rémunéré à chaque fois que sa machine sera choisie aléatoirement parmi les 100 000. Avec plusieurs ordinateurs, il va donc pouvoir gagner plus de *bitcoins*.

Il est, par conséquent, difficile de connaître le nombre d'utilisateurs, de même que le nombre de « mineurs » car, par définition, il n'est pas possible de connaître les personnes faisant des transactions à l'intérieur du système *bitcoin*. L'identité des personnes ne peut être connue, à condition évidemment d'une régulation adéquate, que lorsqu'elles vont transformer des *bitcoins* en monnaie ayant court légal. Si je fais des transactions à l'intérieur du système, je peux être « mineur » et rester invisible, mon identité ne sera connue que dès lors que je transforme les *bitcoins* en argent, par exemple en euros, pour faire d'autres achats. À ce moment-là, il est possible d'imaginer connaître les identités des utilisateurs, à condition de régulation adaptée, à l'instar de ce qui s'est apparemment passé, si j'ai bien compris, dans la collaboration entre la société *Paymium* et les douanes.

Il faut donc bien distinguer le passage de *bitcoin* vers l'extérieur, qui peut être facilement régulé et où il est relativement facile d' « installer des radars », du système *bitcoin* « à l'intérieur », où les radars permettront de voir les transactions, mais pas les personnes qui les effectuent. C'est là que se trouve la difficulté. Par analogie avec la sécurité routière, je peux mettre des radars au sein du système, je saurai la vitesse de la voiture mais je n'aurai pas la plaque d'immatriculation.

Ceci correspond à la première distinction que je souhaitais faire, entre « *bitcoin* à l'intérieur » et *bitcoin* avec le « reste du monde ».

M. Gonzague Grandval. – Cette distinction est en partie vraie mais il existe des outils, certes lourds à mettre en place, qui permettent de remonter aux adresses IP à partir d'une transaction *bitcoin*. La technique est compliquée, pas encore tout à fait au point et demande des efforts majeurs pour la mettre en œuvre, mais ce n'est pas impossible. Les Etats-Unis devraient, à n'en pas douter, développer les outils permettant d'obtenir cette traçabilité des transactions en *bitcoins*.

M. Jean-Michel Cornu. – Effectivement, cela soulève donc deux questions différentes, l'une étant davantage du domaine classique du régulateur, l'autre étant plus complexe et relevant du domaine technologique.

S'agissant de la place de la France, il convient de distinguer *bitcoin* de l'ensemble des monnaies, y compris des nouvelles monnaies virtuelles et décentralisées. Une autre monnaie virtuelle a été développée par un Français, sous le terme d'*OpenUDC*. Fondée sur la théorie relative de la

monnaie, laquelle a, d'ailleurs, été également en partie développée en France, elle se distingue de *bitcoin* sous deux aspects en termes de création monétaire, même si elle est également décentralisée et unique.

S'agissant du mécanisme de création monétaire dans le système *bitcoin*, 50 *bitcoins* ont été créés toutes les dix minutes pendant quatre ans, comme cela a déjà été dit. Ce n'est pas tout à fait vrai mais on considère que l'état d'un calculateur va pouvoir effectuer un certain nombre de calculs en dix minutes. Au fur et à mesure des années, il va évidemment falloir réaliser des calculs un peu plus complexes pour que cela continue de durer à peu près dix minutes. Cela correspond ainsi à environ 2,6 millions de *bitcoins* par an.

Ces *bitcoins* sont affectés à toute personne qui ouvre un compte. À chaque fois qu'est justifié un « paquet » de transactions, le détenteur du compte reçoit une rémunération qui était de 50 *bitcoins* pendant les quatre premières années de sa création et de 25 *bitcoins* maintenant.

Ainsi, 2,6 millions de *bitcoins* pendant quatre ans aboutissent à environ 10,5 millions de *bitcoins* à l'issue de cette période, auxquels s'ajoutent près de 5 millions de *bitcoins* avec la création de 25 *bitcoins* tous les dix minutes pendant les quatre années suivantes, pour aboutir, au final, à un maximum de 21 millions de bitcoins. C'est le mécanisme de création monétaire propre à *bitcoin*.

Pour *OpenUDC*, le mécanisme de création monétaire retenu se fonde, non plus sur la puissance de calcul de l'ordinateur, mais sur un système de dividende universel. Chaque personne appartenant à ce système reçoit, selon la fréquence de son choix, chaque semaine ou chaque mois, vous pouvez choisir, une part de la création monétaire. Ces mécanismes sont dont un peu différents.

Ensuite, et c'est particulièrement important, notamment lorsqu'on parle de rareté, il convient de distinguer le protocole, d'une part, de ses paramétrages, d'autre part.

Le protocole peut être libre et il est d'ailleurs publié. J'ai moi-même analysé une partie du code du protocole *bitcoin* pour pouvoir répondre à vos questions aujourd'hui, c'est un peu technique mais c'est possible. Ensuite, il y a le paramétrage de ce protocole. Le code est libre et visible par tous, actuellement mis en œuvre dans un logiciel téléchargeable lorsqu'on souhaite obtenir le système *bitcoin*.

En revanche, les choix de paramétrage de bitcoin ont été faits par une personne anonyme se présentant sous un nom à consonance japonaise - on ne sait d'ailleurs pas s'il n'y a derrière qu'une seule personne ou plusieurs -, qui s'est depuis retirée du système.

Cette personne ne reçoit pas de rémunération directe. Mais les premiers *bitcoins* échangés, « genesis », c'est-à-dire le premier « paquet » de

transactions, ont été échangés avec lui et/ou les personnes appartenant à ce groupe, qui n'ont pas à être rémunérés puisqu'existe un avantage aux « premiers arrivants ».

Bitcoin correspond donc non seulement à un protocole mais également à des paramétrages de ce protocole.

Le système *OpenUDC* en est à un stade moins avancé. Il est possible d'y développer des monnaies, c'est-à-dire des paramétrages (de ce protocole) ayant des caractéristiques différentes. Certaines de ces caractéristiques sont communes et d'autres peuvent varier, notamment le choix de la fréquence de rémunération des utilisateurs (par mois ou par semaine) ou encore son caractère convertible ou non en une autre monnaie.

C'est pourquoi il me semble très important de distinguer les mécanismes monétaires des protocoles appliqués, lesquels peuvent eux-mêmes être biaisés. Le fait d'avoir des logiciels libres dans tous ces nouveaux systèmes, et y compris d'ailleurs dans les SEL ou d'autres systèmes d'échanges de monnaies comme « Open money », ou le système « Flowplace », dans lequel la France est également active, permet d'en connaître les paramétrages. C'est cette transparence qui offre la possibilité de savoir si cette monnaie entre dans un système qui convient au législateur ou, au contraire, un système qui nécessiterait régulation.

Les « radars » pourraient donc également être installés sur ces paramétrages, si on ne sait pas les mettre sur les transactions, pour déterminer les systèmes qui paraissent acceptables et ceux qui ne le sont pas.

Le « grand architecte » de *bitcoin* a établi un paramétrage une fois pour toute, avant de s'en éloigner. Aucune gouvernance n'est prévue puisqu'elle est *a priori* prévue dans le code du système lui-même. Comme le disait Lawrence Lessig en parlant d'Internet, il a été mis de la liberté dans le code, c'est-à-dire que le système même offre lui-même de la liberté, des opportunités, des contraintes et des difficultés.

Pour procéder à une régulation, il n'est donc pas nécessaire d'être un spécialiste de la technique mais bien, en revanche, de l'architecture du système. Par analogie avec l'augmentation de la largeur des rues opérées à Paris, il n'est pas nécessaire de savoir comment construire un bâtiment pour comprendre comment rendre plus difficile la formation de barricades. On a ainsi procédé à une régulation de la société.

M. Philippe Marini, président. – Le préfet Haussmann a procédé à une régulation efficace !

M. Jean-Michel Cornu. – En conclusion, il faut bien distinguer ce qui se passe au sein du système *bitcoin* et son interaction avec les autres monnaies, les places de marchés pouvant alors être un élément de régulation. Je rejoins Gonzague Grandval en affirmant que la régulation de

ces places de marché pourrait être un élément très positif et je partage en grande partie les réflexions qu'il a développées.

Il est également nécessaire de distinguer *bitcoin* des autres monnaies virtuelles puisque les paramétrages ne sont pas les mêmes. Les réponses que vous apporterez pourront donc différer d'un système à l'autre.

Enfin, s'agissant du statut légal, la question n'est pas de savoir lequel mettre en place mais plutôt quand intervenir. La difficulté est de trouver le bon moment car si vous intervenez trop rapidement, vous couperez l'innovation. Si vous légiférez trop tard, le système sera déjà trop développé pour intervenir correctement. Le passage de l'un à l'autre peut être très rapide, comme pour *bitcoin*, et c'est à vous, législateur, de trouver le bon moment.

M. Philippe Marini, président. – Merci beaucoup de ce conseil avisé.

M. Gonzague Grandval. – Je souhaiterais ajouter deux éléments à ce qu'a dit Jean-Michel Cornu.

En premier lieu, le fait que les codes et les paramétrages de *bitcoin* soient effectivement figés est essentiel pour la communauté *bitcoin*. La possibilité de changer un quelconque paramétrage constitue justement une des dérives des autres systèmes.

En second lieu, s'agissant du fait qu'une grande quantité de *bitcoins* soit détenue par un nombre limité de personnes, il convient de préciser qu'il est possible de surveiller l'ensemble des adresses, du fait que toutes les données sont publiques, à l'instar de celle du FBI qui détient plus d'une centaine de milliers de *bitcoins*, ce qui est considérable. Tout le monde scrute, d'ailleurs, avec attention cette adresse et chacun sera en mesure de savoir à quel moment le moindre *bitcoin* sera utilisé, si le FBI décidait de mener des actions, de perturber le marché…

Les adresses censées appartenir aux créateurs de *bitcoin* sont également surveillées avec attention. Nous pensons que ces *bitcoins* ne seront pas utilisés car ils pourraient, dès lors, être tracés et rendre identifiables leurs détenteurs. Ces adresses devraient donc vraisemblablement être maintenues dans le système pour l'éternité.

M. Philippe Marini, président. – M. le directeur national du renseignement et des enquêtes douanières, votre administration possède-t-elle toujours des *bitcoins* comme le FBI, sans doute à une plus faible échelle ?

M. Jean-Paul Garcia. – Nous possédons toujours des *bitcoins* et je pense que nous pourrions vous en céder, M. le Président, si vous le souhaitez…

M. Philippe Marini, président. – Nous demanderons à la Questure si nous avons le droit !

M. Jean-Paul Garcia. – Évidemment, ce sont des quantités très limitées, qui se comptent en unités. Sur l'opération que nous avons réalisée, nous avons utilisé moins d'un *bitcoin* pour acheter une petite quantité de stupéfiants.

Comme cela a toujours été fait, depuis 1945 que nous accompagnons ce mouvement de libéralisation des échanges, nous ne participerons pas à l'établissement de la régulation, mais nous l'appliquerons.

C'est à partir des échanges de marchandises que nous pénétrons le système. Il est très important d'avoir des personnes ou des entreprises comme *Paymium* qui nous permettent d'entrer dans le système. En effet, il est impossible d'entrer dans le système et de traquer quelque chose par hasard puisque le système Tor est fait pour garantir l'anonymisation.

Une fois que nous avons une cible, globalement nous saurons la traquer. L'essentiel est d'avoir les intermédiaires.

Je ne crois pas que l'on puisse dire que l'on peut lutter contre le développement de ce système qui est plutôt globalement bien reçu, qu'il s'agisse des sociétés ou des particuliers.

M. Philippe Marini, président. – Cet avis est-il partagé par TRACFIN ?

M. Jean-Baptiste Carpentier. – Je vais encore jouer le rôle du grognon ! Nous suivons ce phénomène depuis trois ans. On poursuit une analyse stratégique sur la question.

Il faut faire un distinguo. Il y a le sujet du *bitcoin* et les autres. Nous essayons de faire tourner nos différents « capteurs », sur lesquels je ne peux pas m'étendre car un certain nombre de données sont classifiées.

Paradoxalement, le sujet du *bitcoin*, au vu des évolutions observées, est celui qui nous paraît le moins inquiétant. Par construction, c'est une monnaie hyper déflationniste, parce qu'il y a une masse globale finie et que le nombre d'utilisateurs tend à s'accroître. La valeur croît rapidement, associée d'ailleurs à une hypervolatilité. Au total, en tant qu'unité transactionnelle, le *bitcoin* n'est pas très aisé. En outre, il faut quelques minutes pour utiliser un *bitcoin*. Ainsi, entre le moment où j'achète mon bien et le moment où le marchand reçoit mon *bitcoin*, sa valeur a pu varier du simple au double. En l'état actuel des choses, on se retrouve un peu dans la situation, en sens inverse, de la période du *Reichsmark*, où on ne savait pas s'il fallait prendre une brouette ou billet pour payer.

Toute proportion gardée, on est en 1637 au moment de la spéculation sur les bulbes de tulipe. Je ne sais pas si nous assisterons à un krach du *bitcoin* comme celui des tulipes. Quoi qu'il en soit, en tant que monnaie transactionnelle, cela reste difficile. On nous dit que son usage s'accroît mais nous ne partageons pas la même analyse. En toute hypothèse, il s'accroît toujours dans une situation *a-légale*.

Je ne suis pas totalement sûr que la DGFiP soit submergée de déclarations de transactions en *bitcoins*. Et on pourrait même dire que le phénomène devient alors illégal car il s'inscrit clairement dans une situation d'évitement des obligations fiscales.

Le *bitcoin* nous apparaît donc moins comme une unité de transaction mais plutôt comme une unité de réserve ce qui, de notre point de vue, tend à réduire le risque. Ce n'est clairement pas le cas des autres monnaies virtuelles. Dans le cas du site « *Silk Road* », la principale monnaie utilisée n'était pas le *bitcoin* mais le « *liberty reserve* », qui était une autre unité de compte. Or certaines d'entre elles présentent une plus grande stabilité et donc une plus grande maniabilité pour un cadre transactionnel qui est totalement opaque, sauf au niveau des carrefours. C'est d'ailleurs là qu'il faut placer les radars, sous réserve qu'il existe des carrefours. Il n'est pas exclu qu'apparaisse un jour un système totalement parallèle qui fonctionnera uniquement en monnaie virtuelle.

Il est clair qu'il y a un besoin de régulation, comme nous l'avons fait ces dernières années pour d'autres activités économiques et financières. Je ne partage d'ailleurs pas tout à fait l'analyse tendant à comparer le *bitcoin* et le *shadow banking*. Celui-ci s'inscrit dans un cadre alors que les monnaies virtuelles sont encore dans une boîte noire.

La question, déjà évoquée, est de savoir si la régulation elle-même ne fera pas perdre son intérêt au dispositif. Dès qu'il y a régulation, on crée des coûts supplémentaires.

En outre, la régulation est nécessaire mais son respect sera extrêmement difficile à contrôler, compte tenu de la nature même du dispositif, de l'extraterritorialité d'un certain nombre d'acteurs et de notre difficulté à intervenir sur ce réseau.

M. Denis Beau. – Le sénateur Yung a indiqué que la France est peu active en matière d'innovation dans les moyens de paiement. De notre point de vue, nous n'avons pas tout à fait la même perception. Les exemples donnés par Jean-Michel Cornu montrent qu'il y a une dynamique importante, même si elle ne porte pas forcément sur le segment sur lequel est positionné le *bitcoin*. Au niveau européen, la promotion des nouvelles technologies dans les systèmes de paiement est une réelle préoccupation. Après le SEPA (*Single Euro Payments Area*), nous avons ouvert le chantier e-SEPA.

L'Observatoire de la sécurité des cartes de paiement effectue une veille technologique et publie tous les ans le résultat de ses travaux. Vous pourrez constater les innovations dans ce domaine, en particulier de la part des acteurs français.

S'agissant de la demande de régulation, je ferais deux observations. Le cadre établi par le législateur est proportionné à l'importance de l'utilisation des moyens de paiement. Ainsi, nous pouvons promouvoir la

concurrence mais sans jamais affaiblir nos exigences en matière de sécurité. Or si un attrait du *bitcoin* tient aux faibles coûts de transaction, le revers de la médaille, ce sont les préoccupations sur la sécurité du système.

Dans le cadre de régulation que vous avez instauré, dès lors qu'un moyen de paiement se développe, la loi vient le contraindre de se doter d'un certain nombre de sécurités. C'est l'enjeu pour l'intégration dans les systèmes de paiement de monnaies virtuelles telles que *bitcoin*.

De ce point de vue, il faut prêter attention à l'activité des plateformes de conversion qui font le lien entre l'univers du *bitcoin* et l'univers des monnaies régulées. Je crois qu'il faudra réaffirmer, au niveau européen, que cette activité est une prestation de services de paiement.

Enfin, je terminerais sur les risques du *bitcoin*. Dès lors qu'on le qualifie de monnaie vis-à-vis de ses utilisateurs, il faut faire très attention à la portée de ce type de communication.

M. Philippe Marini, président. – Tout cela nous incite à réfléchir à des travaux législatifs dans ce domaine. À cet égard, il serait utile de savoir si la Commission européenne compte se saisir de ces questions. Il serait en effet surprenant que cette « machine à normaliser » ne s'empare pas d'un tel sujet, aux enjeux transfrontaliers par nature. Madame d'Amarzit, savez-vous s'il existe actuellement des travaux en cours au niveau européen ? Cela pourrait nous servir de support à une proposition de résolution européenne.

En outre, plusieurs questions restent ouvertes sur le statut en droit national des agents de ce système – prestataires de services de paiement –,la fiscalité, la régulation des transactions, le rôle de la Banque de France. Des éléments d'information et de réflexion sur ces aspects pourraient nous permettre de déposer une proposition de loi. Pourriez-vous réagir sur ces différents points ?

Mme Delphine d'Amarzit. – La question de savoir s'il faut légiférer ou non se posera si nous ne parvenons pas à interpréter les statuts existants pour qualifier des opérations réalisées en *bitcoins*. Si l'on estime que la qualification est trop incertaine, il faudra trouver le niveau de norme adéquat pour le faire (clarification de la doctrine, décret…).

Mais ce n'est pas uniquement une question fiscale. Par exemple, dans le domaine des plateformes de services de paiement, qui a été cité, notre interprétation a été clarifiée par la jurisprudence ; il sera utile de faire remonter ce point au niveau européen : l'ABE a justement pour rôle de coordonner les interprétations en cas de différences d'appréciation entre les pays. C'est un premier outil pour s'assurer de la bonne transposition de la norme européenne. Ensuite, des réflexions sont en cours sur la deuxième directive sur les services de paiement, ce qui permettra également de débattre de ces questions.

Monsieur le rapporteur général, vous avez évoqué la question de savoir si on peut donner un statut de monnaie légale au *bitcoin* : cela impliquerait soit d'abandonner le caractère souverain de la monnaie, soit d'interdire les *bitcoins*.

La question est plutôt de savoir si l'on peut donner une qualification : celle-ci peut-t-elle relever de catégories existantes ou bien faut-il créer de nouvelles catégories juridiques ? Nous sommes conscients de la nécessité de clarifier les choses.

M. François Marc, rapporteur général. – Je souhaiterais préciser mon propos pour éviter toute ambiguïté : il ne s'agissait pas de reconnaître un caractère de monnaie légale au *bitcoin* mais de donner un statut légal à l'existence de ce dispositif qui est déjà utilisé, de fait, dans les transactions. Dès lors, une clarification de ce statut permettrait de recourir au *bitcoin* sur des bases plus efficaces et mieux acceptées par tous.

M. Philippe Marini, président. – L'argument de la compétitivité est essentiel ; le fait de définir les conditions des opérations est un élément pour créer la confiance dans le territoire France par rapport à d'autres territoires.

Nous n'avons sans doute pas épuisé le sujet, mais nous nous emploierons à en approfondir les différents aspects. De façon plus générale, tous les travaux liés à Internet sont indispensables et passionnants à mener pour la représentation nationale. Nous sommes profondément interpellés par ces évolutions qui appellent des adaptations de notre droit et de notre fiscalité. Je pense qu'il serait tout à fait dommageable que les autorités nationales se cantonnent à une attitude d'abstention et d'attentisme sur ces questions. Cela ne ferait qu'aggraver le sentiment d'impuissance souvent exprimé vis-à-vis de nos institutions. Je remercie nos intervenants pour leur participation.

COMMUNICATION EN COMMISSION DE PHILIPPE MARINI ET FRANÇOIS MARC

Réunie le mercredi 23 juillet 2014, sous la présidence de M. Philippe Marini, président, la commission a entendu une communication de MM. Philippe Marini et François Marc sur les enjeux liés au développement du *bitcoin* et des autres monnaies virtuelles.

M. Philippe Marini, président. – Je développerai des considérations de portée économique et générale, et le rapporteur général nous dira les conclusions que l'on peut tirer, et les propositions que l'on peut formuler, à partir des éléments que nous a fournis le Gouvernement. Nous l'avions notamment interrogé afin d'obtenir des éléments de comparaisons internationales, qui nous ont semblé très utiles sur un tel sujet.

Notre commission avait organisé, le 15 janvier dernier, une audition conjointe sur les enjeux liés au développement des « monnaies virtuelles », parmi lesquelles figure le célèbre *bitcoin*. Nous avions pu entendre le Trésor, les douanes, la Banque de France, Tracfin, mais aussi un entrepreneur et un universitaire spécialiste du sujet. Comme nous en étions convenus, deux questionnaires avaient ensuite été adressés au Gouvernement et aux services économiques de nos représentations diplomatiques.

On peut observer que les choses ont beaucoup changé depuis six mois : le développement des monnaies virtuelles s'est poursuivi, avec son lot d'innovations et de canards boiteux voire de scandales ; le *bitcoin* a été présent dans l'actualité, et les autorités ont poursuivi leur réflexion pour obtenir une certaine forme de régulation. Le 11 juillet dernier, le ministre des finances et des comptes publics, Michel Sapin, s'est appuyé sur les travaux qui avaient été effectués pour annoncer plusieurs mesures d'encadrement des monnaies virtuelles, dont nous parlera le rapporteur général.

L'intérêt que porte la commission des finances du Sénat à ce sujet n'a pas lieu de surprendre : il s'inscrit dans les travaux que nous avons entamés dès 2008-2009 sur les transformations profondes qu'induisent, pour notre fiscalité et pour les mécanismes économiques et financiers, les technologies numériques. L'irruption du numérique dans la vie ne laisse à cet égard à peu près rien dans le *statu quo*.

Il y a d'abord les conséquences fiscales : la concentration de la valeur sur des actifs immatériels, facilement (dé)localisables sous des latitudes aussi clémentes par leur droit et leur fiscalité que par leur climat, a provoqué, comme nous pouvions le redouter, une attrition des assiettes fiscales dont les grands pays ont aujourd'hui pris conscience. Mais au-delà de la fiscalité, la révolution numérique vient bouleverser de fond en comble différents secteurs économiques : le monopole des taxis est remis en cause par des applications comme *Uber* – nous en discuterons cet après-midi en séance

publique –, et le modèle des hôtels est bousculé par le développement des sites de réservation en ligne ou des sites proposant des solutions d'hébergement alternatives comme *Airbnb*, par exemple.

Avec les « monnaies virtuelles », nous touchons à quelque chose de plus fondamental encore : le monopole d'émission des banques centrales, manifestation par excellence du pouvoir régalien. Exemple le plus connu et le plus « réussi », le *bitcoin* est un système de paiement libre, anonyme et décentralisé, qui permet aux utilisateurs d'échanger entre eux des biens et des services sans avoir recours à la monnaie classique. *Stricto sensu*, toutefois, il ne s'agit ni d'une monnaie ayant cours légal, ni d'un moyen de paiement au sens du code monétaire et financier. C'est quelque chose d'innomé, de non-qualifié juridiquement. Le *bitcoin* n'est pas émis contre la remise de fonds. Il est un support de transactions. Pour l'instant, le *bitcoin* relève avant tout d'une forme de troc en version numérique : parfois, ce qui était le plus archaïque peut devenir, grâce aux technologies d'aujourd'hui, le plus moderne et le plus innovant.

Toutefois, on ne peut écarter d'un revers de main cette innovation, sous prétexte qu'il ne s'agirait que d'un épiphénomène. De plus en plus de e-commerçants acceptent les paiements en *bitcoins*, de même que la plateforme *PayPal*. Si le *bitcoin* connaît un tel succès, c'est qu'il présente des avantages tangibles. Lesquels ? Tout d'abord, les frais de transaction : ils sont réputés quasi-nuls – j'insiste sur le mot « réputés ». Une récente étude de Goldman Sachs les estime à 1 %, contre 2,5 % pour un virement par carte bancaire. Signalons toutefois que ce débat n'est pas tranché, dans la mesure où une estimation exacte devrait inclure, d'une part, le coût de l'équipement informatique et de l'électricité, et d'autre part, le coût du risque associé à la volatilité du *bitcoin* et des éventuelles couvertures à prévoir en conséquence. Surtout, le *bitcoin* se caractérise par un ingénieux mécanisme de « création monétaire », ou de création de signes quasi-monétaires, qui rémunère ses utilisateurs : mettez la puissance de calcul de votre ordinateur à la disposition du réseau afin de valider les transactions, et vous serez rémunérés en *bitcoins*.

Ce système, nous en sommes conscients, comporte des risques notoires. Ceux-ci sont connus depuis l'origine mais sont apparus très clairement ces derniers temps, et ne peuvent que conduire les pouvoirs publics à émettre un certain nombre d'avertissements. Le *bitcoin* se caractérise par une extrême volatilité – un *bitcoin* valait moins d'un dollar jusqu'en 2011, presque 1 200 dollars à l'automne 2013, et environ 650 dollars aujourd'hui… De fait, le système est spéculatif, puisque le rythme de création des *bitcoins* suit une courbe décroissante, jusqu'à atteindre un maximum de 21 millions d'unités en 2140, contre environ 12 millions aujourd'hui. Le système est clos, construit pour toute sa durée de vie. C'est une véritable « rareté organisée », qui est aussi la condition de son succès

puisqu'elle garantit les détenteurs contre une éventuelle dévaluation de leurs avoirs : il ne peut pas exister de « planche à *bitcoins* ».

De plus, le *bitcoin* ne bénéficie d'aucune garantie de convertibilité en monnaie « réelle », ce qui laisse les utilisateurs bien dépourvus en cas de perte généralisée de confiance dans le système.

Ensuite, si le protocole de validation des transactions est lui-même très sécurisé, il n'en va pas de même pour le « stockage » des *bitcoins*. La plupart des utilisateurs décident de stocker leurs *bitcoins* sur des « comptes » ouverts auprès de plateformes d'échange en ligne. Mais le piratage est possible : la faillite de *Mt. Gox*, la plus grande plateforme au monde, a ruiné plusieurs milliers d'utilisateurs le 28 février dernier, ce qui démontre la fragilité de ces « coffres forts » virtuels. Bien sûr, il est aussi possible de conserver ses *bitcoins* sur son propre disque dur, chez soi : James Howell, un jeune Britannique qui avait acquis 7 500 *bitcoins* contre une poignée de livres sterling en 2009, serait aujourd'hui multimillionnaire s'il n'avait pas malencontreusement jeté le sien dans une immense décharge publique du Pays de Galles…

Surtout, l'anonymat qui s'attache aux transactions fait du bitcoin une aubaine pour la cybercriminalité ou le blanchiment. L'audition du 15 janvier dernier a permis d'apprendre que les services de la douane avaient arrêté un trafiquant de stupéfiants qui se faisait payer en *bitcoins*. Certes, le site *Silk Road*, véritable caravansérail de la drogue en ligne, et arsenal virtuel d'armes bien réelles, a été fermé fin 2013 par le FBI. Mais il ne faudrait pas en déduire que tout risque est écarté, comme en témoigne l'arrestation, mardi 28 janvier à New York, du vice-président de la *Bitcoin Foundation*.

Il faut toutefois raison garder – même si la Banque de France, Tracfin et l'AMF sont dans leur rôle en appelant à la vigilance. Pour l'heure, c'est la volatilité et l'absence de statut légal du *bitcoin* qui devraient limiter son développement au-delà d'un cercle d'initiés : en effet, quel particulier, quel commerçant, et même quel réseau criminel aurait intérêt à réaliser ses transactions au moyen d'un étalon dont la valeur peut être divisée par deux en quelques instants ? De même, le *bitcoin* ne constitue pas une menace pour la stabilité macroéconomique, compte tenu de la masse monétaire qu'il représente : 5 à 8 milliards de dollars seulement, contre des milliers de milliards de dollars pour les grandes devises. Aujourd'hui, il me semble que le *bitcoin* tient davantage du produit spéculatif de niche que d'une véritable alternative à la monnaie. Et l'on ne peut s'empêcher de penser que les quelques distributeurs et magasins Monoprix qui acceptent cette « devise » le font d'abord par souci de publicité…

Surtout, se concentrer uniquement sur les risques – ce qu'il faut néanmoins faire – revient à ignorer les multiples opportunités qu'ouvrent les monnaies virtuelles. Ce n'est pas parce qu'une innovation peut mettre au

défi certaines de nos conceptions traditionnelles qu'il faut les rejeter en bloc, d'autant que le rejet risquerait d'être assez fortement théorique : comment, en effet, discipliner les comportements individuels et interdire à nos concitoyens de faire usage de plateformes étrangères ?

Comme alternative aux monnaies classiques, le *bitcoin* commence à peine à montrer son potentiel. Certains, qui ont une imagination développée, pensent déjà à la mise en place d'offres de crédit ou de financement participatif (*crowdfunding*) en monnaies virtuelles. Je suis personnellement très réservé sur ces idées, mais elles méritent d'être analysées, et de nouveaux développements pourraient intervenir.

Mais surtout, plus qu'une « monnaie », le *bitcoin* est une technologie, un protocole de validation des transactions totalement décentralisé, « auditable » par tous et très sécurisé. Or, s'il est possible de valider des transactions, pourquoi ne pas s'en servir pour valider autre chose ? Par exemple, des mots de passe, des titres d'identités, des diplômes et autres certificats, ou même des votes électroniques ! Dans un monde proche, personne ne pourrait plus frauder sur les diplômes qu'il a obtenus, et ce serait un progrès. Quant au vote électronique, je pense à celui des Français de l'étranger dont le développement est entravé par des doutes sur sa sécurité. La validation décentralisée est une amélioration du principe de la cryptographie : aucun « tiers de confiance » ne se retrouve jamais en possession de l'information complète, mais celle-ci est néanmoins parfaitement vérifiée.

Il existe d'autres « monnaies virtuelles » : il y en a eu d'autres hier (par exemple *Liberty Reserve* ou *e-Gold*), il peut y en avoir d'autres demain, même si le *bitcoin* s'est réellement développé. Il est donc très important pour les pouvoirs publics d'apprécier ce phénomène tel qu'il est, de ne pas rester en retrait, d'intervenir à bon escient de guider les raisonnements. Il appartient au rapporteur général de nous éclairer sur cette dialectique entre innovation et régulation, qui apporte la sécurité nécessaire aux acteurs du marché.

M. François Marc, rapporteur général. – Je voudrais vous faire part d'une réminiscence déjà fort ancienne, qui concerne l'apparition des cartes bancaires. J'étais à l'époque jeune chercheur à l'université et je travaillais sur les moyens de paiement, lorsque la carte bancaire commençait à apparaître dans les commerces. Je me souviens qu'à l'époque, on était dans la méfiance la plus absolue. Cette innovation était présentée par les uns et les autres, dans les publications scientifiques, comme une source de risques considérables, qui n'irait pas très loin et connaîtrait une désaffection une fois connues les dérives qui allaient se manifester. Avec le *bitcoin*, le sujet est certes différent mais j'ai le sentiment que l'on retrouve, à travers ce que l'on peut lire, la même anxiété face à l'évolution des choses. Dans ce contexte fort incertain, où l'on ne maîtrise pas encore tous les paramètres ni tous les usages, la question de la régulation se trouve d'emblée posée.

Il n'est pas facile d'apporter une réponse normative à un phénomène qui se joue des frontières géographiques autant que des cadres conceptuels. Pourtant, une régulation est absolument nécessaire, ne serait-ce que pour sécuriser les utilisateurs et les acteurs qui prennent le risque d'innover, ainsi que pour prévenir les dérives qui, sinon, pourraient conduire à décrédibiliser rapidement le système dans son ensemble.

Le président Philippe Marini a parlé de la fermeture du site *The Silk Road* et de la faillite de la plateforme *Mt. Gox*. J'évoquerai pour ma part un événement plus proche de nous : il y a deux semaines, les gendarmes de la région Midi-Pyrénées ont arrêté trois personnes qui opéraient une plateforme d'échange de *bitcoins* sans autorisation, et « saisi » 388 *bitcoins*, ce qui correspond à environ 200 000 euros… Heureusement, l'audition du 15 janvier dernier au Sénat nous a permis de réaliser que certains acteurs privés présents sur le marché du *bitcoin* étaient en attente d'une régulation. Bien sûr, les professionnels demandent toujours un maximum de souplesse, là où les autorités poussent pour des contrôles plus pointilleux. Comme souvent, l'enjeu est de réguler efficacement sans « tuer » l'innovation.

Il faut se féliciter que la France ait su réagir assez rapidement en matière de régulation. Il y a dix jours, se fondant notamment sur les travaux conduits à l'initiative de notre commission, le ministre des finances et des comptes publics, Michel Sapin, a annoncé plusieurs mesures très concrètes.

Premièrement, une clarification du régime fiscal des monnaies virtuelles : les plus-values seront ainsi imposées au barème de l'impôt sur le revenu, au premier euro, au titre des bénéfices industriels et commerciaux (BIC) si l'activité d'achat-revente est habituelle, ou des bénéfices non-commerciaux (BNC) si celle-ci est occasionnelle. Par voie de conséquence, les moins-values seront déductibles sous certaines conditions. Les *bitcoins* et leurs équivalents entreront par ailleurs dans le patrimoine imposé au titre de l'impôt de solidarité sur la fortune (ISF) et seront soumis aux droits de mutation à titre gratuit (DMTG). En revanche, la France soutiendra au niveau européen un non-assujettissement à la TVA, afin d'éviter de réitérer l'expérience malencontreuse des quotas carbone qui ont donné lieu à un gigantesque « carrousel TVA ».

Deuxièmement, une limitation de l'anonymat : le ministre entend imposer aux plateformes d'échange une obligation d'identification à l'occasion d'une ouverture de compte, d'un retrait, d'un dépôt ou d'une transaction. Une concertation a été engagée à ce sujet, qui est extrêmement délicat puisqu'il touche au fondement même du système.

Troisièmement, un plafonnement des paiements en monnaies virtuelles, comme cela existe pour le numéraire : dans les deux cas, cela se justifie par l'anonymat qui s'attache aux transactions.

Il faut ajouter à cela que l'Autorité de contrôle prudentiel et de régulation (ACPR) estime que les intermédiaires proposant d'échanger des

« monnaies virtuelles » contre des monnaies ayant cours légal sont soumis au statut de prestataire de services de paiement (PSP). C'est par exemple le cas de la plateforme *Bitcoin-Central* proposée par *Paymium*, dont nous avions auditionné le fondateur. À ce titre, ils doivent respecter un certain nombre d'obligations prudentielles, et sont assujettis aux règles de lutte contre le blanchiment et le financement du terrorisme.

On peut se poser la question suivante : les positions prises par la France sont-elles similaires à celles des autres pays ? Pour le savoir, nous avions adressé un questionnaire aux missions économiques de la direction générale du Trésor, afin d'obtenir des éléments de comparaison avec treize autres pays dûment sélectionnés. Ce questionnaire est complété par un autre, de portée plus générale. Les réponses à ces questionnaires constituent un travail inédit qui permettra d'éclairer les décisions futures, notamment au niveau européen. Ces comparaisons montrent que si tous les pays se posent à peu près les mêmes questions, tous n'y apportent pas les mêmes réponses – ceci n'est pas une formule rhétorique, c'est un constat assez préoccupant puisque nous parlons d'un phénomène qui est par essence transnational. De fait, la France se situe à mi-chemin entre les pays les plus régulateurs et les pays les plus libéraux.

En ce qui concerne la qualification juridique des monnaies virtuelles, la France évolue dans le même flou que la plupart des pays, faute d'accord entre leurs différentes administrations. Toutefois, certains pays comme la Chine, la Thaïlande ou la Corée considèrent clairement les *bitcoins* comme des « biens » ou des « marchandises », fussent-elles numériques, à l'instar d'un fichier musical « mp3 ». Le gouverneur de la Banque centrale chinoise a ainsi comparé les *bitcoins* aux timbres échangés par les philatélistes… Moins poétique peut-être, et surtout très isolée pour l'instant, l'autorité de supervision allemande qualifie les monnaies virtuelles d'unités de compte, entrant dans la catégorie des instruments financiers au même titre que les devises.

Peu pressés de définir les monnaies virtuelles, les pays se sont en revanche montrés plus prompts à les taxer…

M. Philippe Marini, président. – Je taxe donc je suis !

M. François Marc, rapporteur général. – Toutefois les régimes fiscaux choisis demeurent très hétérogènes : assimilés aux gains aux jeux en ligne par la Chine et à ce titre taxés à l'impôt sur le revenu, les *bitcoins* sont imposés comme des biens immobiliers par l'Allemagne et comme des revenus du capital par les États-Unis. L'Allemagne, le Royaume-Uni et d'autres pays ont aussi choisi d'assujettir les monnaies virtuelles à la TVA, mais n'ont pas encore trouvé comment s'y prendre… Le Japon, lui, fait confiance au civisme déclaratif de ses contribuables.

En ce qui concerne la régulation des transactions et des plateformes d'échange, la plupart des pays ont multiplié les avertissements, d'abord sur

les risques encourus par les utilisateurs des monnaies virtuelles, et surtout sur les risques de blanchiment et de financement du terrorisme. Toutefois, tous n'en concluent pas que cela justifie une intervention du régulateur, voire du législateur : beaucoup considèrent, à l'instar du Japon, que réguler revient à légitimer, et donc à encourager. Ainsi des pays comme l'Allemagne, Israël ou le Canada se contentent-ils de prévenir les utilisateurs de *bitcoins* qu'ils agissent « à leurs risques et périls », sans garantie publique d'aucune sorte. Les positions les plus strictes viennent de la Chine et de la Russie, qui interdisent – sauf exception – l'usage des monnaies virtuelles et y attachent une présomption d'utilisation à des fins de blanchiment. La France fait à cet égard preuve d'un libéralisme prudent, en n'interdisant pas les monnaies virtuelles mais en assujettissant les plateformes au statut encadré de prestataire de service de paiement (PSP).

Enfin, en ce qui concerne l'innovation, ce sont sans surprise des pays comme les États-Unis, le Canada et Israël qui se montrent les plus ouverts. Les incubateurs, *business angels* et autres *start-ups* s'y multiplient, dans un contexte de bienveillance des autorités publiques. À Chypre, l'université de Nicosie accepte le paiement des frais de scolarité en *bitcoins*, même si peu d'étudiants ont sauté le pas. La France n'a toutefois pas à rougir en matière d'innovation : nos entreprises spécialisées dans les technologies financières font preuve d'une remarquable créativité, pour les monnaies virtuelles, mais aussi les autres modes alternatifs de paiement (*crowdfunding*, paiement par smartphone etc.).

Il y a, pour résumer, trois types d'attitudes face au développement des monnaies virtuelles. Les sceptiques, parmi lesquels de nombreux juristes et économistes, qui soulignent à bon droit que le *bitcoin* n'est pas une véritable monnaie – mais ils oublient la très prometteuse dimension « technique » du système. Les inquiets, dont font partie nos régulateurs, car il est de leur devoir d'anticiper les problèmes et de les prévenir. Et les optimistes, pour lesquels le *bitcoin* est aux transactions ce que *l'email* a été au courrier et le *web* à l'édition. Tâchons de rassurer les uns sans décourager les autres.

Quelles recommandations peut-on, dès lors, formuler ? Les pouvoirs publics doivent mener dans la durée un véritable travail de veille et de réflexion sur les monnaies virtuelles, continuer à informer les utilisateurs sur les risques mais aussi les droits associés, et travailler à l'élaboration d'une régulation adaptée. Il importe surtout de mener ce travail à l'échelle européenne, sans laquelle nulle mesure efficace n'est concevable.

En ce qui concerne la question de la qualification juridique des monnaies virtuelles, nous pourrions proposer de « tester » pour l'instant le recours aux catégories du droit existantes, plutôt que d'inventer une catégorie ad hoc. C'est le pari fait par de nombreux pays, et auquel se tient pour l'instant la France : considérer les *bitcoins* comme des « biens » par défaut permet l'application du droit commun, notamment en matière de

protection des consommateurs, d'escroquerie et de résolution des litiges commerciaux. Je précise que nous parlons ici de la « chose » (les *bitcoins*), et non pas du « service », lequel est d'ores et déjà considéré comme une prestation de service de paiement (PSP) et régulé à ce titre.

Comme à chaque nouvelle révolution portée par l'économie numérique, il est clair que la France et l'Europe ont une carte à jouer. Pour réussir ensemble, nous devrons accompagner l'innovation tout en l'encadrant pour en éviter les dérives, faire preuve d'ouverture tout autant que de vigilance.

M. François Trucy. – Le fait que les promoteurs des monnaies virtuelles les comparent à Internet en termes de bouleversement et d'essor tend à montrer les perspectives de développement qui existent dans ce domaine. En outre, l'adoption du *bitcoin* par *Paypal* constitue un atout, ce service étant très exigeant en matière de sécurité.

J'en viens à mes deux questions : vous l'avez dit, la régulation devra d'abord se faire au niveau européen. Où en sont les autorités européennes sur ce sujet, a-t-on une idée de l'avancée de leurs réflexions ? Deuxièmement, les sites d'information parlent de système cryptographique : on comprend qu'une signature puisse être cryptée, par exemple, mais quelle est la signification de ce terme lorsqu'il est appliqué au système des *bitcoins* ?

M. Philippe Adnot. – Je souhaiterais que nous puissions disposer de vos propos par écrit, car je les trouve très intéressants, et je pense qu'ils vont marquer la réflexion sur le sujet, bien qu'il ne soit pas épuisé ! Il est toujours bon de marquer des étapes. Ainsi, au cours de la réunion du 15 janvier 2014 organisée par la commission sur ce même thème, plusieurs intervenants nous avaient expliqué que les monnaies virtuelles ne posaient pas de réelles difficultés. Or, peu de temps après, on a constaté la réalisation de plusieurs opérations loin d'être anodines.

Bien sûr, il faut agir au niveau européen, mais cela ne me paraît pas suffisant. Le système pourrait fonctionner de manière régulée en Europe. Mais cela n'empêchera pas des manœuvres frauduleuses dans d'autres zones, aux Etats-Unis ou au Canada par exemple, d'autant plus que les transactions en *bitcoins* sont anonymes. Je pense donc qu'il faudrait disposer d'un organisme mondial de régulation et de surveillance en ce domaine.

Par ailleurs, vous avez considéré dans votre propos qu'il ne peut pas exister de « planche à *bitcoins* ». Pourquoi une telle certitude ? En effet, on constate aujourd'hui que tous les disques durs peuvent être piratés, que la plupart de nos ordinateurs sont soumis au risque de virus dormants, bref, que l'ingéniosité des hackers est permanente ! Dans ce contexte, qui peut prétendre qu'il n'y aura pas un jour quelqu'un capable de créer du *bitcoin* ?

M. Philippe Marini, président. – Nous répondrons sur le fond à vos questions dans quelques instants. Sur la publication de nos propos, si la commission des finances nous y autorise tout à l'heure, la communication

présentée ce matin sera étoffée puis publiée sous la forme d'un rapport d'information, auquel nous joindrons en annexe les éléments issus de l'enquête effectuée à notre demande par le ministère des finances, avec notamment les éléments comparatifs les plus précis dont nous disposons.

Je pense en outre qu'il serait utile que notre texte puisse faire l'objet d'une traduction en anglais et soit également mis en ligne dans cette langue.

M. Jean Germain. – Voilà un sujet passionnant dont nous avons évidemment intérêt à poursuivre l'exploration ! L'utilité d'une publication en anglais est évidente !

Je pense que ce qui est en jeu ici est l'évolution du métier de banquier. Je discute beaucoup avec mes étudiants et je partage pleinement ce qu'a dit François Marc tout à l'heure : au moment de la création de la carte bleue, c'était quelque chose de terrifiant. Aujourd'hui, les étudiants, qu'ils soient en France, en Angleterre, aux Etats-Unis, au Japon ou en Chine, se montrent très critiques sur le métier de banquier. Les étudiants en gestion, en sciences-économiques ou de Sciences-Po savent très bien ce que sont les régulateurs. La question est de savoir si ce métier doit évoluer.

Je citerai à cette occasion un proverbe que notre collègue Michèle André répète souvent : « ce n'est pas en améliorant la bougie qu'on a créé l'électricité ». De la même façon, je dirais que ce n'est pas en améliorant la banque ou en la régulant que l'on va créer autre chose. Le développement des monnaies virtuelles, avec les tricheries qu'il peut comporter, est un mouvement qu'on ne pourra pas enrayer. Ce sont les banques qui ont créé un certain nombre de difficultés et qui s'opposent partout à la création de nouvelles richesses. Il faut examiner les nouveaux instruments que vous évoquez, car c'est sans doute l'un des sujets dont on parlera le plus dans les cinq à dix ans qui viennent, comme la révolution numérique dans la musique.

Je rappelle que l'on peut déjà, à Berlin ou à Paris, payer des loyers en *bitcoins*. Mes étudiants m'ont donné des exemples de jeunes personnes habitant dans ces villes et y payant leurs loyers en *bitcoins*. De même, à Genève, où je me suis rendu récemment, on compte déjà dix distributeurs de *bitcoins*, et les Suisses comptent en créer d'autres. Bien sûr, cela pose des questions de régulation et de surveillance dont le Parlement aura à traiter, mais ils existent !

Je voudrais également attirer votre attention sur l'arrivée imminente en France et en Europe du système américain *Ripple*, à savoir un protocole de paiement libre qui permet d'échanger toutes les devises, immédiatement, dans la monnaie de votre choix, par exemple en dollars aux Etats-Unis, ou en euros en Europe. Je souligne aussi que l'ordonnance sur le *crowdfunding* a été publiée dans une certaine discrétion, sans susciter beaucoup de réactions, le 30 mai dernier. Elle sera applicable le 1er octobre 2014 pour certaines dispositions, et le 1er octobre 2016 pour d'autres. Elle s'attaque véritablement

au monopole bancaire. Ce n'est que le début mais cela me paraît un sujet important. Je partage complètement ce qu'ont dit le président et le rapporteur général à propos des aspects positifs de ces innovations – le rapporteur général m'ayant semblé le plus confiant à cet égard. Une autre application, Square, existant déjà aux Etats-Unis et au Japon, arrive en Europe : elle permet non seulement de payer avec son portable, mais aussi de faire part de vos observations ou remarques à celui que vous réglez, qu'il s'agisse d'un commerçant ou d'une entreprise. Vous pouvez par exemple vous plaindre de la durée de livraison de votre achat. Certains ne voient pas l'intérêt de ce type d'application, mais il n'empêche que celle-ci fonctionne et qu'elle permet aux services de marketing concernés de connaître les dispositions et les remarques de la clientèle, en direct, sans passer par des intermédiaires écrits. Je citerai enfin l'arrivée en France, au 1er janvier 2015, de l'*Amazon Coin*, soit la monnaie virtuelle du géant américain. J'ai été informé de ces sujets dans le cadre d'une conférence au Collège de France. On apprend bien des choses des universitaires, c'est peut-être ma formation qui me fait parler ainsi. Comme disait Clemenceau, « les polytechniciens connaissent tout, sauf le reste ». Je pense que cela peut s'appliquer à d'autres personnes, et que le reste est important…

Je pense donc qu'au lieu de tout arrêter, il nous faudrait réfléchir à la façon dont nous allons développer et réguler ces monnaies virtuelles ainsi que les activités qui en découlent. On pourrait considérer que les monnaies virtuelles n'ont pas d'avenir et qu'il faut arrêter le mouvement, en se contentant de suivre les conseils de la Banque de France, de la Cour des comptes ou de la Caisse des dépôts. Au contraire, si l'on veut que ceux qui ont vingt-cinq ans aujourd'hui soient demain en mesure d'influer sur les évolutions en cours, je pense qu'il faut aider à développer ces monnaies virtuelles, tout en y mettant des règles. Il faut donc que le débat se poursuive.

Mme Michèle André. – Je pense que ce débat est utile et qu'il mérite que nous fassions des efforts pour comprendre les enjeux liés au développement des monnaies virtuelles. C'est indéniablement complexe. Pour ma part, j'ai la chance de vous représenter à la Banque de France, à l'Observatoire des modes de paiement, qui s'intéresse exclusivement à la sécurité des transactions et en particulier des cartes de toute sorte. Cela me permet de toucher un peu à ces questions.

Nous sommes issus d'une culture de la monnaie, c'est-à-dire du papier. Mais en Nouvelle-Calédonie, où je me suis rendue il y a quelques années, on s'aperçoit que certaines zones conservent des marges d'échange issus du troc, tels que des coquillages. Aujourd'hui, on constate que l'on a quelque peu abandonné la monnaie papier. Par exemple, les chèques, qui ont été longtemps le mode de paiement le plus employé, régressent au bénéfice de la carte, même sans contact.

Dans tous ces systèmes, on trouvera toujours des personnes pour tricher. Mais je pense qu'il faut poursuivre la réflexion plutôt que de se cacher comme si on avait peur de la suite. Il faut d'abord que nous soyons capables de déterminer une référence de base en la matière. Comme Jean Germain, je pense qu'il faut creuser cette problématique des monnaies virtuelles pour la comprendre davantage et faire progresser notre réflexion. Et n'ayons pas peur de nous prêter à des expériences.

M. François Marc, rapporteur général. – S'agissant de la cryptographie, elle s'attache à protéger les messages, en assurant leur confidentialité, leur intégrité et leur authenticité. Dans le cas des *bitcoins*, le caractère décentralisé du système permet d'assurer une très grande sécurité des transactions : celles-ci sont non seulement cryptées mais aussi validées non par un ordinateur central mais à la suite d'une sorte de tirage au sort des ordinateurs appelés à valider le paiement. Ainsi, il n'y a pas stockage en un seul lieu ou dans un seul outil informatique des éléments d'information qui pourraient permettre à une personne de pirater le système. Le détail de ce mécanisme est assez complexe mais, de l'avis des spécialistes, il s'agit d'une innovation remarquable et très sécurisée. C'est un élément rassurant.

Concernant la régulation, évidemment, il serait préférable qu'elle soit mise en œuvre directement à l'échelle mondiale. Ceci dit, de nombreux utilisateurs de *bitcoins* se trouvent en Europe ou aux États-Unis. Une convergence de ces pays en matière de régulation serait déjà un premier pas important. Par ailleurs, la coopération en matière de lutte contre le blanchiment fonctionne relativement bien au niveau international. En Europe, l'exemple de la TVA nous montre qu'il y a toujours un désaccord entre ceux qui veulent assujettir les *bitcoins* – comme le Royaume-Uni et l'Allemagne – et les autres. En ce qui concerne la régulation des plateformes d'échange, une révision de la directive relative aux services de paiement (DSP) est en cours, qui pourrait être l'occasion de mieux réguler ces activités au niveau européen.

Enfin, je souscris à la vision positive de ce type d'innovation exprimée par Jean Germain.

M. Philippe Marini, président. – Voici ce que l'on peut dire sur le risque de « planche à *bitcoins* » : à notre connaissance, à ce jour, tous les piratages ont porté sur le stockage des unités et non sur l'algorithme qui les génère – jusqu'à l'échéance de 21 millions. L'algorithme est lui-même surveillé en permanence par la communauté des utilisateurs. Dans un système open source tel que celui du *bitcoin*, on peut penser qu'une modification ne saurait passer inaperçue et qu'il existerait une sorte d'autocontrôle. Ceci me conduit d'ailleurs à relever le propos de Michèle André : cette construction intellectuelle et technologique a une dimension originale, elle fonctionne de façon circulaire, sur la base d'un réseau cogéré par ses participants, et non de façon centralisée autour d'un acteur dominant. Est-ce une fiction ? La réalité est-elle moins flatteuse ? Au plan

des principes, il convient de reconnaître que les systèmes de monnaie virtuelle, et le *bitcoin* en particulier, sont des mécanismes autogérés qui créent une rupture par rapport aux édifices verticaux et centralisés que nous connaissons ; ceci interpelle.

Comme indiqué par Jean Germain, la remise en cause potentielle du monopole des banques ne peut que faire réagir ces dernières. BNP Paribas, la Société générale et la Banque postale ont par exemple développé le système de paiement par smartphone appelé *PayLib*. Il est clair que les édifices traditionnels vont se défendre et s'efforcer de récupérer à leur profit ces nouvelles technologies.

La commission des finances, quels que soient ses responsables à l'avenir, aura à poursuivre ce chantier. Je crois que nous sommes encore en peine de proposer une initiative législative à ce stade. Nous n'avons pas encore acquis de conviction définitive, même si des voies peuvent être imaginées.

Aujourd'hui, les services d'échange de monnaies virtuelles sont bien considérés comme des prestations de services de paiement (PSP), régis par le code monétaire et financier. En ce qui concerne les plateformes, nous ne sommes donc pas dans le vide juridique. S'agissant de la « chose » qui s'échange, plusieurs options sont possibles : nous pouvons rester encore quelques temps dans le statu quo, c'est-à-dire l'absence de qualification spécifique, ce qui conduit à appliquer le droit commun des biens, notamment en matière de protection des consommateurs, de lutte contre les escroqueries et de règlement des litiges. Comme vous l'a indiqué François Marc, les conséquences fiscales de ce statut ont déjà été tirées par l'instruction fiscale du 11 juillet 2014. Nous pourrions aller plus loin et envisager la qualification d'instrument financier, par analogie avec les devises, ou bien qualifier les monnaies virtuelles de biens meubles. En tous cas, les pouvoirs publics ne sont pas impuissants à réprimer les éventuelles dérives mafieuses ou délinquantes.

M. François Marc, rapporteur général. – Nous pouvons nous féliciter des travaux engagés sur ce sujet par la commission des finances, il y a déjà plusieurs mois. C'est à la lumière des enseignements tirés de la réflexion engagée au Sénat que le Gouvernement a pu établir l'instruction du 11 juillet dernier. Grâce à cette dernière, les choses ont été clarifiées sur le plan fiscal. À l'avenir, il s'agira de voir quels ajustements pourront être apportés à ces dispositions. Nous pourrons opérer ce suivi ; il s'agit d'un sujet d'avenir, sur lequel il est important de se positionner.

À l'issue de ce débat, la commission a donné acte de cette communication à M. Philippe Marini, président, et à M. François Marc, rapporteur général, et en a autorisé la publication sous la forme d'un rapport d'information.

ENGLISH VERSION OF THE COMMUNICATION BY PHILIPPE MARINI AND FRANÇOIS MARC

This is an English translation of the speech given on 23rd July 2014 by Mr. Philippe Marini, president of the committee on finance of the French Senate, and Mr. François Marc,* rapporteur général *of the committee on finance of the French Senate.

Mr. Philippe Marini, president of the committee on finance. – Dear colleagues, I will first make general observations about the development of virtual currencies, and I will then let the *rapporteur général* tell us about the conclusions we can draw from the elements provided by the administration. A few months ago, we asked for a number of comparisons with other countries, since virtual currencies undeniably require an international approach.

On 15th January 2014, the committee on finance of the Senate held a joint public hearing on the development of virtual currencies, and among them the well-know *bitcoin*. The Treasury, the Customs, the *Banque de France* and the anti-money laundering service *Tracfin* were given the chance to expose their positions, as well as an entrepreneur and a scholar working on the subject. As agreed upon, we then sent a questionnaire to the administration and to the economic services of our embassies.

Many things have changed in the last six months: virtual currencies have continued to thrive, carrying along a number of nice innovations and lame ducks; the *bitcoin* hit the headlines on a regular basis; and public authorities have pursued their thinking in order to set up some kind of regulation. On 11th July 2014, the minister of finance and public accounts, Michel Sapin, eventually made a series of announcements based on all this work.

The interest of the committee on finance for virtual currencies should not surprise anyone: this is part of our ongoing interest for the deep transformations caused by the irruption of digital technologies in economic and financial life. As a matter of fact, the digital revolution leaves pretty much nothing unchanged. There are, in the first place, important consequences for our taxation systems: the concentration of value on intangible assets, easily located in fiscal heavens, has led to an erosion of taxation bases – happily major countries are now aware of this problem. Beyond taxation, the digital revolution has turned upside down a number of economic sectors: the monopoly of taxi drivers is disputed by mobile applications like *Uber*, while hotels are now challenged by online booking websites and alternative accommodation offers such has *Airbnb*.

With the development of virtual currencies, something even more important is at stake: the monopoly of emission held by central banks, traditionally considered as a major attribute of sovereignty. The *bitcoin* is the most famous and most successful example of virtual currencies; it is a free, anonymous and decentralized payment system, which allows the exchange of goods and services without using traditional currencies. Strictly speaking, though, the *bitcoin* is not a legal tender for payments, and is not issued in exchange for lawful money. It has no legal status. It is only a support for transactions. So far, the *bitcoin* is, above all, a digital version of barter – sometimes, an archaism can become an innovation, with a little help from technology.

It is not possible, though, to disregard this new trend on the grounds that it might just be another short-lived buzz. More and more e-commerce businesses accept *bitcoins* for payments, including the payment system *PayPal* itself. Such a success builds on real advantages. First of all, extremely low transaction fees – at least allegedly. A recent study from Goldman Sachs found an average of 1% for transaction fees, compared to 2.5% for credit card payments. However, it must be said that an "honest" estimation should include the cost of computer equipment and power supply, as well as the cost of risk associated with the volatility of the *bitcoin* and its insurance. More importantly, the *bitcoin* system is based on an innovative "money creation" mechanism: the users of the system are "rewarded" in *bitcoins* for their participation to the decentralized transaction validating process.

We are well aware that this system carries important risks. These risks have been known from the start, but appeared very clearly in the last few months, and led public authorities to issue a number of public warnings. Firstly, the *bitcoin* suffers from its very important volatility: one *bitcoin* was worth less than one dollar until 2011, and then surged to 1,200 dollars by fall 2013, before moving back to 650 dollars today. As a matter of fact, the *bitcoin* protocol is inherently speculative, because the rhythm of creation of new *bitcoins* is decreasing, until a "cap" of 21 million units is reached in 2140 – in comparison, 12 million units exist today. The system is "locked" for its lifetime. This "organized scarcity" is also the condition of its success, because it guarantees *bitcoin* holders against a devaluation of their assets: artificial "*bitcoin* pumping" is simply not possible.

Another weakness of the system is the absence of a legal guarantee for exchange in "real" currencies. The system entirely relies on the trust people place into it… and a sudden loss of confidence could easily bring it to an end.

Moreover, if *bitcoin transactions* are very secure, the same does not apply to *bitcoin storage*. Most users chose to open virtual "wallets" at online exchange platforms, but the bankruptcy of *Mt. Gox* on 18th February 2014 shows that hacking is more than just a possibility. Of course, people can still chose to store their *bitcoins* at home, on a personal hard drive. That's what

James Howell did, after buying 7,500 *bitcoins* for just a few pounds sterling in 2009 : this young man would certainly be a multi-millionaire today if he had not unintentionally dumped his hard drive in the meantime…

Most importantly, the fact that *bitcoin* transactions are anonymous makes the system a big opportunity for cybercrime and money laundering. On the 15th January public hearing, we were told that the Customs had arrested a drug trafficker who asked for payments in *bitcoins*. Of course, the website *The Silk Road*, the biggest online shopping center for drug dealers and weapon seekers, was shut down by the FBI at the end of 2013. But closing the website does not eliminate the risk: on 28th January 2014, the vice-president of the *Bitcoin Foundation* was arrested in New York and charged on money laundering.

However, those risks should not be overestimated – even if regulators such as the *Banque de France* and *Tracfin* are just doing their job when calling for increased vigilance. For now, the volatility of the *bitcoin* and its lack of legal status should limit its development to a small group of initiated persons: whether you are an individual, a business, or even a criminal network, would you accept to make your payments with something that can shrink to half of its value in a few minutes? Besides, the *bitcoin* does not represent any threat to the global financial stability, given its negligible money stock, just worth a few billions of dollars, as opposed to several billions of billions of dollars for main international currencies. In short, today, the *bitcoin* seems to be more like a niche speculative asset than a credible alternative to money. And as for the few *Monoprix* retail shops that accept *bitcoins* as a means of payment, this is probably not much more than an advertising campaign…

The most important point is that focusing *exclusively* on the risks leads to ignoring the multiple opportunities opened by the development of virtual currencies. The fact that an innovation questions our traditional conceptions should not lead us to reject it automatically. Besides, this rejection would likely remain very theoretical, since it is not possible to prevent individuals to use online exchange platforms…

As an alternative to legal currencies, the *bitcoin* is just beginning to unveil its potential. Those with a far-reaching imagination are already thinking about credit offers or *crowdfunding* systems based on virtual currencies. I personally hold strong reserves about these ideas, but they undeniably deserve to be analyzed – and further developments could make them more interesting.

Beyond that, it is important to understand that the *bitcoin*, more than a "*currency*", is actually a *technology*, an open-source, decentralized and very secure validation protocol. So, if it is possible to validate transactions, why not use this protocol to validate other things, such as passwords, identity documents, degrees and certificates, and even electronic votes? In the near

future, it could become impossible to lie on your graduation – and that would be a great improvement. As for electronic votes, this may be an opportunity to improve the voting system for the French citizens living abroad, which as been under criticism for its lack of security… The decentralized validation protocol is an improvement of cryptography: no central entity acting as a "third party" will ever be in possession of the whole information, and yet this information is perfectly accurate and verified.

Although the *bitcoin* has acquired an important position, there are other virtual currencies – there were others yesterday, such as *Liberty Reserve* or *e-Gold*, and there will be others tomorrow. It is therefore extremely important for public authorities and regulators to understand the full extent of their development, to be proactive, and to step in whenever it appears necessary. The *rapporteur général* will now tell us more about innovation/regulation dialectics, and how to give *bitcoin* stakeholders the security they need.

Mr. François Marc, ***rapporteur général*****.** – Dear colleagues, I remember the time when I was a young university researcher working on payment systems. At that time, the development of credit cards was causing a widespread suspicion among specialists, who saw it as an extremely risky system that was not deemed to have any great future. Even though *bitcoin* might not exactly be the same subject, it's interesting to note that we always face, at first, a global environment of fear and suspicion towards this kind of innovations. While we do not understand every single aspect of this subject yet, the need for regulation is already here.

It is uneasy to give a legal answer to a phenomenon that challenges both our geographical borders and intellectual categories. Nevertheless, regulation is absolutely necessary, in order to secure users and investors, and to prevent abuses which would otherwise undermine the credibility of the whole system.

The president talked about the closing of websites such as *The Silk Road* and the bankruptcy of platforms such as *Mt. Gox*. I would add to the list an event that took place in France: two weeks ago, the *Gendarmes* of the region of Midi-Pyrénées arrested three individuals who operated an illegal *bitcoin* exchange platform, and seized 388 *bitcoins*, worth more or less 200 000 euros.

Luckily, as the public hearing held on 15th January 2014 demonstrated, some private *bitcoin*-related businesses are calling for a regulatory framework. Unsurprisingly, they ask for maximum flexibility, whereas public authorities push for more control. Here's what is at stake: regulating effectively without killing innovation.

I am pleased to say that France reacted promptly to set up a regulatory framework. Ten days ago, Michel Sapin, the minister of finance

and public accounts, announced several measures based on the work conducted at the initiative of our committee:

1. A clarification of the tax regime of virtual currencies. The gains from buying and selling *bitcoins* will be taxed under the progressive rate of the income tax (*impôt sur le revenu*) as commercial profits (*bénéfices industriels et commerciaux – BIC*) if the activity is ordinary, or as non-commercial profits (*bénéfices non commerciaux – BNC*) if the activity is occasional. As a consequence, losses will be deductible under certain conditions. Virtual currencies will also be considered as part of an individual's assets, and subsequently liable for wealth tax (*impôt de solidarité sur la fortune*) and transfer duties (*droits de mutation à titre gratuit*). As for VAT, France will support at the European level a tax exemption, in order to avoid reiterating the unfortunate experience of the massive VAT fraud over CO2 quotas.

2. A limitation of anonymity. Exchange platforms should be required to identify individuals when proceeding to an account opening, a cash withdrawal or deposit, and a transaction. A discussion has been launched on this topic, which is particularly complex since it has to see with the very principles of the system.

3. A cap on payments in virtual currencies, as it already exists for cash payments. In both cases, the reason is to compensate for the anonymity of transactions.

In addition, the prudential supervising authority (*Autorité de contrôle prudentiel et de resolution – ACPR*) estimated that companies operating as exchange platforms of virtual currencies vs. legal currencies would be considered – and regulated – as "provider of payment services" (*prestataire de service de payment – PSP*). For example, the exchange platform *Bitcoin-central* operated by *Paymium* holds an agreement from the ACPR, as its founder explained on the public hearing in January. *Providers of payment services* must respect a number of prudential ratios and anti-money laundering regulations.

How do French positions compare to those adopted by other countries? We have sent a questionnaire to the economical services of our embassies, and another one to the ministry of finance. The answers constitute an original work that will help understand and take upcoming decisions, especially at the European level.

Although all countries are facing the same questions, all do not come up with the same answers – this could be worrying as regards to the transnational nature of virtual currencies. In this international benchmark, France is situated halfway between the most regulatory jurisdictions and the most liberal ones:

1. As for the legal definition of virtual currencies, France has not been more successful than most other countries in establishing an official definition. In some countries like China, Thailand and South Korea, though,

virtual currencies are assimilated to "goods", or more precisely "virtual goods" such as "mp3" audio files. The governor of the Chinese central bank made a parallel between *bitcoins* and stamps collections... Perhaps in a less poetical and so far more isolated way, the German supervision authority (*BaFin*) defined virtual currencies as "units of account", part of the boarder category of "financial instruments", like foreign currencies.

2. Many countries have been keener to tax virtual currencies than to define them – yet tax regimes remain very different. Virtual currency gains are liable for income tax in China, just like online gaming gains; they are taxed as real estate gains in Germany and as capital gains in the United States. Germany, the United Kingdom and other jurisdictions also chose to collect VAT on virtual currencies, but they are still looking for an effective way to do it... In Japan, tax payers are kindly invited to declare their transactions in *bitcoins*.

3. As for the regulation of transactions and exchange platforms, most authorities issued official warnings about the risks taken by users of virtual currencies, and the risks of money laundering and terrorism financing. However, not all countries decided to take regulatory actions in consequence – in fact, most of them tend to think, like Japan, that regulation equals legitimation, and therefore promotion. Countries such as Germany, Israel and Canada only warned *bitcoin* users that they were operating "at their own risks", without a public guarantee of any kind. "Hardline jurisdictions" are represented by China and Russia: these countries forbid, with some exceptions, the use of virtual currencies, and link it with a suspicion of money laundering. France could, in comparison, be deemed "carefully liberal": French authorities do not ban the use of virtual currencies but they subject platforms to the strict regulation of "provider of payment services" (PSP).

4. As for innovation, the United States, Canada and Israel are, unsurprisingly, among the most welcoming countries. Start-ups and business angels thrive while public authorities remain in a largely benevolent laissez-faire attitude. In Cyprus, the University of Nicosia accepts *bitcoins* for the payment of tuitions fees – although it seems few students have actually taken the plunge. That said, France has no reason to be ashamed when it comes to innovation: our finance technologies companies can be remarkably creative in the field of virtual currencies, but also in the field of alternative payments and funding (*crowdfunding*, smartphone payment, etc.).

In short, there are three ways to face the development of virtual currencies. The skeptical way, chosen by several legal experts and economists, who rightly underline that *bitcoin* is not a real currency – thereby forgetting the promising "technical" dimension of the system. The anxious way, chosen by most regulators – it is their job to foresee risks and prevent crises. And the optimistic way, chosen by those who believe that *bitcoin* will

change transactions the same way e-mail changed traditional mailing, and the same way Internet changed traditional publishing. It is important to reassure the skeptical and the anxious, without discouraging the optimistic.

As a consequence, we make the following proposals. Public authorities should keep working and analyzing in the long term the development of virtual currencies. They should keep informing users and other stakeholders about the risks associated with virtual currencies, but also about the rights and protections they have. They should work on an adapted regulatory framework. All these actions are to be undertaken at the European level in order to be truly effective.

As for the legal definition of virtual currencies, we recommend to keep "testing" the use existing categories rather than creating new ones. Several countries, including France, chose to consider *bitcoins* as "goods": this "default status" allows the application of usual provisions for consumer protection, fraud and commercial disputes. This applies to the "thing" – as for the "service", it is already defined and regulated as a "provider of payment services" (PSP).

As in past revolutions brought along by digital technologies, France and Europe have opportunities to take. If we want to succeed together, we must support innovation and, at the same time, keep an eye on it to avoid taking the wrong way.

Exhibit L

SENATE | SÉNAT
CANADA

DIGITAL CURRENCY: YOU CAN'T FLIP THIS COIN!

REPORT OF THE STANDING SENATE COMMITTEE ON BANKING, TRADE AND COMMERCE




The Honourable Irving R. Gerstein
C.M., O.Ont., Chair

The Honourable Céline Hervieux-Payette
P.C., Deputy Chair

June 2015

Ce rapport est aussi disponible en français

****

This report and the committee's proceedings are available online at:
www.senate-senat.ca/banc.asp

TABLE OF CONTENTS

MEMBERS

The Honourable Irving R. Gerstein, C.M., O.Ont., Chair
The Honourable Céline Hervieux-Payette, P.C., Deputy Chair

and

The Honourable Diane Bellemare
The Honourable Douglas Black, Q.C.
The Honourable Larry W. Campbell
The Honourable Stephen Greene
The Honourable Ghislain Maltais
The Honourable Paul J. Massicotte
The Honourable Pierrette Ringuette
The Honourable Scott Tannas
The Honourable David Tkachuk

Ex-officio members of the Committee:
The Honourable Senators Claude Carignan, P.C., (or Yonah Martin) and James S. Cowan (or Joan Fraser).

Other Senators who have participated from time to time in the study:
The Honourable Senators Marjory LeBreton, P.C., Michael L. MacDonald, Fabian Manning, Don Meredith, Percy Mockler, Thanh Hai Ngo, Dennis Glen Patterson, Rose-May Poirier, Nancy Greene Raine, Michel Rivard, Betty E. Unger and David M. Wells.

Parliamentary Information and Research Service, Library of Parliament:
Michaël Lambert-Racine, Brett Stuckey and Adriane Yong, Analysts.

Senate Committees Directorate:
Keli Hogan, Danielle Labonté and Barbara Reynolds, Committee Clerks; and Brigitte Martineau, Administrative Assistant.

ORDER OF REFERENCE

Extract from the *Journals of the Senate* of Tuesday, March 25, 2014:

> The Honourable Senator Gerstein moved, seconded by the Honourable Senator Lang:
>
> That the Standing Senate Committee on Banking, Trade and Commerce be authorized to examine and report on the use of digital currency including the potential risks, threats and advantages of these electronic forms of exchange; and
>
> That the Committee submits its final report no later than June 30, 2015, and that the Committee retains all powers necessary to publicize its findings until 180 days after the tabling of the final report.
>
> After debate,
>
> The question being put on the motion, it was adopted.

Gary W. O'Brien

Clerk of the Senate

EXECUTIVE SUMMARY

The Minister of Finance often asks the Standing Senate Committee on Banking, Trade and Commerce to undertake studies that might be helpful for government policy-making. This was the case when the late Jim Flaherty asked us to study cryptocurrency. Committee members had only a vague idea of what the Minister was talking about. We had no choice but to start at the beginning, with the essential question:

What is cryptocurrency?

The answer is complicated. The passionate and optimistic witnesses we heard from described a genuinely new technology. One that may well usher in a world where money flows as freely as data flows over the Internet; where there are no intermediaries (such as a bank) between you and your transaction, and where the 2.5 billion unbanked people in the world can potentially enjoy access to financial services.

While the Committee gave itself a broad mandate to study "digital currencies" in general, most witnesses discussed the subcategory of cryptocurrencies.

Cryptocurrencies belong to a nascent industry that has brought with it an entirely new vocabulary. In this report we provide a glossary of terms and technical descriptions of what cryptocurrencies are and how they work.

For this executive summary, the Committee will keep it simple:

Cryptocurrencies are a new medium of exchange. In their most basic form, they are a communications technology that offers peer-to-peer (P2P) transactions, eliminating the need for a third-party (ie. a bank) to carry out and authorize the transaction.

Of the hundreds of cryptocurrencies that have been created since 2009, Bitcoin is by far the most popular and has become synonymous with cryptocurrency itself. For these reasons, the Committee thinks a description of Bitcoin is useful to illustrate cryptocurrencies in general.

What is Bitcoin?

Bitcoin is a computer-coded, P2P cash system. Value is measured in units of bitcoin (lower case b) divisible (into satoshis[1]) like a dollar into cents. It relies on its own, unique and novel architecture. Bitcoin (upper case B) is a payment system, a decentralized (controlled by users) P2P network that allows for transactions with built-in security, eliminating the need for a central bank. This is Bitcoin's most distinctive feature – it is not associated with any physical commodity, central banking authority, or government.

Bitcoin transactions are made on the public ledger. The public ledger is exactly what it sounds like – a large bulletin board (written in a cryptic computer database called the blockchain). The public ledger logs and broadcasts transactions to the entire network.

Everyday transactions – using, for example, a debit or credit card to buy a cup of coffee – are tied to a bank. If you have enough money in your account, or credit on the card, the bank authorizes the

[1] Named after the alleged and mysterious inventor of Bitcoin, Satoshi Nakamoto. While an inventor published *Bitcoin: A P2P Electronic Cash System* in 2008 under the name of Satoshi Nakamoto, this inventor has never been identified. So, the true identity of the inventor of Bitcoin is a mystery. The idea of Satoshi Nakamoto is a big part of Bitcoin culture, and when weighing in with their opinion, Bitcoiners are known to say "that's just my two satoshis".

transaction and you get your coffee. If you bought that same cup of coffee with bitcoin, you would simply announce it on the public ledger without the bank or any other financial institution (and all their transaction fees) being involved. The merchant gets their money and you get your coffee.

The public ledger is always accessible through computers literate in the blockchain. It cannot be forged or changed. It provides a permanent record of all bitcoin transactions that have ever happened, a history that within an hour is unalterable.

The *'if a tree falls in the forest'* thought experiment is useful here. In the case of Bitcoin if a tree falls in the forest, and millions of independent computers with cameras record its fall, we can trust that it fell. That is the value of Bitcoin – the mathematical verification by millions of computers reaching a consensus that they witnessed the same thing at the same time. Trust in Bitcoin is a product of that security – which brings us to Bitcoin mining operations.

Bitcoin mining is a kind of lottery, except that your computer has to work in order to have a chance at winning. Of the millions of computers working to verify the public ledger, one will receive bitcoin as a reward. And presto, more bitcoin enters the money supply. Thousands of people are acquiring bitcoin this way, and an incredible amount of computing power has gathered to mine and verify the public ledger.

That's Bitcoin and cryptocurrency in a nutshell. But, our inquiry did not end there. Several times in our study, the Committee heard that bitcoin, the currency, is not the most significant innovation - but rather, the real innovation is blockchain technology.

What is blockchain technology?

Blockchain technology is an ingenious computer code, stored entirely by computers, that forms the underlying architecture for hundreds (if not thousands) of cryptocurrencies and also shows great promise in extending beyond the realm of just currency.

Opportunities

We took a close look at blockchain technology and considered its opportunities. Bringing financial services to the unbanked in the developing world is one of the exciting things we heard about. The Committee developed a vivid sense of how this is possible and already happening.

Another opportunity offered by blockchain technology is its ability to put a person's security and online identity into their own hands. Cyber-attacks for the purpose of identity theft are becoming one of the defining security threats of the 21st Century. Databases filled with our personal information are under attack from nation-states and organized crime. Hackers who target governments, data breaches at large department stores, even celebrity nude photo leaks are the result of the same problem; criminal elements breaking through cybersecurity to their prize; databases filled with valuable personal information.

FBI Director James Comey recently told CBS's 60 Minutes, "*Cybercrime is becoming everything in crime because people have connected their entire lives to the Internet. That's where those who want to steal money or hurt kids or defraud go. And so it's an epidemic."*

A Canadian chartered bank explained that their cybersecurity faces thousands of attacks a day from hackers. Fortunately, they have the resources to fight this onslaught. But the same information consumers are sharing with banks, they are also sharing with online retail outlets. These retail outlets cannot deploy the financial resources a major bank puts into cybersecurity and are left vulnerable to cyber-attacks.

Blockchain technology offers a secure alternative to consumers who do not wish to see their personal information fall prey to the Internet. It offers the ability to transact on the Internet without sharing their personal information with third parties whose databases make juicy targets for hackers. Instead, blockchain technology gives consumers the power to provide their own hack-proof online security.

Risks

The security offered by blockchain technology on the Internet has a flip side, however. The anonymity it provides presents an opportunity for criminals and terrorists. Our study takes a look at the criminality around digital currencies, most infamously represented by Silk Road transactions on the so-called Deep Web – an untraceable part of the Internet that allows users to avoid being found by search engines like Google.

U.S. Senator Tom Carper (Democrat, Delaware), the lawmaker who exposed online drug and criminal elements using Bitcoin, stated, "*The ability to send and receive money over the internet, nearly anonymously, without a third party, has a lot of wide-ranging implications. The government needs to pay attention to this technology and to understand, and where appropriate, address these implications.*"

The 'wide-ranging implications' that Senator Carper refers to are money laundering, terrorist financing, and tax evasion. These are the risks inherent in the technology and they mean that, like all industries, a certain amount of regulation is prudent. But to what extent?

The Committee traveled to New York – specifically to meet with the New York State Department of Financial Services – to hear firsthand about proposed regulations being debated, including BitLicenses. These licenses, currently being developed in consultation with stakeholders, seek to regulate the so-called "on and off ramps" for exchanges that buy and sell cryptocurrencies. In short, licensing means that cryptocurrency exchanges would have to know their customers. The Committee believes this is reasonable.

Conclusion

New technologies attendant to cryptocurrency have unimagined applications. We've heard, and we agree, that blockchain technology is at a delicate stage in its development and use. This is why we urge the Government to explore the vast potential of this technology, while treading carefully when contemplating regulations that may restrict and stifle its use and development.

We believe that the best strategy for dealing with cryptocurrencies is to monitor the situation as the technology evolves; that Canada Revenue Agency and Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) must prepare to navigate and use blockchain technology; that this technology offers new ways to protect the personal information of Canadians; and, finally, that this technology requires a light regulatory touch – almost a *hands off* approach. In other words, not necessarily regulation, but regulation as necessary.

LIST OF RECOMMENDATIONS

The Committee recommends that:

Recommendation 1 (page 13)
The federal government, in considering any legislation, regulation and policies, create an environment that fosters innovation for digital currencies and their associated technologies. As such, the government should exercise a regulatory "light touch" that minimizes actions that might stifle the development of these new technologies.

Recommendation 2 (page 14)
The federal government consider the use of blockchain technology when advantageous to deliver government services and to enhance the security of private information.

Recommendation 3 (page 14)
Digital currency exchanges, the "on and off ramps" of the digital currency system, be defined as any business that allows customers to convert state-issued currency to digital currency and digital currencies to state-issued currency or other digital currencies. To minimize the risks of illegal activity in relation to Canada's anti–money laundering and anti–terrorist financing laws, the federal government should require digital currency exchanges, with the exclusion of businesses that solely provide wallet services, to meet the same requirements as money services businesses.

Recommendation 4 (page 15)
The federal government, on an active and ongoing basis, work with other countries to formulate global guidelines for digital currencies while respecting the "light touch" premise outlined in Recommendation 1 above.

Recommendation 5 (page 15)
The Minister of Finance convene a roundtable with stakeholders, including banks, to look for solutions to the lack of access to banking services for digital currency related businesses, while recognizing the requirements of Canada's anti–money laundering and anti–terrorist financing regime.

Recommendation 6 (page 16)
The federal government, through appropriate federal entities, provide concise information to the public about the risks of digital currencies and alternative payment systems.

Recommendation 7 (page 17)
The federal government, through the Canada Revenue Agency, provide concise information to Canadians about the tax obligations of digital currencies when received as income, held as an investment, or used to purchase goods or services.

Recommendation 8 (page 17)
Due to the evolving nature of digital currencies, the Standing Senate Committee on Banking, Trade and Commerce review this study of digital currencies and their associated technologies to assess the appropriateness of the regulatory environment in the next three years.

CHAPTER 1: INTRODUCTION

On 25 March 2014, the Senate authorized the Standing Senate Committee on Banking, Trade and Commerce (the Committee) to study digital currencies, with a particular focus on the potential risks, threats and advantages of these electronic forms of exchange. The Committee's interest in the topic was partially motivated by media reports about bitcoin being used to make and receive payments over the Internet, and comments by witnesses during our recent statutory review of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* about trends in the use of the Internet to launder money.

Throughout the study, the Committee was reminded that identifying the types of technology that will succeed or fail is difficult – if not impossible – to predict with any accuracy. It seems that, for every television and Internet, there is a Betamax and Segway. In thinking about technology and financial services, the Committee recognized that – over the past decade – the Canadian payments system has changed in substantial ways, including the introduction of Internet-based and mobile-based payment methods. Along with cash, cheques, credit cards and debit cards, Canadians and Canadian businesses now have more ways to make and receive payments, and undertake their banking activities.

While the focus of the Committee's study was "digital currencies" in general, many of our witnesses spoke specifically about cryptocurrencies, which are digital currencies that rely on encryption; in particular, their focus was often Bitcoin. This emphasis is probably not surprising, as Bitcoin is currently the most widely used cryptocurrency. Created in 2009, this decentralized convertible cryptocurrency enables funds to be transferred over the Internet without the need for an intermediary, such as a bank or money services business. Witnesses said that Bitcoin consists of a combination of four technologies that the Committee feels are quite innovative and provide opportunities in both the financial services sector and possibly other areas:

- a decentralized peer-to-peer network;
- a currency-issuing system;
- a transaction verification system; and
- a public ledger relying on the "blockchain."

During the study, 55 witnesses appeared before the Committee in Ottawa. Witnesses included representatives from federal departments and agencies, the Bank of Canada, law enforcement entities, provincial securities regulators, the financial services sector, money services businesses, payment card operators, academics, lawyers, digital currency-related businesses, trade associations, a charity and individuals who participate in the digital currency sector.

The Committee's witnesses spoke about potential definitions for the term "digital currency," common types of digital currencies and potential uses for these currencies. As well, they identified a range of opportunities resulting from the use of digital currencies and their technologies, such as Bitcoin's blockchain technology. Of particular note was the innovation associated with these technologies, the implications for transaction costs, the availability of another payment option, and the impact on the protection of users' identities and the recording of transactions. Finally, the Committee's witnesses highlighted a variety of challenges with digital currencies, technologies and businesses. In this context, such issues as potential criminality and its effects, losses, taxation, and access to

information and protection for users were discussed. Their testimony is summarized in Chapter 3, and their names and organizations are listed in Appendix A.

The witnesses' comments were invaluable in helping the Committee to understand the issues relating to the digital currency sector, and informed our thoughts and recommendations, which appear in Chapter 2. The Committee's conclusions are contained in Chapter 4.

The Committee also took a fact-finding trip to New York City in February 2015 to learn about New York State's proposed regulations for digital currency-related businesses and the potential effects on that state's digital currency sector. The groups and individuals with whom the Committee met in New York City are indicated in Appendix B.

A glossary of digital currency-related terms is provided in Appendix C.

As final points of context for this report, the Committee provides one definition and one data-related caution. For the purposes of this report, the term "digital currency" describes electronic forms of exchange and their associated technologies that operate on the Internet and/or on mobile devices, and that are not issued or governed by a government or central bank. Finally, as the study commenced more than a year ago, the data in Chapter 3 are now somewhat dated, as the digital currency sector has evolved in the last year. For this reason, dates for particular amounts and percentages are indicated, as the data may not reflect the sector's current state.

CHAPTER 2: THE COMMITTEE'S THOUGHTS

A. Digital Currency Types and Uses

When the Committee began its study on digital currencies, a priority was understanding the meaning that should be given to the term "digital currency." One key conclusion that the Committee reached is that elements of the "digital currency sector" – the currencies, the technologies and the businesses – are constantly evolving, and the terms used when discussing the sector are often unclear. On balance, the Committee supports the Department of Finance view that a digital currency is defined by four key characteristics:

- Its value can be held and exchanged without the use of banknotes or coins.
- It is not the official currency of a country.
- It has the intended purpose of being exchanged for real or virtual goods and services.
- Its units can be transferred between individuals, between businesses, and between individuals and businesses.

During the study, the Committee learned about various classification systems for digital currencies, including whether they can be converted to state-issued currencies, and whether they are "centralized," and thus managed by a central authority, or "decentralized," and thereby controlled by the users of the digital currency. The Committee determined that decentralized convertible digital currencies, which are known as cryptocurrencies and of which Bitcoin is the most popular example, should be the focus for any potential regulations.

Cryptocurrencies protect their technology from cyber-attacks and counterfeiting attempts through both encryption and a decentralized network called the public ledger.

In the Committee's view, Bitcoin's blockchain – or public ledger – technology is extremely innovative and has the potential to be used in a growing number of applications, including as a registry to record such events as marriages and real estate purchases, and in the context of "smart contracts" that can be executed by a computer. The Committee firmly believes that additional applications for this technology are on the horizon, that may result in reduced costs, increased choices and convenience, for individuals and businesses.

As well, the Committee agrees with witnesses that – at present – digital currencies have three main roles in Canada:

- a form of money;
- a commodity; and
- a payments system.

In our opinion, the role that digital currencies play as a payments system is perhaps the most significant of the three functions. The Committee holds this view largely because of the blockchain technology that records bitcoin transactions and – as noted above – may hold the promise of many more applications.

The Committee believes that digital currencies, technologies and businesses give rise to a number of opportunities, but like almost all new and emerging technology, there are also challenges and

risks. In our view, the federal government should consider actions in four main areas in order to maximize the opportunities associated with digital currencies, and to manage their associated challenges. These areas are:

- the effect of regulation on innovation in the digital currency sector;
- the use of digital currencies to launder money and finance terrorist activities;
- protecting the users of digital currencies; and
- taxation challenges in relation to digital currencies.

B. Digital Currency-Related Opportunities

During the study, the Committee learned that the emergence of digital currencies has led to a range of opportunities, and that Canada could become a global hub for the digital currency sector if the legislative and regulatory environment is conducive to innovation. In our view, to foster this type of environment in Canada, it is critically important that regulations for the digital currency sector be appropriate.

In particular, the Committee is aware of the potentially negative impacts that future regulations imposed on the digital currency sector could have on innovation. In the Committee's view, digital currencies, especially their associated technology, is among the most notable developments in recent history, and was even compared to the invention of the Internet itself by several witnesses. Blockchain technology is particularly promising as a means to transact without a third party and as a permanent public database. The Committee believes that, in time, even incumbent financial institutions will recognize the benefits of this technology and may adapt it to meet their needs. Many witnesses stated that this technology is at a risk of failure because of poor judgement on the part of regulators and lawmakers. Therefore the Committee understands that familiar, centralized solutions built from a centralized financial system are unsuitable for this decentralized payments technology. Believing that conscious efforts are required to support digital currency-related innovation, the Committee recommends that:

Recommendation 1:

The federal government, in considering any legislation, regulation and policies, create an environment that fosters innovation for digital currencies and their associated technologies. As such, the government should exercise a regulatory "light touch" that minimizes actions that might stifle the development of these new technologies.

The Committee heard of the many opportunities resulting from the emergence of digital currencies and their technologies. Lowering transaction costs may be the first opportunity realized by the marketplace, as increased choices for payment systems may put pressure on the current high cost for international remittances. In our opinion, lower costs are relevant for the many Canadians making international transfers.

As well, it seems to the Committee that there is also an opportunity for the government. Blockchain technologies that facilitate identity protection can benefit Canadians, as governments seek to protect the information they hold on behalf of its citizens. The Committee recognizes that, in recent years,

hackers have targeted government databases, including those at the Canada Revenue Agency, in an attempt to steal identities and other personal information. In our view, compared to centralized databases, blockchain technology may provide a more secure way to manage information, as it does not rely on security software developed by third parties. From this perspective, the Committee recommends:

Recommendation 2:

The federal government consider the use of blockchain technology when advantageous to deliver government services and to enhance the security of private information.

C. Digital Currency-Related Risks

1. Use of Digital Currencies to Launder Money and Finance Terrorist Activities

In the Committee's view, potential criminality is perhaps the greatest challenge to be managed. The Committee has a long and ongoing interest in issues of criminality, having conducted two statutory reviews of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, and having held hearings on various proposed amendments to the Act.

The Committee understands that digital currencies can be attractive to criminals who want to launder money, finance terrorism or perpetrate other crimes. As well, the Committee recognizes that it is the anonymity of digital currencies, and the ease they can be used to make domestic and – particularly – international transfers, that may make them conducive to criminal activity.

In the Committee's opinion, illicit users of digital currencies are most readily identified at the "on and off ramps," or digital currency exchanges, where digital currencies are converted to and from state-issued currencies. Furthermore, in recognizing the Committee's past and likely future examinations of Canada's anti–money laundering and anti–terrorist financing regime, we also believe that the similarities in the operations of digital currency exchanges and money services businesses give rise to a need for identical obligations for these two groups in relation to that regime. Therefore, the Committee recommends that:

Recommendation 3:

Digital currency exchanges, the "on and off ramps" of the digital currency system, be defined as any business that allows customers to convert state-issued currency to digital currency and digital currencies to state-issued currency or other digital currencies. To minimize the risks of illegal activity in relation to Canada's anti–money laundering and anti–terrorist financing laws, the federal government should require digital currency exchanges, with the exclusion of businesses that solely provide wallet services, to meet the same requirements as money services businesses.

Partially because of the Committee's previous studies on Canada's anti–money laundering and anti–terrorist financing regime, the Committee is aware of the global nature of the real and potential

criminality that is facilitated by digital currencies and – thereby – the need for global solutions. In today's globalized world, improvements in technology have made it easier for legitimate and illegitimate businesses to transact internationally.

A recurring theme with cryptocurrencies is the idea of *consensus*. It is consensus which provides transaction verification, and it is consensus which gives value to a cryptocurrency. As it is a theme of cryptocurrency, so it must be a theme in laws and regulations. The Committee believes that, where cryptocurrencies are shaped by network consensus, laws and regulations ought to be shaped by jurisdictional consensus.

In the Committee's view, coordinated international efforts are a particular priority to effectively counter the international nature of criminal activities and to prevent "jurisdiction shopping" by digital currency-related businesses. Consequently, the Committee recommends that:

Recommendation 4:

The federal government, on an active and ongoing basis, work with other countries to formulate global guidelines for digital currencies while respecting the "light touch" premise outlined in Recommendation 1 above.

During the study, the Committee was told that the association of certain digital currencies with criminal activity has had a negative effect on industry-wide growth. One obstacle is regulatory uncertainty. Regulators – such as Quebec's Autorité des marches financiers and New York State's Department of Financial Services – have started to implement licensing requirements for certain digital currency-related businesses in their jurisdictions.

Another obstacle faced by some cryptocurrency businesses is the inability to establish banking relationships.

The Committee listened to witnesses describing their difficulty in accessing financial services. The Committee does not believe that banks are prejudiced against cryptocurrency businesses, and think this is perhaps a result of banks being concerned about inadvertently violating the obligations of Canada's anti–money laundering and anti–terrorist financing regime. The Committee is mindful that, before money services businesses were regulated, banks were reluctant to accept these businesses as customers. In that context, the Committee recommends that:

Recommendation 5:

The Minister of Finance convene a roundtable with stakeholders, including banks, to look for solutions to the lack of access to banking services for digital currency related businesses, while recognizing the requirements of Canada's anti–money laundering and anti–terrorist financing regime.

2. Protecting the Users of Digital Currencies

During the study, the Committee learned that digital currency losses can occur in a variety of situations, and the Committee believes that any loss of funds – whether through cyber-theft,

bankruptcy or price volatility – is regrettable for financial services providers and their customers. The Committee recognizes that such losses are not limited to digital currencies in their role as a form of money or a commodity; in that regard, the periodic volatility in the relative value of the Canadian dollar and the current decline in oil prices should be remembered. In the same way individuals presumably consider the risk-return trade-off when purchasing or holding state-issued currencies or commodities, the Committee urges this type of analysis when considering the purchase of digital currencies.

The Committee has come to appreciate the importance of the digital currency sector being aware of any weaknesses in their technologies and systems, and of taking appropriate efforts to protect against cyber-attacks. Equally, the Committee believes that individuals must consider the risks that may result when holding funds in digital wallets, which are also being used for digital representations of state-issued currencies, or when placing their digital currency with digital currency exchanges, which are not regulated prudentially. While the Committee does not believe that these issues warrant regulation, the Committee encourages digital currency-related businesses and individuals to be mindful of these potential risks.

While securities regulation is not within the federal jurisdiction, the Committee is confident that Canada's securities regulators have expertise in assessing risk, and encourages them to continue to release relevant and timely information about digital currency-related risks. As well, notwithstanding our earlier comments about the need for digital currency-related businesses and individuals to be aware of weaknesses and risks, the Committee believes that the federal government has an important role to play in developing policies and providing information that will help consumers and merchants assess the benefits and risks of various financial products, and make the choices that are most appropriate for their situations. For these reasons, the Committee recommends:

Recommendation 6:

The federal government, through appropriate federal entities, provide concise information to the public about the risks of digital currencies and alternative payment systems.

3. Taxation Challenges in Relation to Digital Currencies

During the study, the Committee learned that there is some question about the taxation of digital currencies, such as bitcoin, which are used as a form of money by some and as a commodity by others. The Committee is also mindful that, due to the difficulties associated with tracing digital currency transactions, the government may have difficulty combating tax evasion that is committed using digital currencies. Nevertheless, the Committee urges the government to work with other countries and in appropriate venues to address, in particular, this taxation issue.

The Committee believes that providing the public with specific and comprehensive guidance about the taxation rules for digital currencies – whether received as business or employment income, held as an investment, or used to buy goods and services – would assist individuals and businesses in understanding the rationale for these rules and in complying with them. As well, further examination of the use of digital currencies as a form of money would assist the government, particularly the Canada Revenue Agency, in determining whether other taxation rules – such as those that apply to

foreign currencies – should apply to digital currencies. In that context, the Committee recommends that:

Recommendation 7:

The federal government, through the Canada Revenue Agency, provide concise information to Canadians about the tax obligations of digital currencies when received as income, held as an investment, or used to purchase goods or services.

D. Focusing on the Future

In the Committee's view, there is currently not a need for the government to take actions to regulate digital currencies beyond those that are specifically mentioned in our recommendations. The Committee believes that additional actions could have unintended consequences, such as hampering the innovative aspects of digital currencies that may hold great future promise in finance and other areas. With traditional methods of payment and institutions, individuals are expected to undertake due diligence, and – in our view – the same situation should exist regarding digital currencies, their technologies and businesses.

The Committee understands that, as can be seen with other new technologies in the payments sector, the technology associated with digital currencies is dynamic and evolving rapidly; thus, the opportunities and challenges identified in this report may no longer be applicable in just a few years. The Committee intends to revisit the issue of digital currencies, and, at that time, the Committee hopes to learn about the evolution of the digital currency sector, and to make recommendations for further federal action to maximize the opportunities and manage the risks that have arisen since this study. In this light, the Committee recommends that:

Recommendation 8:

Due to the evolving nature of digital currencies, the Standing Senate Committee on Banking, Trade and Commerce review this study of digital currencies and their associated technologies to assess the appropriateness of the regulatory environment in the next three years.

CHAPTER 3: WITNESSES' TESTIMONY

A. Digital Currency Types and Uses

1. Definitions for "Digital Currency"

Some of the Committee's witnesses spoke about the term "digital currency." According to the Department of Finance, there is no universally agreed upon definition for the term; it may include electronic forms of a state-issued currency, such as prepaid access cards and wire transfers. Similarly, the Bank of Canada stated that the term may include online credit card transactions, Interac transactions sent by email, online bill payments and the cashing of cheques with a smart phone's camera. The Bank also indicated that individuals often use terms such as "e-money," "e-cash," "digital money," "digital currency" and "virtual currency" interchangeably, erroneously believing that they have the same meaning.

The Bitcoin Alliance of Canada suggested that a "virtual currency" is based on a ledger, a "digital currency" only exists digitally, and a "cryptocurrency" is based on cryptography. It identified cryptocurrencies as a subset of digital currencies, which are a subset of virtual currencies.

The Department of Finance said that it considers a digital currency to have four characteristics:

- its value can be held and exchanged without the use of banknotes or coins;
- it is not the official currency of a country;
- it has the intended purpose of being exchanged for real or virtual goods and services; and
- its units can be transferred between individuals, between businesses, and between individuals and businesses.

2. Common Types of Digital Currency

Witnesses noted that digital currencies can be classified in several ways. The Department of Finance indicated that a digital currency can be classified in relation to its convertibility: a "convertible" digital currency can be converted to a state-issued currency, while a "non-convertible" digital currency can be used only to purchase real or virtual goods and services from particular retailers. It suggested that convertible digital currencies should be the primary focus for possible regulation.

As well, the Bank of Canada and the Department of Finance identified a classification method that focuses on whether a particular digital currency is "centralized" or "decentralized." According to the Bank, a centralized digital currency can be used to purchase a variety of goods and services, and is issued – and often managed – by a central authority that typically has a corresponding debt for the amount of digital currency that it has issued. The Department described these central authorities as entities that – in relation to a particular digital currency – verify the transactions, determine the supply, and create rules regarding exchange or use.

According to the Bank of Canada, prepaid payment cards are a good example of a centralized digital currency; in this case, such entities as Visa and MasterCard are the central authorities. The Bank also provided another example of a centralized digital currency: the pre-paid Octopus card in Hong

Kong; originally intended as a prepaid transit card, the card has become generally accepted by retailers. The Royal Canadian Mounted Police mentioned Liberty Reserve, which had a central authority that issued Liberty Reserve dollars and was used as part of a global money laundering scheme.

The Bill and Melinda Gates Foundation discussed the mobile phone-based centralized digital currencies that are used in a number of developing countries. For example, it mentioned M-PESA, which is owned by Vodafone – a mobile telecommunications company – and is used in Kenya and other countries. It said that M-PESA allows individuals to exchange an electronic form of the local currency through their mobile phones.

The Bank of Canada characterized decentralized digital currencies, which are sometimes referred to as cryptocurrencies, as digital currencies that operate over peer-to-peer networks where no single entity manages the currency or assumes a debt for the currency that has been issued. Samir Saadi, of the University of Ottawa, stated that digital currencies and online payments have existed for decades, but that cryptocurrencies are unique because decentralized peer-to-peer networks allow the ownership of digital currencies to be transferred without the need for an intermediary.

In providing examples of decentralized digital currencies, the Department of Finance noted that bitcoin is a decentralized, convertible digital currency. The Canadian Virtual Exchange and the Bank of Canada commented on litecoin, which is the second most popular decentralized, convertible digital currency. The Bank also mentioned peercoin and Ripple.

Ripple Labs described Ripple as an open-source payment protocol designed to provide interoperability among the payments systems of financial institutions, clearing houses and central banks. It indicated that the Ripple network relies on a decentralized public ledger and cryptographic technology that are similar to those used by Bitcoin; however, its "consensus" verification process differs from that used by Bitcoin. It also mentioned that all currencies – state-issued or digital – can be traded over the Ripple network, and that the system has its own digital currency – the XRP – that is used as a security mechanism and to convert currencies. TD Bank Financial Group commented that some banks are experimenting with the Ripple network to exchange funds between them.

The Bitcoin Strategy Group stated that, as of 9 April 2014, there were more than 100 different decentralized, convertible digital currencies worldwide. According to Bitcoin Foundation Canada, as of 2 October 2014, between 500 and 1,000 cryptocurrencies were being used, and between 50 and 100 digital currency exchanges were converting bitcoin to other digital currencies. Andreas Antonopoulos, author of *Mastering Bitcoin*, highlighted that anyone can – at minimal cost – create a new digital currency that is secure and globally accessible.

3. Potential Uses for Digital Currencies

A number of the Committee's witnesses identified the various ways that digital currencies are being used in Canada, and generally commented on three roles: a form of money; a commodity; and a payments system. They also discussed other potential uses for digital currencies.

(i) A Form of Money

The Bank of Canada discussed the definition for the term "money," indicating that three characteristics must exist:

- in being a medium of exchange, it must be generally accepted among individuals and businesses;
- in being a unit of account, it must allow the value of various goods and services to be compared; and
- in being a store of value, it must enable individuals and businesses to assume – with confidence – that its value will be stable over time.

According to the Department of Finance, if digital currencies become both a stable store of value and generally accepted as a means of payment for goods and services, they could become more widely used as money. That said, it noted that long-term use of digital currencies as a form of money would be unlikely, partially due to volatility in the price of digital currencies, as has occurred with bitcoin.

The Canadian Payments Association suggested that confusion exists about the role that digital currencies play in the Canadian economy. In its view, digital currencies – particularly bitcoin – do not constitute money, as they are not a medium of exchange, a unit of account and a store of value.

Similarly, the Bank of Canada highlighted that bitcoin and other cryptocurrencies currently are not a popular medium of exchange. As of 2 April 2014, less than 200 Canadian retailers accepted bitcoin. Regarding bitcoin as a unit of account, the Bank noted that the value of a transaction where bitcoin is the method of payment is often considered in terms of a state-issued currency. It also suggested that, as of 2 April 2014, the price of bitcoin was forty times more volatile than the relative value of the U.S. dollar; thus, bitcoin is not a stable store of value.

The Department of Finance stated that the *Currency Act* governs legal tender and currency, lists the characteristics of coinage and banknotes, and identifies the dollar as Canada's monetary unit. It highlighted that the Act does not limit the use of digital currencies for transactions in Canada, and that merchants can accept a variety of methods of payment in exchange for goods and services, including U.S. dollars and Canadian Tire "money." Joshua Gans, of the University of Toronto, indicated that – in Canada – taxes must be paid with legal tender; therefore, as long as bitcoin is not considered to be legal tender, the Canadian dollar will be required for that function.

The Bitcoin Alliance commented on the meaning that Canadian law gives to the term "money"; "legal money" likely does not include bitcoin, which is not state-issued and is not universally accepted. It also noted that the Canada Revenue Agency and the Bank of Canada do not view bitcoin as "legal money," and observed that bitcoin cannot denominate a negotiable instrument under the *Bills of Exchange Act* if it is not "legal money."

HISTORY *of* MONEY IN CANADA

1600 - 1850 Wampum (strings and belts with beads and shells) and copper shields

1600 - 1770 Beaver pelts, wheat, moose skins, and French and Spanish coins

1685 - 1759 Card money (playing cards) and paper money

1700 - 1870 UK and US coins

1817 - 1934 Bank notes issued by commercial banks

1854 Introduction of *Currency Act* and Canadian dollar (UK coins and US coins declared legal tender)

1867 - 1935 Dominion notes issued by the provinces

1870 Canada's first coins issued

1935 First bank notes issued by the Bank of Canada

1970s Credit cards

1990s Debit cards

2009 Cryptocurrencies?

Source: Bank of Canada, A History of the Canadian Dollar, December 2005, figure prepared by the Library of Parliament.

According to John Jason, of Norton Rose Fulbright Canada, the *Currency Act* states that any contract in Canada that references "money" is referring to Canadian dollars; thus, if contracts refer to payment in bitcoin, they will have to describe the way to make that type of payment. He also said that the government became the issuer of currency to support economic activity and so that people had confidence in using paper notes as a medium of exchange. In his view, people may not have confidence in bitcoin, as its price fluctuates significantly; that said, those who advocate using bitcoin believe that its price will stabilize as its supply rises.

Jeremy Clark, of Concordia University, highlighted the Royal Canadian Mint's "Mint Chip" project, stating that Mint Chip is a "digital representation" of Canadian currency.

(ii) A Commodity

The Department of Finance pointed out that many people have invested in digital currencies, and – on 26 March 2014 – noted that an exchange-traded fund based on bitcoin would soon be available in the United States. Similarly, Joshua Gans indicated that a number of holders of bitcoin are not exchanging their bitcoin for goods and services; instead, they are retaining their bitcoin, which will be beneficial if the price of bitcoin rises. According to the Department of Finance, it is too early to determine whether digital currencies will be successful as a commodity, as any value they might have in this regard is linked to their use as a currency. Bitcoin Foundation Canada suggested that, although bitcoin is likely not a security, it can be used as the unit of account for a securities transaction, such as an investment fund denominated in bitcoin.

Samir Saadi stated that New York's Wall Street has recently shown an interest in digital currency trading. He highlighted that hedge funds are being created that involve strategic trading based on volatility in the price of digital currencies. He also mentioned that Nasdaq Group is providing Noble Markets – a company that facilitates institutional trading in bitcoin – with software used by major securities exchanges, and that the New York Stock Exchange is providing Coinbase – a digital wallet provider and the first U.S.-based digital currency exchange – with capital. In his view, Coinbase appears to be a reliable and secure platform for trading in bitcoin.

The Ontario Securities Commission indicated that platforms for trading bitcoin-based derivatives are being developed in the United States, and that the U.S. Securities and Exchange Commission has received applications to create exchange-traded funds using bitcoin.

The Department of Finance suggested that digital currencies, as a commodity, could be subject to securities regulation in Canada. According to Quebec's l'Autorité des marchés financiers and the Ontario Securities Commission, because of their current form, digital currencies do not qualify as "securities" or "derivatives" under their provinces' securities and derivatives legislation; consequently, they are not regulated as such. In their view, if digital currencies are packaged as an investment product or a derivative, that legislation would apply. The Ontario Securities Commission also stated that any publicly traded digital currency-related business is subject to the same regulatory requirements as other publicly traded companies, including disclosure to investors about material risks.

Elliot Greenstone, of Davies Ward Phillips & Vineberg LLP, noted that no Canadian securities regulator has indicated whether digital currencies should be treated as a security or derivative for the

purposes of securities law. He highlighted l'Autorité des marchés financiers' recent decision to monitor digital currencies pursuant to Quebec's *Securities Act*, *Derivatives Act* and *Money-Services Businesses Act*. He also mentioned that the *Securities Act* does not define the term "security," although it does define the term "investment contract."

Regarding Ontario's securities legislation, Elliot Greenstone and John Jason suggested that bitcoin may not fall within the definition for the term "security," as there is no person or entity that "issues" bitcoin. Elliot Greenstone said that the Ontario Securities Commission plans to monitor investment activities that are related to digital currencies and to take action when Ontario's *Securities Act* is violated.

(iii) A Payments System

The Department of Finance and the Canadian Payments Association stated that because of Bitcoin's framework, it is like a payments system. The Canadian Payments Association commented that a digital currency may not be appropriate for Canada's clearing and settlement system, as the system facilitates transactions in Canadian dollars; in 2012, $16.7 trillion in payments – excluding cash transactions – were made in Canada. It indicated that, of these payments, 80% was cleared through the Canadian Payments Association's systems, including the Automatic Clearance Settlement System – which is used by private payment networks, such as Interac, for clearing and settlement – and the Large Value Transfer System; the remaining 20% was cleared by credit card companies, within financial institutions or through closed-loop mechanisms, such as prepaid payment cards and digital currencies.

According to the Interac Association, as of 12 June 2014, its network was used an average of 12 million times daily through Automated Teller Machine (ATMs), e-commerce purchases and person-to-person e-transfers; these transactions represented approximately 55% of all payment card-based transactions. As well, the Canadian Payments Association mentioned that the unregulated payments sector, which includes PayPal and Google, has not yet identified a need to access the Canadian clearing and settlement system. The Interac Association and PayPal stated that they do not process digital currency payments.

Using global data, the Canadian Payments Association estimated that – as of 10 April 2014 – there were between 1,000 and 2,000 daily transactions in Canada involving bitcoin, which represented 1/100 of 1% of the total volume of daily Canadian payments transactions. It noted that developers of digital currencies are not eligible for membership in the Canadian Payments Association, as they are not regulated financial institutions. Bitcoin Foundation Canada said that, as of 2 October 2014, approximately 80,000 Bitcoin transactions occurred daily around the world.

SELECTED POINT-OF-SALE PAYMENT METHODS USED IN CANADA

Cash

According to the Bank of Canada, while the use of cash for retail payments is declining due to advancements in payment method technologies, cash is Canada's most commonly used and accepted form of retail payment, as it is perceived to be less costly, easier to use, more secure and more widely accepted than debit cards and/or credit cards. In 2013, cash accounted for 43.9% of the volume and 23.0% of the value of point-of-sale transactions.

Debit Cards and Credit Cards

According to the Bank of Canada, debit card use increased significantly over the period from 1994, when the Interac system was introduced, to the early 2000s; credit card use has grown consistently since 2000, partly due to an increasing number of rewards programs. Bank of Canada data show that, in 2013, debit cards and credit cards accounted for 21.1% and 30.8% respectively of the volume of point-of-sale transactions, and 25.1% and 45.9% respectively of the value of such transactions. Contactless payments represented 2.9% of debit card and 19.3% of credit card point-of-sale transactions in that year.

Cryptocurrencies

According to the Canadian Payments Association, as of 10 April 2014, there were between 1,000 and 2,000 daily transactions in Canada involving bitcoin. These transactions represented 1/100 of 1% of the total volume of Canada's daily payments transactions.

Visa Canada Corporation and MasterCard suggested that an important indicator of whether Bitcoin has a role to play in the Canadian payments system is the number of merchants that accept bitcoin as a method of payment. The Department of Finance said that, as of 26 March 2014, approximately 1,500 businesses around the world accepted – or were willing to accept – bitcoin; of these, about 200 were located in Canada. It also noted that many of these businesses are online retailers, particularly in the technology sector, or offer online gambling; examples of businesses that accept bitcoin include Overstock.com, WordPress, Zynga, Tesla and Virgin Galactic. The Department suggested that Canadian merchants that accept bitcoin as a method of payment, and the extent to which they are treating bitcoin as a currency and paying suppliers with it, should be identified.

According to the Canadian Virtual Exchange, as of 9 April 2014, there were 22 Canadian merchants accepting bitcoin as a method of payment for online purchases; it stated that another 150 Canadian merchants would be doing so by 9 May 2014, and an additional 1,000 by October 2014. Andreas Antonopoulos identified Bitcoin as being most commonly used for charitable donations and tipping.

MasterCard indicated that digital currency payments could be incorporated into its network or processed through a separate network if digital currencies become regulated. In its view, digital currencies can be useful for person-to-person payments and business payments. It also noted that it has U.S. patents for digital currencies.

TD Bank Financial Group said that banks incur costs in settling transactions; thus, they would welcome less expensive forms of settlement, including through the use of digital currencies if appropriate regulation and security exist. As well, TD Bank Financial Group noted that it does not compete with digital currencies.

PayPal mentioned that it does not accept deposits in PayPal wallets in the form of cash or digital currencies. MoneyGram International commented that, while it does not currently transfer digital currencies, it would consider doing so if these currencies are regulated.

Selected Payments Systems Used in Canada

CRYPTOCURRENCIES

Some cryptocurrencies function as both a currency and a decentralized payments system, such as bitcoin and Bitcoin respectively. Users of cryptocurrency-based payments systems perform all steps in a transaction, interacting with each other directly through an Internet-based peer-to-peer network without the need for a central computer server. Transactions are recorded on a public ledger, which is shared across the network, and their validity is verified through cryptographic techniques. Merchants accepting cryptocurrencies may use payment processors, such as BitPay, Coinbase and BitNet, to help with clearing and settling cryptocurrency payments. As well, payment processors may convert such payments into a state-issued currency for deposit into a merchant's bank account.

PAYPAL

PayPal is a third-party intermediary that verifies and settles online transactions between a purchaser and a merchant. It allows a merchant to accept a credit card or debit card as a method of payment without having a direct relationship with the credit card or debit card company, or with a payment processor that clears and settles transactions. Verification is conducted on the PayPal website when the purchaser opens an account and registers his/her financial information with PayPal. Settlement occurs when a payment is transferred by PayPal from the purchaser's account to the merchant's account.

CREDIT CARDS

In Canada, Visa and MasterCard are structured in accordance with the four-party model: the cardholder; the merchant; the card issuer; and the payment processor. A fifth participant is the credit card company itself. Visa and MasterCard have proprietary clearing systems that are not subject to the Canadian Payment Association's rules or standards.

DEBIT CARDS

Like credit cards, point-of-sale debit card transactions in Canada are structured in accordance with the four-party model; with these transactions, a fifth participant is the Interac Association. The Interac Association's Direct Payment network is decentralized, with clearing and settling occurring at the financial institution where the funds are located. The Interac Association's members clear and settle their transactions through the Canadian Payments Association's Automated Clearing Settlement System.

The Canadian Bankers Association indicated that Canada's banks support the creation of new ways for consumers and merchants to engage in e-commerce, and noted that banks are involved in promoting new payments technologies, such as near field communication (NFC) for contactless payment cards and mobile wallets on cell phones. It also mentioned that Canadian banks and credit unions have been collaborating on a set of principles, entitled the Canadian NFC Mobile Payments Reference Model, for mobile payments. Similarly, MasterCard said that, as cash is used less often as a method of payment, payments system developments have included contactless payment cards, mobile payments and direct deposit to prepaid cards.

The Royal Bank of Canada commented on its "RBC Secure Cloud," which allows its clients to choose among debit, credit or gift cards when making a mobile payment; sensitive information is stored on its servers in Stratford, Ontario and Guelph, Ontario, and not on a cell phone. It also noted that it offers free person-to-person transactions that can be accessed through bank accounts or Facebook.

The Interac Association mentioned Interac Flash, which allows contactless use of a debit card and can be used with other technologies, such as RBC Secure Cloud. The Canadian Payments Association commented that it has participated in the implementation of products that enable consumers to make deposits with photographs of cheques and to use contactless debit cards.

PayPal said that it allows users to transfer money or make payments online without having to disclose banking or financial information. It noted that – as of 12 June 2014 – $1 of every $6 spent globally on e-commerce was processed through PayPal, and it had 148 million active registered accounts; 5.5 million of these accounts were held in Canada. It also stated that it processed $27 billion in mobile payments in 2013, an increase from $600 million in 2010.

According to the Bill and Melinda Gates Foundation, mobile phone-based digital currencies – such as M-PESA – are used as digital payments systems for making low-cost transfers and payments. It said that there are more than 250 mobile phone-based payments systems worldwide, which together have more than 200 million users. It explained that an individual can use M-PESA to exchange cash for an electronic form of the local currency through an agent, generally without a fee, and then – at a cost of $0.02 or less in some countries – transfer this electronic money to another individual using his/her mobile phone; the recipient can then exchange the electronic money for cash at an agent, with the fee for this service ranging from $0.25 to $0.35.

MasterCard highlighted the use of mobile phones in some countries – such as the Democratic Republic of the Congo – to receive government benefits and as a means of identification, as few individuals have access to a bank account. Visa Canada Corporation mentioned Fundamo, a South African company that it owns; the company enables individuals to send money to others using mobile phones and text messages, with the mobile phones linked to a mobile network operator account or a bank account.

(iv) Other Potential Uses

According to the Bitcoin Embassy, digital currencies are not simply another payments system to be studied within the traditional framework for financial services, and nor are they a new form of money that can be examined like a foreign currency or a commodity; rather, they could be viewed as a new technology that is replacing their obsolete predecessors. Elliot Greenstone said that many research

papers refer to cryptocurrencies as "pseudo-fiat currencies." In his view, this term suggests that cryptocurrencies have the characteristics of a commodity, such as having a limited supply, and of a currency, such as being used to make payments.

The Bitcoin Embassy stated that new products involving digital currencies are currently being developed, such as smart contracts, decentralized autonomous corporations, and decentralized markets that enable peer-to-peer sales of goods and services. Similarly, Ripple Labs commented on smart contracts, which it described as contracts having a set of automatic rules that are entirely readable and operable by computers. L'Autorité des marchés financiers noted that, in the United States, there have been attempts to use Bitcoin's technology to develop decentralized securities exchanges.

Andreas Antonopoulos said that Bitcoin's technology in relation to its public ledger is being used to record events, such as the purchase of automobiles, company shares and real estate, as well as marriages. The Bill and Melinda Gates Foundation suggested that this technology could be used to develop title registries for land and other types of assets, from which low-income people would benefit; Ripple Labs and Elliot Greenstone also mentioned title registries. Moreover, Elliot Greenstone indicated that the blockchain technology could potentially be used to rent cars with digital keys.

Andreas Antonopoulos noted that some individuals and organizations are providing "digital tokens" when a transaction is submitted on the blockchain; these tokens allow an individual or organization to access a service, such as Internet bandwidth or an AirBnB property.

As well, Andreas Antonopoulos noted that a business operating internationally could use a digital currency to pay employees who live in various countries, and suggested that a computer programmer could easily incorporate a digital currency into payroll software.

4. Bitcoin as an Example

In commenting on digital currencies, the Committee's witnesses often focused on bitcoin and Bitcoin, the currency and the payments system respectively. In particular, they spoke about the creation of the underlying technology and the functioning of the payments system, and the currency that is used with that system.

(i) The Technology and Payments System

According to the Department of Finance and the Bank of Canada, the term "Bitcoin" generally describes the decentralized, cryptographic network that functions as the payments system for "bitcoin," which is the digital currency used by Bitcoin.

The Bitcoin Embassy and Andreas Antonopoulos described Bitcoin as a combination of four new mathematical and cryptographic technologies: a decentralized peer-to-peer network; a decentralized currency-issuing system; a decentralized transaction verification system; and a public ledger, called the blockchain, that records transactions. The Bitcoin Embassy noted that Bitcoin's most distinctive features are its decentralized and interdependent payments system and digital currency, which cannot function without each other.

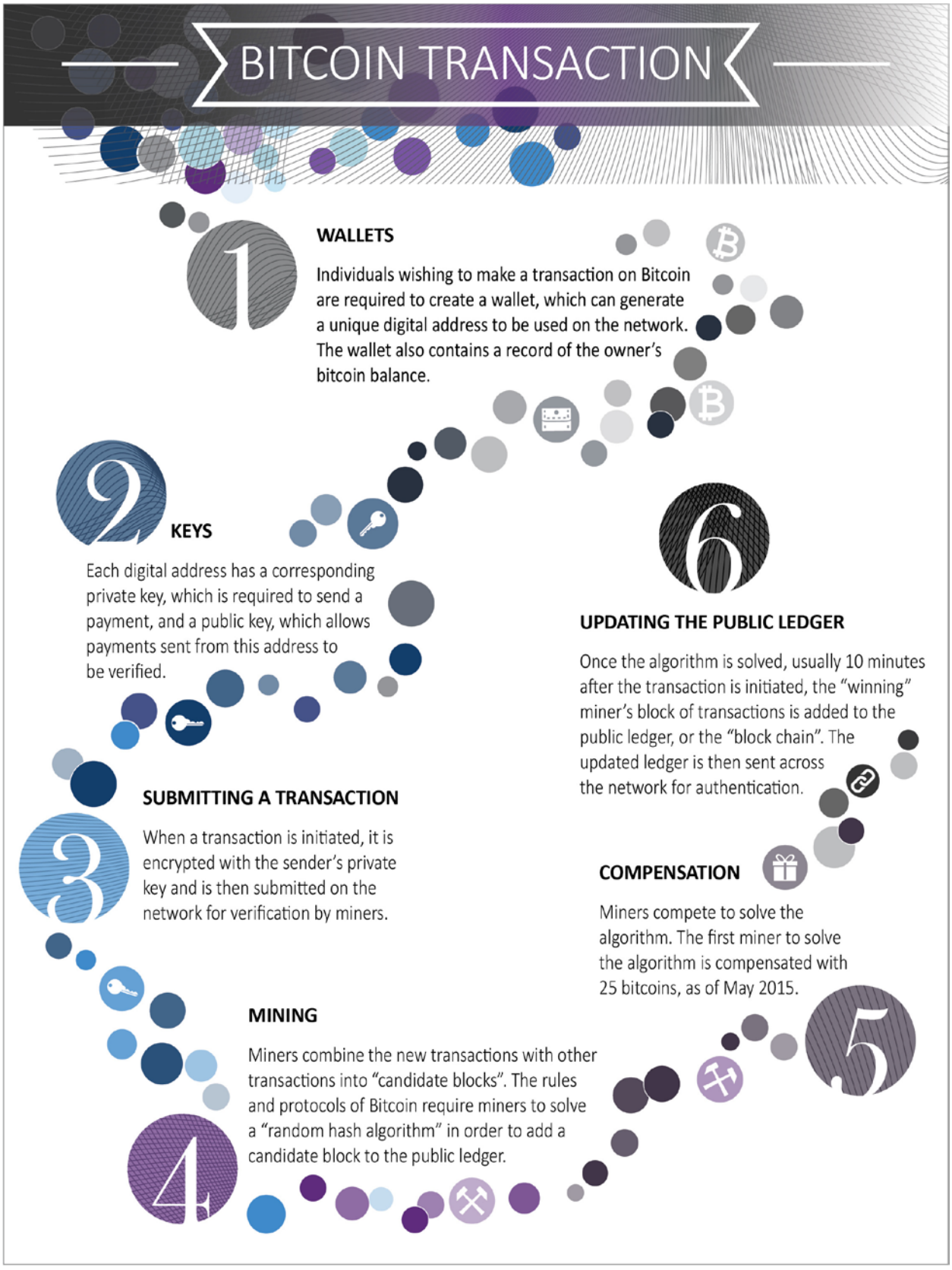
BitPay indicated that Bitcoin was created in 2009 as an open-standard, open-protocol and open-source payments system; it is designed for the Internet and is owned collectively by all of its users. The Department of Finance mentioned that the demand for digital currencies, particularly bitcoin, originated with people who had a libertarian philosophy, and who wished to transfer money without government interference and at low cost. It also commented that Bitcoin was developed by a group of people who were interested in mathematics, and was not created in order to generate a profit. Samir Saadi highlighted that Bitcoin was created after the 2008 global financial crisis, when some people lost faith in the traditional financial system.

Andreas Antonopoulos said that Bitcoin is at the same stage of development as the Internet was in the early 1990s. He suggested that, within eight years, more applications relating to Bitcoin will be available to consumers.

According to the Bank of Canada, before the creation of Bitcoin, decentralized digital currencies were not considered to be feasible, as it was not possible to verify whether "double spending" – an amount sent to one individual is also sent to another person – had occurred. The Bank stated that Bitcoin's verification of transactions through the blockchain ensures an absence of "double spending."

The Department of Finance noted that Bitcoin transactions are recorded on a public ledger that can be accessed on a website, and that "miners" undertake a "mining" process to verify the availability of funds for a transaction. According to it, the miners' computers solve mathematical problems to ensure that each bitcoin's private key, which is like a personal identification number, is authentic; once the mathematical problem is solved, the transaction is verified and recorded on the public ledger. Andreas Antonopoulos emphasized that the main purpose of mining is to secure and verify transactions, and that receiving bitcoin as compensation for mining activities is meant to provide Bitcoin users with an incentive to verify the transactions.

BitPay and Andreas Antonopoulos described Bitcoin transactions as being more similar to cash, than to credit card, transactions; for example, a payment made using bitcoin involves the purchaser sending a precise amount directly to the seller, while a payment made using a credit card involves the purchaser providing his/her credit card number to a merchant, which – through the authorization associated with its receipt of that number – receives payment after involving intermediaries. Andreas Antonopoulos also commented that a single Bitcoin transaction does not authorize any future payments or reveal the sender's identity to the entity receiving the payment.



Source: Figure prepared by the Library of Parliament.

Bitcoin Foundation Canada indicated that, as of 2 October 2014, the cost of mining and the price of acquiring one bitcoin were approximately US$310 and US$385 respectively. It noted that this gap is narrowing, and that mining costs are falling as miners consolidate and offer "cloud mining services," rather than using individual computers to mine bitcoin. Samir Saadi suggested that increased computing power and the development of new technologies could offset the increased costs of verifying Bitcoin transactions.

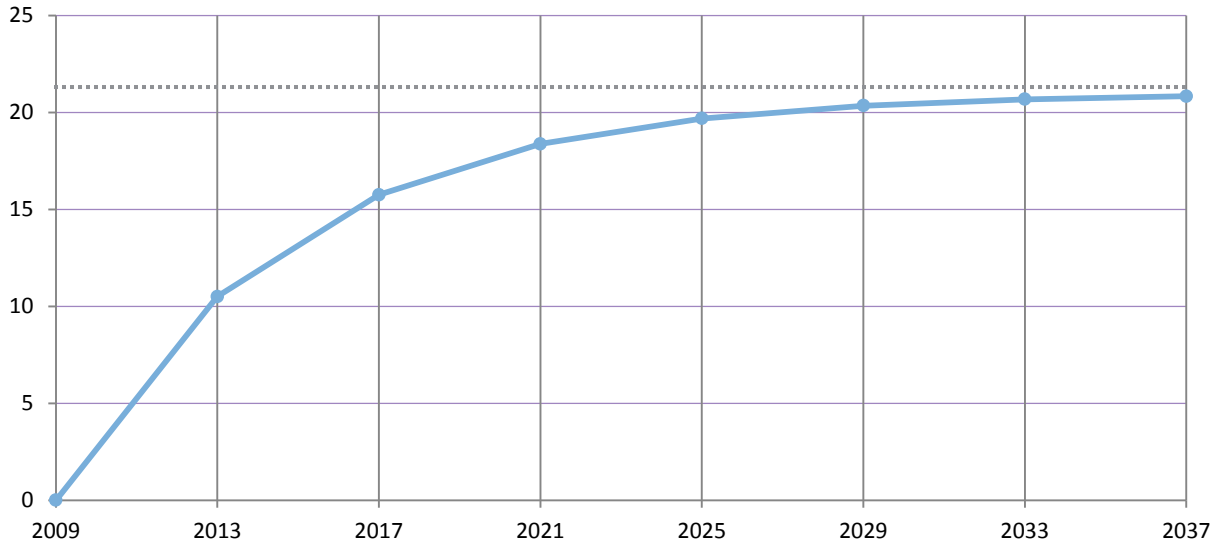
Andreas Antonopoulos commented on a group of independent miners – called GHash.IO – that, in 2014, was undertaking nearly 51% of Bitcoin's mining activities. He said that some miners voluntarily left GHash.IO and joined other mining groups due to the "reputational risk" to Bitcoin of one mining group potentially being able to disrupt the verification of transactions. In his view, if a mining group controls more than 50% of Bitcoin's mining activities, it could delay the processing of transactions; however, it would not be able to steal bitcoin or invalidate transactions.

(ii) The Currency

The Department of Finance stated that a bitcoin is not a file, but rather a number associated with a Bitcoin address, which functions like a bank account. According to Jeremy Clark, bitcoin is not a bearer instrument and cannot be held physically; rather, an individual obtains a cryptographic – or private – key that gives him/her "signing authority" for the Bitcoin address. Bitcoin Foundation Canada noted that the loss of the only copy of a private key results in a permanent loss of the associated bitcoin. Andreas Antonopoulos highlighted that private keys, which are essentially numbers, can be stored digitally or physically; physical storage involves printing the keys out on paper, which is relatively more secure and not subject to hacking.

As well, the Department of Finance said that the supply of bitcoin – which was 15 million as of 26 March 2014 – is limited to 21 million; the supply is determined not by a central authority, but rather by a mathematical formula in the mining process, with miners receiving new bitcoin when they verify transactions. It suggested that miners may charge a fee to verify transactions once this limit is reached and bitcoin is no longer received as compensation.

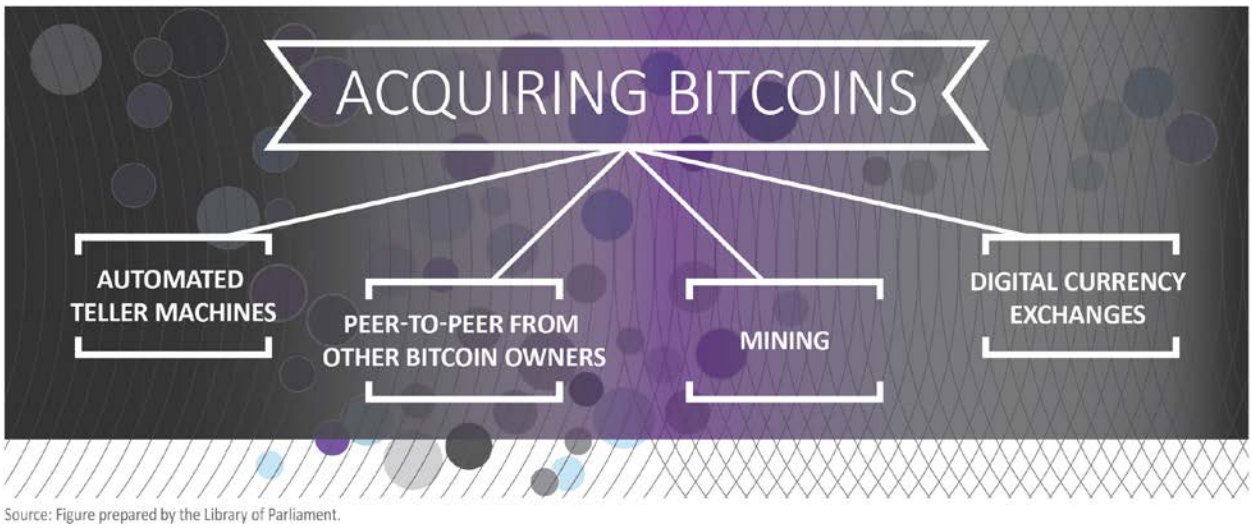
Projected Supply of Bitcoin, 2009–2037 (millions)



Source: Figure prepared using information obtained from: Coin wiki, "Controlled Supply."

Andreas Antonopoulos noted that the mathematical algorithm that regulates the supply – and determines the maximum supply – of bitcoin is based on the supply curve of a precious metal, such as gold, which is just one option when considering the supply of a digital currency. Bitcoin Foundation Canada mentioned that, although the supply of bitcoin is limited to 21 million, the ability to divide one bitcoin will allow Bitcoin to expand.

The Bitcoin Strategy Group said that, in addition to mining, bitcoin can be obtained in three ways, with the price of a bitcoin perhaps being different in each case: directly from a holder of bitcoin; through a bitcoin exchange; or from a bitcoin ATM.



Source: Figure prepared by the Library of Parliament.

Bitcoin Foundation Canada highlighted that making a payment with bitcoin is separate from having the transaction recorded on the blockchain, and noted that a bitcoin payment occurs instantaneously, while the recording of the transaction can take between 30 seconds and 60 minutes. The Department of Finance stated that the average time taken to verify a transaction – about 10 minutes – is a result of the computing power required for the verification process.

B. Digital Currency-Related Opportunities

1. Innovation

In speaking to the Committee about the innovation arising from digital currencies and their technologies, witnesses discussed the possible impacts of regulation, Canada's role as a digital currency hub, and state-supported digital currencies and associated technologies.

(i) Possible Impacts of Regulation

Witnesses commented that regulations for digital currencies could negatively affect innovation in relation to them and their technologies. The Department of Finance noted that digital currencies may not be extensively regulated in Canada in the future, as doing so could constrain these currencies' innovative aspects, while Jeremy Clark and Joshua Gans indicated that any federal regulations for these currencies should be implemented in a way that would encourage innovation. Similarly, the Royal Canadian Mounted Police said that laws and regulations for digital currencies should not negatively affect the innovative benefits that legitimate users derive from these currencies.

In focusing on a particular digital currency, Andreas Antonopoulos and the Digital Finance Institute suggested that regulations for digital currencies should not be implemented until Bitcoin's technology, and its potential applications, are better understood. The Bitcoin Alliance supported regulations that would be technologically neutral and respect Bitcoin's innovative aspects, while Ripple Labs said that any regulations should consider digital currencies' reliance on decentralized public ledger technology and its potential use in ways that would benefit payments systems.

Andreas Antonopoulos also said that imposing a centralized model of regulations for all digital currencies would not be suitable or efficient for decentralized networks, as this approach would weaken Bitcoin's security and hamper innovation; it would be more appropriate to secure decentralized digital currency networks through innovative decentralized technologies, including smart contracts, multi-signature escrow to release funds and "hardware wallets." The Bitcoin Embassy stated that Bitcoin should not be regulated, as doing so would discourage innovations designed to address potential cybersecurity risks, but noted that some digital currency-related businesses have indicated that they want to be regulated. The Digital Finance Institute mentioned the importance of dialogue among digital currency stakeholders regarding potential regulations.

John Jason noted that there are two perspectives to consider when deciding whether to regulate digital currencies: the need to protect consumers against harm, and the development of Canada's digital currency sector. He also said that legal issues may arise over the next few years, as Canada's legal framework may not currently address certain aspects of digital currencies' technologies.

According to the Canadian Payments Association, any potential regulations for digital currencies should consider past market failures – and their impacts – in the areas where these currencies could play a role in the Canadian economy, including as a form of money, an investment or a payments system.

(ii) Canada as a Global Digital Currency Hub

Witnesses said that Canada could become a global hub for digital currencies. For example, Samir Saadi noted that digital currency-related businesses seeking to expand are looking for countries where regulations are not onerous. The Bitcoin Embassy stated that Canada has the potential to become a global hub for these businesses, as it has a high rate of Internet usage, a skilled workforce that is knowledgeable about technology, competitive electricity rates, and "organized" Bitcoin meetings and groups in almost every major Canadian city. Similarly, Bitcoin Foundation Canada suggested that Canada could play a lead role in digital currency mining if it maintains a fiscal and regulatory framework that is technologically neutral in relation to digital currencies. Elliot Greenstone mentioned that Canada should not implement regulations for digital currencies that are more stringent than those in other countries, as doing so could hamper the expansion of Canada's digital currency sector.

Warren Weber, who appeared as an individual, indicated that Canada could have a larger share of global digital currency-related businesses and investment if the country were to be a "first mover" in establishing a stable legislative and regulatory environment for digital currencies. That said, he also commented that Canada could avoid expensive mistakes if it first considers the impacts of digital currency-related regulations in other countries. According to Jeremy Clark, if Canada were to be among the first countries in the world to regulate Bitcoin, entrepreneurship and innovation could result, both generally and regarding Bitcoin.

David Descôteaux, of the Montreal Economic Institute, noted that – from a global perspective and as of April 2014 – Canadian Bitcoin-related businesses had received the second-largest amount of venture capital, after the United States. He highlighted the importance of ensuring that individuals, investors and businesses understand the types of legislation that apply to Bitcoin in order to strengthen their confidence in the technology, and of creating a regulatory environment that promotes Bitcoin and encourages venture capital investments in Canada's Bitcoin-related businesses. In his opinion, regulations for digital currencies would reduce investors' perceived risk that Bitcoin will be determined to be illegal in Canada and would increase investment in Bitcoin-related businesses.

(iii) State-supported Digital Currencies and Their Technologies

Witnesses discussed specific federal support for digital currencies and their technologies. For example, Joshua Gans said that a state-issued digital currency in Canada should be considered, while Andreas Antonopoulos indicated that central banks may use Bitcoin's blockchain technology to develop a state-issued digital currency. Regarding its development of a digital currency, the Bank of Canada stated that innovation with respect to digital currencies and payments system technologies is best provided by the private sector, which should be guided by an appropriate legal framework.

Warren Weber suggested that promoting a government-sponsored, centralized digital currency – and restricting decentralized digital currencies – could stifle innovation. According to Samir Saadi,

the federal government should not develop a digital currency, as the failure of a government-sponsored digital currency could affect the entire economy; a digital version of the Canadian dollar would likely be a better option. He also commented that digital currencies should not be viewed as technologies that should either become the dominant type of currency or fail; rather, they could be used alongside state-issued currencies.

The Dominion Bitcoin Mining Company supported the government "sanctioning" or "endorsing" a regime of bitcoin wallets; these wallets would be protected by strong encryption protocols and would be subject to a small fee per transaction, similar to a Tobin tax. It stated that the revenue generated from this proposed fee could be used to establish an insurance scheme, similar to deposit insurance, and that the proposed fee could become a source of revenue for the government if bitcoin becomes widely used. According to it, the existence of "sanctioned" digital wallets could accelerate the use of bitcoin throughout Canada and serve as a model for other countries.

The Digital Finance Institute said that governments should make investments and create policies that would support the development of digital finance technologies. In particular, it and the Bitcoin Embassy said that the government should make positive public statements about digital currency technologies. Similarly, Samir Saadi highlighted that the development and expansion of Canada's digital currency sector could be supported by encouraging the innovative use of bitcoin, as well as the associated technology.

2. Transaction Costs

The Committee's witnesses commented that the use of digital currencies and their technologies affects transaction costs for both individuals and businesses.

(i) Individuals

Witnesses highlighted that digital currencies reduce the need for intermediaries in the payments system, which enables lower costs. According to the Department of Finance, Bitcoin's true technological innovation is the reduced need for intermediaries. Similarly, the Bitcoin Embassy noted that Bitcoin avoids the inefficiencies that result from using financial intermediaries to transfer or store assets; any individual is able to transfer bitcoin to others at low cost, instantaneously and without the need for documentation. Joshua Gans mentioned that digital currencies – such as bitcoin – reduce the need for governments, banks and other financial institutions to be involved in transactions. In his opinion, the lack of such intermediaries results in lower costs for certain types of transactions, especially those that are international.

The Department of Finance suggested that peer-to-peer transfers of digital currencies may be an attractive and cost-effective mechanism for individuals to send international remittances; these transfers can be less costly than those that involve banks or money services businesses, and do not require a currency exchange. Similarly, Jeremy Clark said that Bitcoin's low transaction fees could enable international remittances and micro-transactions, which usually have a value that is less than $1. According to Joshua Gans, international transactions are an area where innovation in digital currencies would provide the largest benefit. As well, the Digital Finance Institute commented that the development of new technologies in the financial sector, such as purely digital financial products and their delivery through international digital platforms, reduces the cost of financial services and their delivery.

BitPay indicated that, in its role as a payments system, Bitcoin could compete with existing financial services, such as money transfers. MoneyGram International stated that it provides money transfer services in more than 200 countries, and that the average transaction amount is $300 to $400; moreover, it can facilitate person-to-person money transfers and transfers of money directly to bank accounts in countries that receive large volumes of international remittances, such as China, Mexico, India and the Philippines. It explained that, with its money transfer services, the sender pays all of the transaction fees, the transfer to the recipient can take only minutes, and the amount of the fees depends on both the country to which the transfer is being sent and the size of the transfer, with relatively higher fees charged when lower amounts are transferred. It also said that, for a transfer of $100, the transaction fee could range from $5.00 to $10.00 and the currency exchange fee could be equivalent to a couple of percentage points of the value of the transaction; for a transfer of $1,000, the transaction fee would be at least $9.99.

Jeremy Clark noted that, as of 3 April 2014, the cost of a standard Bitcoin transaction was approximately $0.05; the fee did not depend on the value of the transaction. He and the Department of Finance indicated that – as of 3 April 2014 – the transaction fee to convert one bitcoin into a Canadian dollar ranged from 0.5% to 1.5%, depending on the bitcoin exchange. According to the Canadian Bankers Association, as of 10 April 2014, the charges that applied when buying bitcoin through a particular exchange included a fee of about $5 per $100 to deposit Canadian dollars into an account with the exchange, and a fee of 1.5% of the amount of the transaction to exchange those dollars for bitcoin; similar fees applied when selling bitcoin and withdrawing the dollars from an account at a particular exchange. The Royal Bank of Canada mentioned that the use of digital wallets involves costs; on 10 April 2014, these costs were a minimum fee of 1% to transfer bitcoin person-to-person.

(ii) Businesses

Witnesses said that digital currencies and their technologies may reduce transaction costs for businesses. For example, the Department of Finance and the Bank of Canada indicated that digital currencies' transaction fees are low in comparison to credit card acceptance fees. The Interac Association highlighted that, as of 12 June 2014, its average fee for retailers was $0.03 to $0.05 per transaction, which included the mark-up by the payment processor. PayPal stated that businesses benefit from its system because they can receive payments without any start-up fees; as of 12 June 2014, the standard processing fee was 2.9% of the value of the transaction plus $0.30. Samir Saadi mentioned that, because of low transaction costs, businesses that export may benefit from using digital currencies. Bitcoin Foundation Canada suggested that, due to China's control over the transfer of yuans outside of the country, Bitcoin has become popular in China as individuals and businesses have sought other options to trade internationally.

Cost of Selected Payment Methods for Merchants, 2014

DEBIT CARD	CREDIT CARD	PAYPAL	BITPAY
$0.03 to $0.05 per transaction	1.5% to 4.0% of the value of the transaction	2.9% of the value of the transaction plus $0.30	No fee per transaction; the cost of monthly plans varies from $0 to $300 or more

Sources: Prepared using data obtained from: Department of Finance, *The Road to Balance: Creating Jobs and Opportunities*, 11 February 2014; and BitPay, BitPay pricing, accessed 2 April 2015. Costs for the debit card and PayPal payment methods are based on testimony by the Interac Association and PayPal in their appearances before the Standing Senate Committee on Banking, Trade and Commerce on 12 June 2014.

BitPay noted that, since its creation in 2011, more than 30,000 merchants have become clients; its competitors include Coinbase and BitNet, and additional competitors are emerging on an ongoing basis. It explained that its role is similar to that of a credit card payment processor: it acts as the merchant's agent to help clear and settle payments made with bitcoin. BitPay also mentioned that merchants can receive the proceeds of their sales in the form of a state-issued currency or as a mix of bitcoin and a state-issued currency.

Andreas Antonopoulos stated that banks could benefit from the blockchain technology; for example, they could adapt it for their own purposes, and eliminate the need for intermediaries in clearing international fund transfers or in purchasing stocks and equities. Similarly, BitPay commented that financial institutions could implement Bitcoin's technological advancements, thereby enabling them to provide interbank settlements, international transfers, foreign exchange transactions and other products at lower cost.

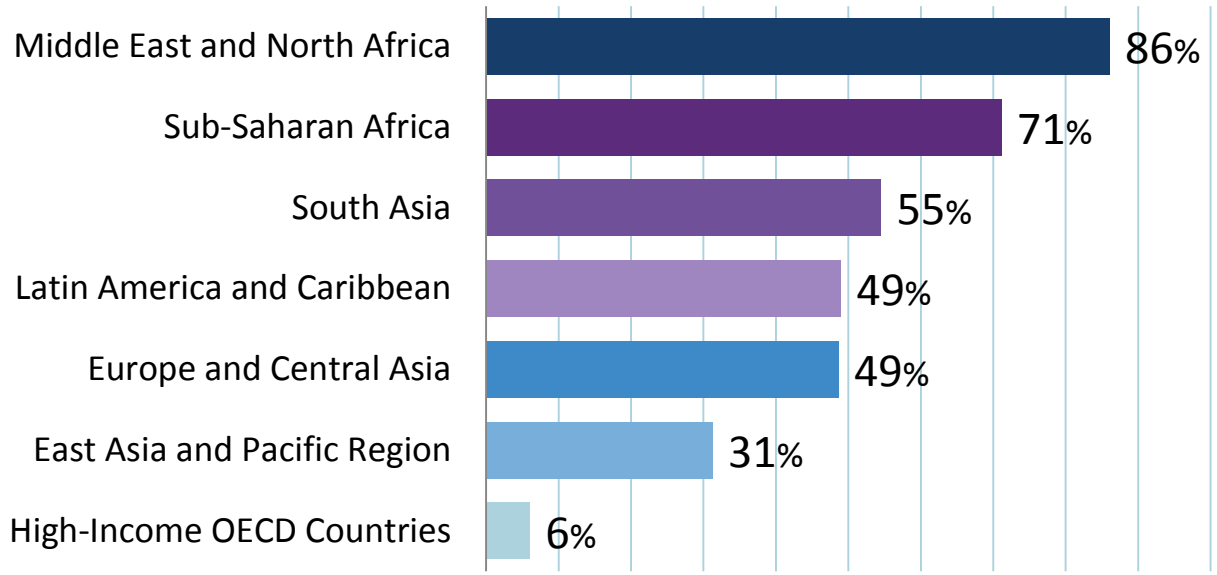
3. Payment Options

According to the Committee's witnesses, the emergence of digital currencies as another payment option in some situations provides an opportunity to increase individuals' access to financial services in developing countries. Witnesses also commented that businesses may benefit from new payment options.

(i) Individuals in Developing Countries

Witnesses highlighted that digital currencies can lead some individuals to have access, or enhanced access, to financial services. Andreas Antonopoulos indicated that individuals who lack access to financial services or international credit have the greatest need for Bitcoin; some of these individuals – many of whom live in Kenya, Lagos, Nigeria and other African countries – use their mobile phone extensively. He stated that, as of 8 October 2014, there were 2.5 billion people worldwide who were "unbanked" and lived in cash-based societies; up to 6 billion individuals could not access international markets or credit with their domestic banking system. According to him, with digital currencies and mobile phones, those who lack access to financial services can connect to the world on an equal basis to those in Western countries.

Adults without an Account at a Formal Financial Institution, Various Regions, 2014 (%)



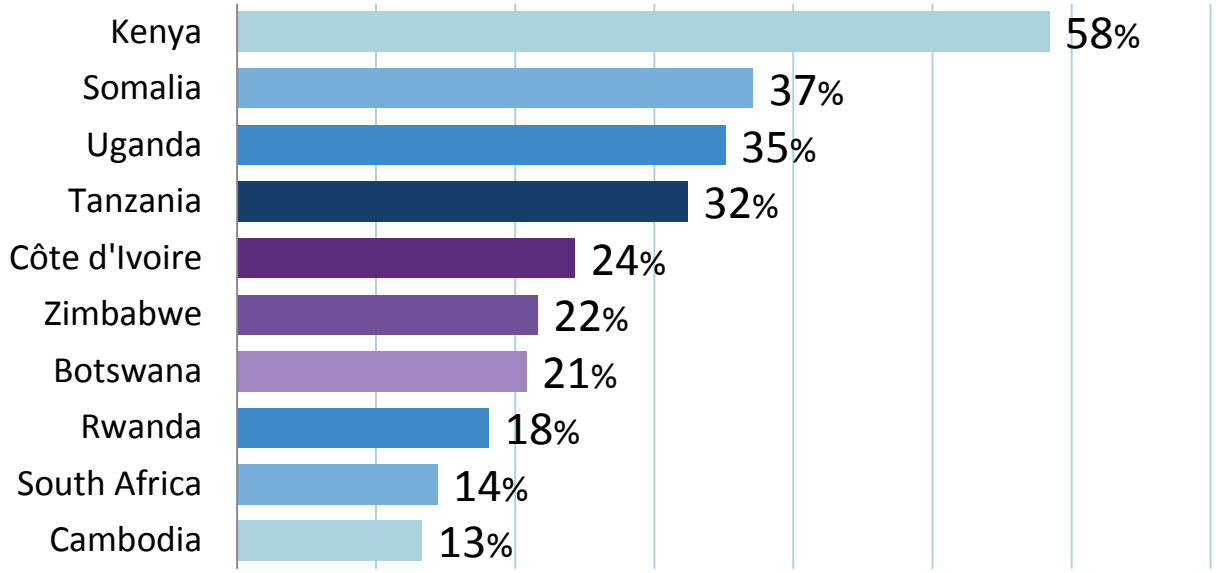
Source: Figure prepared using information obtained from: The World Bank, Global Findex Database, accessed 27 May 2015.

The Bill and Melinda Gates Foundation mentioned that the least expensive way to improve financial inclusion in developing countries is through digital products, including mobile phone-based payments systems. It said that, in many developing countries, a significant portion of the population has a mobile phone, including individuals with lower incomes; consequently, there is great potential to increase financial inclusion through mobile phone-based financial services. It highlighted that a large portion of the population in Tanzania is accessing financial services through a mobile phone.

According to the Bill and Melinda Gates Foundation, mobile phone-based payments systems, such as M-PESA, have a number of advantages in developing countries: they are significantly less expensive than the alternatives currently available to low-income people; the number of access points for these systems is far greater than the number of bank branches; and people who are part of a large mobile payments network are better protected against income shocks, such as a medical emergency, a marriage or having a baby, as it is easier for friends and relatives to send money through the network than through regular channels. It also said that mobile phone-based payments systems can increase access to credit for low-income individuals in developing countries; new banking services offered through M-PESA, such as M-Shwari in Kenya and M-Pawa in Tanzania, make short-term emergency loans based on a user's history of M-PESA transactions.

The Digital Finance Institute suggested that M-PESA's success in Kenya shows that new technologies in digital finance, including cryptocurrencies, have the potential to increase access to financial services for those who are "unbanked" or excluded from financial markets. It noted that, according to a World Bank report, these individuals are mostly women.

Adults Who Reported Using a Mobile Phone for Monetary Transactions, Various Countries, 2014 (%)



Source: Figure prepared using information obtained from: The World Bank, *Global Findex Database*, accessed 27 May 2015.

The Bill and Melinda Gates Foundation explained that some digital currencies, particularly those that offer anonymity, would not meet the needs of low-income individuals in developing countries. It said that being unknown to financial institutions and governments is generally a problem for them, and they may be charged a higher interest rate and not receive government services as a result; using digital currencies to make anonymous transactions would not address the issue of not being known to financial institutions and governments. As well, according to it, bitcoin's price volatility limits its usefulness for low-income people in developing countries, as these individuals need their limited assets to have a stable value.

MoneyGram International said that it can transfer money to mobile phones when countries have appropriate technology; these countries include Kenya. In its view, the ability to make money transfers online and through mobile phones provides individuals with enhanced access to financial services.

Andreas Antonopoulos noted that Bitcoin is not yet adapted for use on Nokia 1000, which is the most widely used cell phone platform in the world. That said, he highlighted that Bitcoin is gradually being used with simpler technologies, such as text messaging, and that the cost of manufacturing smart phones is falling; one smart phone could provide thousands of individuals with access digital wallets and other financial services. According to him, parts of Canada could benefit from Bitcoin, as some regions may have limited access to the traditional banking system.

(ii) Businesses

Witnesses identified a number of unique characteristics of digital currencies and their payments systems from which businesses could benefit. For example, BitPay and MasterCard highlighted the ability to transfer an asset – such as bitcoin – and immediately settle a transaction with no

counterparty risk. According to the Bill and Melinda Gates Foundation, the instantaneous clearing and settlement of small-value payments that is a feature of the mobile-phone based payments systems used in developing countries could benefit developed countries.

The Department of Finance, BitPay, the Bank of Canada and Jeremy Clark commented that payments are irreversible when digital currencies are the method of payment, which is beneficial for merchants; credit card transactions can be reversed when fraud occurs. BitPay also noted that this irreversibility is useful for businesses that wish to sell to customers in jurisdictions where it is difficult to collect payment for goods and services.

The Canadian Virtual Exchange stated that Bitcoin is not affected by banking hours or holidays, as it operates all day, every day.

4. Identity Protection and Recording of Transactions

The Committee's witnesses indicated that digital currencies and their technologies may protect the identity of the parties involved in transactions and provide a payments system that is recorded because of the public ledger.

(i) Identity Protection

Witnesses stated that individuals can protect their personal information when using digital currencies. In the opinion of the Bank of Canada, the anonymity associated with digital currencies may be useful to individuals who wish to conduct specific types of transactions; for example, someone may want to undertake a transaction with an individual who is unknown to him/her without divulging personal information, such as a bank account or credit card number. The Royal Canadian Mounted Police noted that legitimate users of digital currencies can benefit from increased privacy.

According to BitPay, the risk of identity theft can be reduced if bitcoin is the method of payment for online transactions, as – unlike credit card payments – a customer's identity and account number are not provided with Bitcoin transactions; thus, there is no identity information that can be stolen. It stated that, as of 12 June 2014, using bitcoin as the method of payment could have prevented 12 million people annually from becoming a victim of identity theft and $20 billion per year globally in payment fraud. It also noted that one of the major differences between credit card payments and bitcoin payments is that, with the former, merchants can retain and reuse the cardholder's account information to process multiple, perhaps illegitimate, charges; conversely, as each bitcoin transaction is unique, merchants cannot reuse the information. Similarly, the Bill and Melinda Gates Foundation noted that mobile payments systems in developing countries do not require a customer's identity and account number to be provided when a transaction is made, which reduces the risk of fraud; developed countries would benefit from such systems.

The Bitcoin Embassy said that both bitcoin and a credit card can be a method of payment for an average user; however, the former has lower fees and a reduced risk of fraud or identity theft. In comparing transactions with credit cards to those with bitcoin, Andreas Antonopoulos suggested that Bitcoin users have direct control over the privacy of their financial transactions, are not required to disclose their identities to undertake a transaction, and do not have to trust that financial intermediaries will safeguard their financial accounts. He stated that requiring identification for Bitcoin transactions would compromise users' privacy and weaken the payments system.

(ii) Recording of Transactions

Witnesses in Ottawa and groups the Committee met during its fact-finding trip to New York City commented on the record of transactions that is a part of the public ledger. The Department of Finance stated that Bitcoin is one of the most transparent payments systems because transactions are recorded on the public ledger and any emails associated with Bitcoin addresses are traceable. That said, it explained that a Bitcoin address is a series of letters and numbers; consequently, the entity associated with a particular address may be unknown, which gives rise to the notion that Bitcoin is pseudo-anonymous.

Jeremy Clark mentioned that Bitcoin addresses can be identified, as – for example – companies may publish their addresses so that they can receive payments from clients using Bitcoin, individuals may make purchases with bitcoin and have goods shipped to a physical address, or an individual's Internet Protocol address may be discovered.

The Department of Finance suggested that Bitcoin's public ledger generally makes transactions using bitcoin more transparent than those with most other methods of payment, while Jeremy Clark indicated that an individual using bitcoin is more anonymous than someone using a debit or credit card; both said that Bitcoin transactions are more transparent than transactions with cash. Andreas Antonopoulos noted that cash is more useful than digital currencies for illicit activities, as Bitcoin transactions can be traced with the public ledger. Joshua Gans stated that those who engage in illicit activities are dissuaded from using bitcoin because of the public ledger. That said, the Royal Bank of Canada commented that Bitcoin is not more transparent than other payments systems.

According to the Bitcoin Alliance, Bitcoin's public ledger could greatly assist law enforcement agencies that are investigating the flow of money in an allegedly fraudulent transaction; for example, there is little to no delay in retrieving records about a particular Bitcoin transaction, as all transactions are recorded on the public ledger. It mentioned that techniques that are similar to those used in traditional digital forensic investigations, such as linking an Internet Protocol address to a home or business, allow the "owner" of a Bitcoin address to be identified. Similarly, Ripple Labs indicated that a decentralized public ledger may enable suspicious financial flows to be traced, reported and analyzed more easily, as the information on the ledger would be more comprehensive than financial institutions' individual databases if digital currencies become more widely used.

C. Digital Currency-Related Risks

1. Potential Criminality and its Effects

Witnesses told the Committee that certain digital currencies have been linked to criminal activities, particularly money laundering and terrorist financing, and that some regulators have implemented – or are considering the implementation of – licensing requirements as a way to deter criminals from operating digital currency-related businesses and using digital currencies for criminal purposes. They also suggested that the association of digital currencies with criminal activities has negatively affected digital currency related-businesses that are trying to access banking services.

(i) Money Laundering and Terrorist Financing

Witnesses appearing before the Committee in Ottawa and law enforcement agencies the Committee met during a fact-finding trip to New York City commented on specific criminal investigations involving digital currencies that were linked to money laundering activities. The Royal Canadian Mounted Police discussed the Silk Road website, which was an online illegal market that used bitcoin as the method of payment and was shut down by the U.S. Federal Bureau of Investigation in 2013, and the Silk Road 2.0 website, which was shut down by international law enforcement agencies in November 2014. According to the Department of Finance, Canadians were making purchases on the Silk Road website and Canada was the fourth most common country of origin for illicit items listed on the website, after the United States, the United Kingdom and the Netherlands.

The Royal Canadian Mounted Police also mentioned the Liberty Reserve website, where criminal activity was conducted through the Liberty Reserve centralized digital currency exchange. It indicated that the exchange's operators were charged with laundering $6 billion through 55 million illegal transactions, and said that the Liberty Reserve investigation involved 17 countries, including Canada.

CRIMINAL ACTIVITY AND DIGITAL CURRENCIES

Liberty Reserve

Created in Costa Rica in 2006, Liberty Reserve was an international online payment processor whose website operated using anonymous accounts that accepted funds for transfer to other individuals; the funds were converted into Liberty Reserve Dollars that were tied to the value of the U.S. dollar, the euro or ounces of gold. In May 2013, U.S. law enforcement agencies and prosecutors shut down the Liberty Reserve website, arrested five people and seized bank accounts located in eight countries in relation to a money laundering scheme perpetrated by Liberty Reserve's owners. An estimated $6 billion was laundered through Liberty Reserve, which operated in 17 different countries.

Silk Road

Silk Road was an Internet-based black market for illegal goods and services that operated from January 2011 to 2 October 2013. It was used to distribute illegal drugs, as well as other illicit goods and services, to more than 100,000 buyers, with vendors accepting payments in bitcoin. According to estimates, Silk Road generated sales revenue of more than 9.5 million bitcoins and the website's operators collected more than 600,000 bitcoins in commissions from these sales. The U.S. Federal Bureau of Investigation made its first arrests in relation to Silk Road in October 2013. In February 2015, the creator of Silk Road was found guilty on seven charges, including money laundering, narcotics trafficking and computer hacking.

David Descôteaux noted that the amount of state-issued currencies that is laundered annually is several magnitudes larger than the amount of bitcoin in circulation, making this digital currency relatively insignificant in terms of money laundering. That said, the Department of Finance, the

Financial Transactions and Reports Analysis Centre of Canada, l'Autorité des marchés financiers and the Ontario Securities Commission stated that the anonymity provided by digital currencies and the ease they can be used to make transfers make them vulnerable to being used for money laundering and terrorist financing activities. According to MasterCard, regulations that would remove anonymity from Bitcoin transactions, and that would regulate digital currency exchanges in a similar manner to commodity exchanges or banks, would reduce the risk of Bitcoin being used for illicit activities.

The Royal Bank of Canada said that difficulties arise when attempting to trace the source of funds when payments are made using bitcoin; bitcoin exchanges cannot be properly monitored to ensure the absence of money laundering and terrorist financing. Elliot Greenstone highlighted that an individual carrying bitcoin across a border in a digital wallet on a cell phone would not have to report the amount of the bitcoin to border officials, even if it exceeds the $10,000 reporting threshold for the movement of monetary instruments across borders.

According to the Royal Canadian Mounted Police, a major challenge for law enforcement agencies is the time required to identify criminals who are using digital currencies. It stated that digital currency-related businesses could assist law enforcement agencies by being able to identify a client quickly, and in a manner that is similar to banks.

In mentioning the reported use of digital currencies to finance terrorism, the Canadian Security Intelligence Service indicated that it has not seen any evidence to substantiate media reports suggesting that terrorist groups are using bitcoin. It noted that it actively investigates the travel-related financial activities of foreign fighter terrorists; currently, it can identify situations in which state-issued currencies have financed travel, which might indicate that bitcoin is not being used for this purpose. The Digital Finance Institute stated that the U.S. Department of the Treasury has said that bitcoin is not being used to finance terrorism to any significant extent.

The Canadian Security Intelligence Service said that it is not overly concerned about digital currencies or online payments systems being threats to national security, perhaps because of high volatility in the price of digital currencies and relative difficulty in using such currencies to make payments, particularly when travelling. It stated digital currencies have not been found to fund or facilitate threats to Canada or other countries in any substantial way, but they could be used by terrorists in the future.

In commenting on the terrorist financing risks relating to digital currencies, the Digital Finance Institute explained that an individual can set up a bitcoin wallet that is completely anonymous, and can use that wallet to transfer significant sums to the anonymous wallet of a terrorist organization; it is unclear whether such a transaction would be detected under Canada's anti–money laundering and anti–terrorist financing regime's proposed regulations.

In the first budget bill introduced following the 2014 federal budget, the* Proceeds of Crime (Money Laundering) and Terrorist Financing Act *was amended to classify digital currency exchanges as money services businesses for purposes of Canada's anti–money laundering and anti–terrorist financing regime.

In relation to recent amendments to the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, the Department of Finance said that it is currently developing regulations that will define the types of digital currency businesses that will be classified as money services businesses for purposes of Canada's anti–money laundering and anti–terrorist financing regime, and the obligations that will be imposed on these businesses. According to the Department, its regulatory approach will target the most vulnerable areas, including digital currency exchanges that facilitate the conversion of digital currencies to state-issued currencies, and will impose similar obligations on digital currency exchanges and money services businesses. It said that this approach, whereby regulations are not imposed on the technology and infrastructure underlying digital currencies or on digital currency users, should not stifle innovation.

According to MoneyGram International, for purposes of money laundering and safety and soundness requirements, digital currency exchanges and money services businesses should be regulated in a similar manner; consequently, exchanges should be required to have a program to ensure compliance with the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*. It explained that the Act requires money services businesses to collect information on the identity of clients when transactions have a value of $1,000 or more; additional information must be collected if there is a business relationship with a customer. It also noted that reports are sent to the Financial Transactions and Reports Analysis Centre of Canada in two situations: suspicious transactions and international electronic funds transfers of $10,000 or more. John Jason said that regulating digital currency exchanges will target situations where a criminal is likely to convert funds resulting from criminal activities to a digital currency.

The Royal Canadian Mounted Police suggested that the Department of Finance's regulatory approach is consistent with actions being taken by the United States, the United Kingdom, Australia and New Zealand regarding digital currency exchanges. MasterCard and the Department of Finance commented that, in March 2013, the United States classified entities that facilitate Bitcoin transactions as money services businesses; they are subject to reporting requirements and know-your-customer rules under that country's anti–money laundering and anti–terrorist financing regime.

John Jason highlighted that the recently enacted provisions in the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* regarding digital currencies will attempt to regulate entities that operate outside of Canada. He explained that Canadian banking law does not regulate foreign banks unless they operate in Canada.

The Digital Finance Institute noted that no national risk assessment in relation to digital currencies occurred prior to the development of the 2014 amendments to the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*; in its opinion, such an assessment should take place

before these amendments and the related regulations are implemented. It supported consultations with relevant stakeholders to determine the extent to which digital currencies represent a risk of being used in illicit activities, and commented that the government should consider regulations only if the risk of illicit activities rises.

Despite the difficulties with attempting to trace Bitcoin transactions, the Bitcoin Alliance indicated that Bitcoin-related businesses will be able to comply with the requirements of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* once they are in force; for example, they will be able to identify the source of funds in a Bitcoin transaction. The Canadian Virtual Exchange, which has ceased operations, said that it complied with the Act's regulations for money services businesses. BitPay highlighted that it screens potential clients and their businesses to ensure that they are not engaging in money laundering or terrorist financing activities.

The Canadian Virtual Exchange suggested that Bitcoin and foreign currency transactions should be regulated in the same manner, and that bitcoin should be considered a foreign currency under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*. In its view, while such regulation could be inconsistent with the original intent of Bitcoin and could increase the administrative costs for digital currency-related businesses, it would maximize Bitcoin's potential. The Canada Revenue Agency noted that the *Income Tax Act*'s provisions relating to foreign exchange gains and losses would probably apply to digital currencies if they were to be considered a foreign currency.

According to the Royal Canadian Mounted Police, regulations for digital currencies should be designed with a view to deterring crimes that involve these currencies and reducing the use of these currencies by organized crime groups, particularly to transfer funds internationally and to launder money. In its opinion, regulations that allow the tracking and detection of international digital currency transactions, and that require certain digital currency-related businesses to be registered with a government entity, would assist law enforcement agencies in combating money laundering and terrorist financing activities. It noted that it is developing tools to assist in tracking digital currency transactions.

The Canadian Security Intelligence Service suggested that, in the future, law enforcement agencies will likely require the authority to obtain information on individuals who are participating in digital currency transactions. It also supported the introduction of regulations that would ensure that documentation on these individuals' identity is retained.

The Department of Finance said that money laundering and terrorist financing risks with digital currencies are a global issue, and international coordination – including through the Financial Action Task Force – is required to mitigate "jurisdiction shopping." The Financial Transactions and Reports Analysis Centre of Canada stated that it is working with financial intelligence units in other countries to develop a better understanding of digital currencies, as well as guidelines to respond better to money laundering and terrorist financing risks.

(ii) Other Types of Crimes

Witnesses highlighted that, in addition to laundering money and financing terrorist activities, criminals use digital currencies to commit other types of crimes. According to the Royal Canadian Mounted Police, digital currencies are a real and evolving threat to Canada's economic integrity, as

criminals exploit any new technology that provides anonymity and unregulated movement of funds. It explained that digital currencies are a challenge for law enforcement agencies for a variety of reasons: they are not subject to the same laws or regulatory regimes as legal tender; they can be used globally; and digital currency-related businesses can operate in the jurisdictions having the least onerous regulations. It also noted that conducting transactions using digital currencies is not an offence, but financing illegal activities with digital currencies is a crime.

The Digital Finance Institute suggested that the use of bitcoin could facilitate corruption. It provided the example of China, where bitcoin is a preferred method of payment when accepting a bribe, as the digital currency can be moved out of the country easily and anonymously.

The Royal Canadian Mounted Police indicated that, since 2013, the Canadian Anti–Fraud Centre has received more than 3,000 complaints about "ransomware scams." According to it, a criminal hacks into an individual's computer, uploads malware, and then asks for a ransom – typically in bitcoin – in exchange for removing the malware from the computer. It also commented that online websites that sell illegal goods are always emerging, and that international cooperation among law enforcement agencies is required to combat these websites.

(iii) Licensing of Digital Currency Exchanges and Automated Teller Machines

Witnesses mentioned that regulators in Canada and elsewhere – such as Quebec's l'Autorité des marchés, which appeared in Ottawa, and New York State's Department of Financial Services, which the Committee met during a fact-finding trip to New York City – have started to implement licensing requirements for certain businesses in order to provide a mechanism for properly assessing the risks associated with digital currencies and related businesses. Quebec's l'Autorité des marchés financiers said that digital currency exchanges offering person-to-person fund transfers are subject to the province's *Money-Services Businesses Act*. Moreover, New York State's proposed regulations would require digital currency exchanges, digital wallet providers and entities that administer digital currencies to obtain a licence from the New York State Department of Finance Services if they wish to operate in New York State.

Pursuant to Quebec's* Money-Services Businesses Act*, certain digital currency exchanges and operators of automated teller machines must apply for – and obtain – a fund transfer licence issued by l'Autorité des marchés, and comply with a number of obligations. Some of the obligations pertain to keeping records and verifying the identity of their customers.

L'Autorité des marchés financiers also explained that Quebec's *Money-Services Businesses Act* applies to businesses operating digital currency ATMs, and that these businesses are required to obtain a licence from it. It pointed out that, to obtain a licence, a digital currency ATM operator must provide specific information about its business; this information is submitted to the Sureté du Québec and local police forces, which undertake certain investigations and make a recommendation about the granting of a licence. In its view, this process is designed to ensure the integrity of businesses operating digital currency ATMs and to prevent money laundering. John Jason noted that similar

types of investigations are done in relation to banks, and suggested that Quebec's model should be considered by other jurisdictions. Andreas Antonopolous commented that the use of bitcoin on a small scale and for personal use should not be subject to regulation; for example, individuals who hold or transfer bitcoin in these circumstances should not require a licence.

In highlighting that bitcoin ATMs are located in a number of Canadian cities, the Department of Finance stated that the world's first bitcoin ATM was launched in Vancouver, British Columbia in November 2013 and processed about $1 million in transactions in its first month of operation. It also said that some bitcoin ATM owners partner with a bitcoin exchange. Bit Access stated that – as of 9 April 2014 – its ATMs were operating in Slovenia, the United Arab Emirates, Hong Kong, the United States, Mexico, Belgium, Australia, Germany, Switzerland and Canada. It commented that, as of 9 April 2014, it had 15 operational ATMs worldwide; they accounted for approximately 70% of all bitcoin ATM transactions. L'Autorité des marchés financiers mentioned that, as of 12 March 2015, there were about 20 ATMs operating in Quebec.

Elliot Greenstone suggested that Quebec's regulations for bitcoin ATMs should achieve two goals: minimize the extent to which the public associates these ATMs with money laundering and terrorist financing activities; and encourage people to obtain bitcoin from legitimate sources, rather than anonymously from strangers in exchange for cash. The Canadian Virtual Exchange supported regulations for bitcoin exchanges and ATMs, but suggested that these entities should be regulated to a lesser extent than Canadian financial institutions.

(iv) Access to Banking Services for Digital Currency-related Businesses

Some witnesses highlighted that the lack of regulations for digital currencies, particularly in relation to domestic and international anti–money laundering and anti–terrorist financing, has led some businesses to have difficulties in accessing banking services; in certain cases, existing banking relationships have been ended. For example, the Canadian Virtual Exchange stated that two of its chief executive officer's personal accounts with Canadian financial institutions were closed as a result of transfers of bitcoin.

The Department of Finance noted that some banks perceive that providing financial services to digital currency-related businesses could create a risk of non-compliance with Canada's anti–money laundering and anti–terrorist financing obligations, particularly concerning the identification of clients. The Canadian Payments Association explained that the know-your-customer regulations under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* have prompted banks to develop mechanisms to identify their clients. It stated that transactions that use a digital currency would likely require a bank to use different mechanisms for this purpose; a digital currency exchange would be required to identify the counterparty in a transaction, which may be more difficult than identifying a client.

The Bitcoin Embassy commented that individuals and businesses are currently unable to make all necessary payments using Bitcoin; consequently, banks accounts and credit cards are still required. According to Bitcoin Foundation Canada, the inability to open a bank account is a barrier for some Bitcoin-related businesses, as they are unable to pay their employees in Canadian dollars without a bank account.

In mentioning that banking regulators could be concerned about banks being associated with digital currencies, John Jason said that the Office of the Superintendent of Financial Institutions has told Canadian banks not to be a vehicle for money laundering; thus, some banks are hesitant about opening accounts for digital currency-related businesses. He also noted that banks were once reluctant to open accounts for money services businesses; this situation changed when these businesses began to be regulated and to put anti–money laundering compliance programs in place.

According to David Descôteaux, Canada's financial institutions are awaiting regulations that are specific to digital currencies, and are not offering banking services to Bitcoin-related businesses due to a fear of inadvertently violating anti–money laundering and anti–terrorist financing requirements. In his view, clearer legislation could make it easier for banks and Bitcoin-related businesses to work together, and could prevent the movement of Canadian Bitcoin-related businesses to foreign jurisdictions. As an alternative to regulations, Bitcoin Foundation Canada and Andreas Antonopoulos supported clarification of Bitcoin's legal status to assist Bitcoin-related businesses in opening accounts at Canadian banks.

The Department of Finance said that a more risk-based approach to anti–money laundering and anti–terrorist financing legislation could address banks' concerns regarding digital currency-related businesses. It stated that banks make the decision about whether to provide banking services to particular customers, including digital currency-related businesses; with a risk-based approach, banks could provide services if these businesses are determined to present a low risk of money laundering and terrorist financing activities.

TD Bank Financial Group noted that it has no policy against – or formal procedure in relation to – Bitcoin, and indicated that fair banking practices would likely require it to open accounts for applicants unless there is a reason not to do so. It also suggested that unregulated financial entities should be subject to anti–money laundering and anti–terrorist financing obligations that are similar to those imposed on financial institutions, such as verifying client identification and holding clients' funds in segregated accounts. The Royal Bank of Canada highlighted that it does not have concerns about money laundering and terrorist financing by businesses that accept bitcoin as a method of payment.

The Digital Finance Institute said that there is a risk that over-regulation could lead Bitcoin-related businesses to leave the regulated banking system, either voluntarily or because financial institutions do not provide services to them because of concerns about contravening anti–money laundering and anti–terrorist financing laws; these businesses could turn to the "underground banking system," where transactions are not monitored or reported. It supported an approach to regulating Bitcoin that would ensure that banking services are provided to Bitcoin-related businesses, and that transactions by these businesses are monitored and reported pursuant to Canada's anti–money laundering and anti–terrorist financing regime.

2. Losses

According to the Committee's witnesses, digital currencies – and their value – can be lost in a variety of ways. In particular, they commented on cyber-theft and bankruptcy of a digital currency exchange, and volatility in the price of digital currencies.

(i) Cyber-theft and Digital Currency Exchange Bankruptcies

Witnesses mentioned that cybersecurity is a major concern for all entities that offer financial services. For example, TD Bank Financial Group identified cybersecurity as a significant risk for banks, noting that it is attacked by hackers thousands of time daily, employs about 250 people in its cybersecurity program, and spends between $175 million and $200 million annually to address cybersecurity and privacy risks. It also indicated that banks can usually block attempts to hack their databases, but are frequent targets for malware attacks by hackers who try to encrypt the banks' databases and demand a ransom for decryption.

TD Bank Financial Group also highlighted that hackers who have stolen credit card information in recent years did not target banks, but rather merchants or other businesses engaged in bank-like activities; as banks are often involved in resolving problems arising from the theft of credit card information, they are working with merchants to improve cybersecurity programs. It stated that the computers of consumers and small businesses typically do not have adequate protections, and are frequently targeted multiple times by cybersecurity threats after the initial security breach.

Moreover, TD Bank Financial Group commented that, because of quantum computing and human error, digital currency technologies will eventually be hacked. Jeremy Clark explained that it takes a number of years for cryptographic algorithms, such as those used with Bitcoin, to be hacked. According to him, while Bitcoin's cryptography has not yet been hacked, its algorithms will need to be changed within five decades to avoid this situation.

Andreas Antonopoulos said that decentralized digital currencies are less likely than centralized digital currencies and payments systems to be hacked, as hackers would have to target each digital wallet. He stated that decentralized digital currencies are more secure than traditional payments systems, as authority is not concentrated in a single entity. He also noted that, as a single "bad actor" would not be able to compromise Bitcoin, the payments system can be accessed by anyone and with any software application; Bitcoin's prior authorization is not required. In his opinion, while individual digital wallets may be hacked if not secured properly, Bitcoin's technology cannot be hacked. Moreover, he said that modern computer systems and mobile phones are not designed to store digital currency safely; however, new devices are being developed that will be able to store private keys and digital wallets.

Similarly, the Bitcoin Embassy indicated that Bitcoin remains operational because the risks are assumed by individual Bitcoin participants; the failure of one participant, such as a digital currency exchange, does not affect the viability of Bitcoin as a whole. It also mentioned that such failures have resulted in new security innovations that address risks, thereby making regulation unnecessary.

The Department of Finance and the Canadian Bankers Association said that those who hold digital currencies do not have adequate protection if cyber-theft occurs, and nor do they have sufficient recourse when a digital currency exchange goes bankrupt. According to MasterCard, users of digital currencies lack safeguards – including government insurance – if digital currencies are stolen or lost, such as through the insolvency of a digital currency-related business. TD Bank Financial Group indicated, when bitcoin is stolen, the victim has no way to prove that the stolen currency belonged to him/her, a situation that is unlike the theft of information – such as credit card numbers – from a

centralized database; in the latter case, the information that has been stolen is known and it is clear to whom protection should be provided.

CYBERSECURITY RISKS AND DIGITAL CURRENCY EXCHANGES

Mt. Gox

In July 2010, the Tokyo-based Mt. Gox bitcoin exchange was launched; by 2013, it was handling up to 70% of all Bitcoin transactions. On 7 February 2014, Mt. Gox suspended bitcoin withdrawals by customers due to security concerns and, on 28 February 2014, it filed for bankruptcy in Japan, stating that it had lost up to 750,000 of its customers' bitcoins and 100,000 of its own bitcoins; 200,000 of the lost bitcoins were later found by Mt. Gox in a digital wallet. Some have attributed the loss to hackers, while others suspect theft by someone working for Mt. Gox.

CAVirtex

CAVirtEx was a Calgary-based digital currency exchange that provided digital wallets for individuals trading in bitcoin and litecoin. On 17 February 2015, CAVirtex announced that it would cease operations because an older version of its database had been compromised. It indicated that no digital currencies had been stolen and that it would be able to fulfil customers' withdrawals of their digital currencies. It also noted that its closure was influenced by difficulties in obtaining banking services.

Flexcoin

Flexcoin, an Alberta-based company that referred to itself as a "bitcoin bank," announced in March 2014 that it was ceasing operations after 896 bitcoins were stolen from customers' online accounts by hackers. Flexcoin indicated that customers who held bitcoins in Flexcoin's offline accounts would be able to access their bitcoins.

TD Bank Financial Group highlighted ways to enhance the security of payments, including those that occur with digital currencies. It explained that multi-factor authentication requires three pieces of information from an individual: something the individual knows, such as a password; something the individual has, such as a cell phone; and something that is part of the individual, such as a thumbprint. It suggested that, in 10 years, banking activities will be conducted primarily through cell phones' microchips, rather than through payment cards. It also mentioned that digital financial products are not entirely safe, and that some amount of fraudulent activity will always exist; that said, banks and the federal government are working together to develop best practices to address cybersecurity threats. Bitcoin Foundation Canada said that certain types of digital wallets require multiple signatures before funds are transmitted, which enhances security, and that some companies offer digital wallets that have deposit insurance.

The Bitcoin Strategy Group indicated that "hot" digital wallets are susceptible to theft because they are connected to the Internet. It noted that most bitcoin is held in "cold" or offline storage, such as on a Universal Serial Bus (USB) stick or a hard drive, with "deep cold" storage involving additional security, such as a hard drive in a safety deposit box.

John Jason commented on the potential need for mandatory safeguards against cyber-attacks, including in relation to digital wallets; the safeguards could include insurance or third-party testing of an entity's cybersecurity programs. Jeremy Clark supported federal legislation for bitcoin exchanges and the data centres that host their websites, and mentioned that the parties who would be held liable in cases of cyber-theft of digital currencies should be identified in legislation.

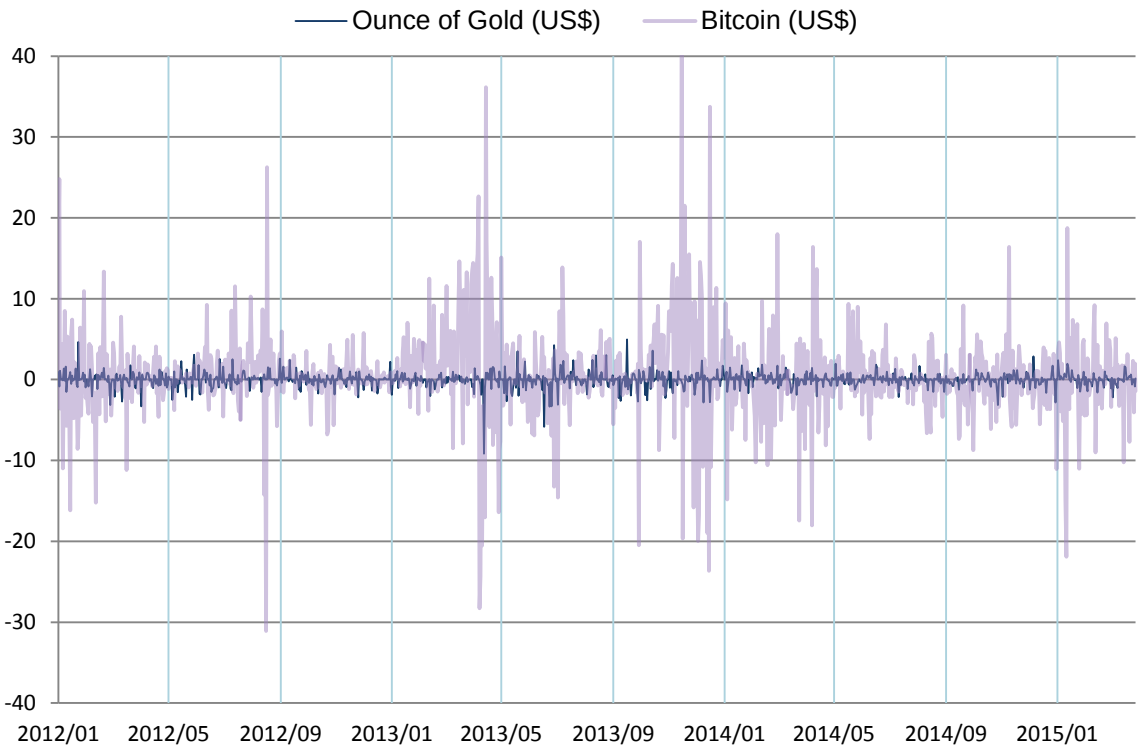
According to Andreas Antonopolous, if a holder of bitcoin gives control of that bitcoin to a "custodian," such as a digital currency exchange, the bitcoin is considered to be outside of the Bitcoin network; as digital currency exchanges are not subject to prudential regulation, there is a risk that bitcoin could be lost due to the bankruptcy of an exchange. In his opinion, when bitcoin is held outside of Bitcoin and authority to access the digital currency has been given to a "custodian," the "custodian" should be subject to regulation, as it would be acting like a bank; however, if the bitcoin holder controls his/her bitcoin, the funds are safeguarded by Bitcoin and regulation is not necessary.

Warren Weber suggested that government-backed insurance may be needed to ensure the stability of Canada's financial system if a particular centralized digital currency begins to be used extensively. In his view, the government may be required to provide financial assistance to Canadians if an entity that issues a widely used digital currency "fails." That said, John Jason noted that the number of people using bitcoin is so low that safeguards, such as deposit insurance, are not warranted.

(ii) Price Volatility

Witnesses discussed a variety of factors that could contribute to volatility in the price of digital currencies, and highlighted the limited supply of bitcoin. For example, the Bank of Canada stated that bitcoin's limited supply contributes to volatility in its price, with price adjustments occurring when supply and demand are not balanced. Andreas Antonopoulos mentioned that – as evidenced by bitcoin – the price of a digital currency is highly volatile when the currency is introduced but, as the number of units in circulation and liquidity rise, volatility declines; he suggested that, as the value of bitcoin in circulation as of 8 October 2014 totalled only $5 billion, the price of bitcoin will remain volatile for many years. Samir Saadi highlighted that bitcoin's price was quite volatile in 2013 and 2014, but is becoming more stable; the volatility is now similar to that of the price of gold. In his opinion, bitcoin was only created in 2009 and people should not be surprised that its price is volatile. John Jason said that, as bitcoin is limited in supply, its price should become more stable as the demand for it rises.

Daily Volatility in the Price of Bitcoin and Gold, 1 April 2012-4 March 2015 (%)



Sources: Figure prepared using information obtained from: World Gold Council, "Gold Price," and CoinDesk, "CoinDesk Bitcoin Price Index," accessed 8 April 2015.

Samir Saadi mentioned that the volatility in bitcoin's price may be the result of such factors as negative media coverage about the illicit activities associated with Bitcoin, the novelty of the technology, trades involving large amounts of bitcoin and "noise trading," which is based on trends and media reports and not on actual data.

TD Bank Financial Group suggested that the prices of decentralized digital currencies fluctuate because these currencies are not usually tied to a state-issued currency.

Bitcoin Foundation Canada commented that China has a major influence on exchange rates between bitcoin and state-issued currencies. It noted that about 70% of the trading volume in bitcoin occurs on Chinese digital currency exchanges, and that volatility in the price of bitcoin and in bitcoin exchange rates is decreasing rapidly.

The Department of Finance and the Canadian Bankers Association suggested that those who hold digital currencies do not have adequate protection against large fluctuations in the price of their digital currency and potential losses in value. MasterCard mentioned that the high volatility in the price of bitcoin may result in consumers and merchants not receiving "fair value" for their bitcoin transactions, as the price of bitcoin may fall before the digital currency is converted to a state-issued currency. That said, Elliot Greenstone indicated that the prices of many state-issued currencies are also highly volatile, which does not appear to impede speculative investment in them. Samir Saadi noted that regulations for digital currencies could lead to greater consumer, investor and business

confidence in these currencies, resulting in increased use of bitcoin and – perhaps – more stability in the digital currency's price.

Regarding other potential effects of the limited supply of bitcoin, BitPay said that – when compared to state-issued currencies – the use of bitcoin may be restricted; as of 12 June 2014, there was 8,000 times more units of state-issued currencies in circulation worldwide than units of bitcoin. According to the Dominion Bitcoin Mining Company, the limited supply of bitcoin is not problematic, as each bitcoin can be divided.

Joshua Gans stated that the limited supply of bitcoin is likely to result in deflation and – potentially – a recession or depression, while the Dominion Bitcoin Mining Company suggested that the deflationary nature of bitcoin could be beneficial.

3. Taxation

Witnesses spoke to the Committee about Canadian taxation of digital currencies when they are received as business or employment income and/or are purchased and sold as an investment, and highlighted some potential taxation challenges.

(i) Taxation as Business or Employment Income

Witnesses discussed the taxation rules that apply when businesses or employees receive digital currencies as income in Canada. According to the Department of Finance, like the U.S. Internal Revenue Service, the Canada Revenue Agency considers digital currencies to be property or a commodity for purposes of taxation; consequently, the taxation rules for barter transactions apply. The Canada Revenue Agency explained that when digital currencies are accepted as a method of payment in exchange for goods or services, they are taxable if earned through a "business." It also indicated that when a business is registered for purposes of the Goods and Services Tax, that tax should be applied on a transaction if a digital currency is the method of payment. The Canada Revenue Agency also said that, because it is treating digital currencies as commodities, no new rules should be required in the *Income Tax Act* to address the use of such currencies when they are earned as income or used as an investment.

For income tax purposes, the Canada Revenue Agency treats digital currencies as a commodity or property, and therefore the taxation rules that are applied to barter transactions are thereby relevant: if digital currencies are accepted as a method of payment, they are taxable if earned through a "business."

According to the Canada Revenue Agency, an employer is required to provide reasonable evidence demonstrating the manner in which bitcoin is valued for purposes of employment income, the Canada Pension Plan and the Employment Insurance program. It also highlighted that fluctuations in the prices of digital currencies make valuations more challenging, but digital currency prices are publicly available. As well, it stated that any profit an employee makes on the sale of bitcoin received from his/her employer is considered to be a capital gain.

The Canada Revenue Agency commented that bitcoin "mining" is currently treated as "the production of inventory" and tax is not paid until the bitcoin is sold; that said, it is examining this policy.

(ii) Taxation as an Investment

The taxation rules that apply when digital currencies are purchased and sold as an investment were mentioned. According to the Canada Revenue Agency, the purchase and sale of digital currencies are treated in the same manner as the purchase and sale of such commodities as copper: 50% of the capital gains resulting from the sale is included as income and, in the case of capital losses, 50% of the losses is deductible against any capital gains. As well, it explained that the capital gains taxation rules apply when bitcoin is considered to be personal property. It also noted that, for taxpayers who are in the business of trading digital currencies, the full value of the transaction is included as income and any losses are deductible against any income earned.

(iii) Potential Taxation Challenges

Witnesses discussed the use of digital currencies to avoid paying taxes, and the potential challenges that arise when digital currencies are treated as a commodity. Joshua Gans said that there is a risk that individuals will use bitcoin to avoid taxation, as some believe that the digital currency cannot be traced to them. Similarly, MasterCard commented that increased use of digital currencies could be a significant challenge for tax authorities. It said that, even if the record of a digital currency transaction is obtained, it could be difficult to identify the parties involved in the transaction and to collect taxes that are owed. As well, the Digital Finance Institute suggested that bitcoin wallets, which are anonymous, could potentially be used for offshore tax evasion. Regarding taxpayers who do not report digital currency income, the Canada Revenue Agency explained that digital currencies can be traced, and that cash transactions are much more difficult to "track."

Bitcoin Foundation Canada mentioned that double taxation of bitcoin could occur if the digital currency is treated as a commodity and thus subject to capital gains taxes, and is then treated as a currency for purposes of the Goods and Services Tax. Andreas Antonopoulos said that taxation of bitcoin should be based on the digital currency's use; it would be subject to capital gains tax if held as an investment and to sales tax when used as a currency. In his opinion, it would be beneficial to clarify tax issues in relation to digital currencies and the rights of those who use digital currencies in commercial arrangements.

The Dominion Bitcoin Mining Company spoke about the appropriateness of making bitcoin subject to capital gains taxation. In its view, it would be relatively easy for an individual to transfer bitcoin to himself/herself anonymously when bitcoin's price falls below the price at which the digital currency was purchased, and then to claim a deduction for the capital loss. It said that, rather than adapting the current taxation system to address digital currency issues, taxation policies that effectively and specifically address bitcoin should be implemented.

4. Access to Information and Protection for Users

Witnesses commented on the amount of information available to, and the nature and extent of protection for, those who use digital currencies.

(i) Access to Information

Witnesses suggested that, perhaps due to a lack of information, users of digital currencies are not well informed about the challenges with these currencies or their associated technologies and businesses. For example, according to the Bank of Canada, consumers may not have sufficient information about a new digital currency or digital currency-related business, especially about the terms and conditions of any contracts, service fees or dispute-settlement procedures that can be used when a contract is violated. It also suggested that users of digital currencies may not be fully aware of potential privacy issues; some business models involve sharing information about digital currency users to earn advertising revenue.

The Bank of Canada identified a need for consumer education, as the media give the impression that bitcoin is a coin. In its opinion, people should know that bitcoin is not a Canadian currency, and that the Canada Deposit Insurance Corporation does not protect bitcoin holdings. Similarly, David Descôteaux said that there is a general lack of public awareness about Bitcoin. The Department of Finance indicated that the Financial Consumer Agency of Canada has provided information about digital currency-related risks, as well as tips about the use and storage of digital currencies.

In commenting on information that Canada's securities regulators have provided about digital currencies, l'Autorité des marchés financiers noted that it has issued a warning about fraud risks and the lack of protection for users of digital currencies under Quebec's financial services compensation fund or its deposit insurance fund. Elliot Greenstone mentioned that the Ontario Securities Commission's initial publication on digital currencies focused on fraud, digital currency exchanges ceasing operations, and the potential connection between digital currencies and money laundering and terrorist financing.

John Jason said that provinces regulate risk through securities laws, such as the requirement to provide a prospectus, and that the government should consider whether digital currencies need to be subject to securities regulation. He suggested that digital currencies should be regulated on the basis of their use – such as an investment or as a currency – and the extent to which, in that use, regulation is required to mitigate any risks. According to Elliot Greenstone, the government has an obligation to provide information about the risks with digital currencies and their technologies, as not everyone has the financial knowledge needed to make informed decisions. He stated that the recent instances of fraud and the Mt. Gox bankruptcy are not representative of all digital currencies and their related businesses.

Although the Department of Finance suggested that Canada's securities regulators could play a role in overseeing digital currencies, l'Autorité des marchés financiers and the Ontario Securities Commission stated that – in their current form – digital currencies do not qualify as "securities" or "derivatives" under their provinces' securities and derivatives legislation and, consequently, are not regulated as such; that said, digital currencies could be packaged as an investment product or a derivative, in which case relevant legislation would apply. L'Autorité des marchés financiers mentioned that a business that markets investments in digital currencies is subject to Quebec's

securities legislation. The Ontario Securities Commission said that any publicly traded digital currency-related business would be subject to the same regulatory requirements as other publicly traded companies, including disclosure to investors about material risks.

(ii) Protection for Users

Witnesses indicated that users of digital currencies and users of traditional banking services do not have the same types of protections. The Royal Bank of Canada suggested that protection when using digital currencies and other types of unregulated payments systems is lacking. The TD Bank Financial Group commented that unregulated digital currencies and payments systems should have consumer protection requirements, as the entities that promote these systems are currently not obliged to disclose the risks with their products, establish procedures to address disputes, or develop processes to enable consumers to monitor their transactions.

According to MasterCard, procedures to resolve unauthorized transactions that occur with digital currencies are inadequate. Visa Canada Corporation said that digital currencies do not provide consumers and merchants with the same types of protection as those with credit cards; the latter offer zero liability for cardholders in the case of unauthorized use of the card and guaranteed payment for merchants.

The Canadian Bankers Association indicated that Canadian banks have not supported any forms of digital currency. It suggested that oversight should be considered for all unregulated payment methods; this oversight would ensure that consumers are properly informed about methods of payment at a merchant or other business, the extent to which payment providers are complying with regulations associated with payments clearing and settlement, and the recourse available if regulatory requirements are not met or there is failure to make the payment in question. It also highlighted the lack of protection if an inadequate number of entities wish to purchase a particular digital currency and illiquidity results.

As well, the Canadian Bankers Association said that there are no advantages to using digital currencies, as financial institutions' digital products provide a better client experience, increased security, a higher level of confidence and clear disclosure of the terms of use. The Royal Bank of Canada stated that Canadians are well served by Canada's current payments system and by the innovations in payments technologies that the country's banks are offering. The Bank of Canada stated that Canadians are well served by the current payments system technologies.

According to the Canadian Payments Association, innovative products and services have enhanced the efficiency of Canada's payments system; however, they have also increased the complexity of – and risks to – that system, and an appropriate level of oversight and regulation must exist. TD Bank Financial Group suggested that there is some systemic risk with unregulated payment method providers, as the standards applied to regulated companies for the protection of Canada's payment system are not applied to these entities.

The Canadian Payments Association explained that not every emerging payment method is subject to oversight in relation to the Canadian payments system. It said that emerging payment methods must be considered in the context of their risks, the ways that these risks can be mitigated, the extent to which these payment methods require access to the clearing and settlement system, and the ability of

regulators to address issues relating to consumer protection and the stability of Canada's payments system.

Regarding regulation of Canada's payments system, the Department of Finance noted that the federal government has broad oversight responsibilities. It mentioned the 2014 federal budget announcement about the development of a comprehensive, risk-based approach to oversight of the Canadian payments system, which will include digital currencies; the Canadian Payments Association supported this announcement. TD Bank Financial Group indicated that Canada's public policy framework for the safety and soundness of the Canadian payments system is operating well because it is based on regulatory oversight of the country's traditional financial institutions. John Jason mentioned that Canada has regulations to ensure the integrity of the payments system, and suggested that some of these safeguards might be applicable to digital currencies.

Bitcoin Foundation Canada commented on Bitcoin, noting that this payments system is largely regulated at present, as consumer protection legislation and the *Civil Code of Quebec* – including provisions regarding implied and legal warranties, as well as disclosure of fees – apply to both digital currency exchanges and consumer contracts where bitcoin is the method of payment.

Similarly, the Bitcoin Alliance of Canada suggested that Bitcoin transactions are currently regulated under consumer protection laws, and that Bitcoin-related businesses will be regulated under anti–money laundering and anti–terrorist financing legislation. In its view, Bitcoin-related regulatory changes may be unnecessary at this time, and Bitcoin should be allowed to find short- and medium-term solutions to consumer-related risks.

Samir Saadi said that regulations for digital currencies should perhaps not be introduced, as the digital currency sector is developing technologies to protect customers against fraud; rather, voluntary standards for best practices, such as for "refundability" of payments, could be less onerous than regulation of digital currency-related businesses. He suggested that, like sellers on eBay, digital currencies and digital currency-related businesses could be rated by their customers. He also indicated that any federal consumer protection legislation in relation to digital currencies should minimize the risk of fraud, and address the ability to reverse transactions and identify the parties involved in a transaction.

The Department of Finance said that it will determine the types of consumer protection measures needed in relation to digital currencies by examining the products and services provided by federally regulated financial institutions.

5. Other Challenges in Using Digital Currencies

In addition to potential criminality, losses, taxation issues, and access to information and protection for users, the Committee's witnesses mentioned other challenges in using digital currencies: the Bitcoin verification process; seignorage revenue for the Bank of Canada and the federal government; and the ability of businesses to access letters of credit for digital currencies.

(i) The Bitcoin Verification Process

Witnesses noted that Bitcoin transactions are not verified immediately. The Department of Finance, BitPay and the Bank of Canada mentioned that the somewhat lengthy verification process for Bitcoin

transactions, which could take an average of 10 minutes, may be a concern for merchants that choose to accept bitcoin directly from customers. In the opinion of Jeremy Clark, these delays are the reason that bitcoin will never replace traditional currencies or become a state-issued currency. According to BitPay, as of 12 June 2014, Bitcoin processed an average of 60 transactions per minute. Visa Canada Corporation said that transactions that occur on Visa's network generally take less than one second to verify and that merchants know instantaneously if the customer has the funds needed to complete the transaction. Ripple Labs highlighted that Ripple's "consensus" verification process takes only a few seconds to complete.

Elliot Greenstone suggested that there is a risk that one entity could acquire 50% of the computing power associated with Bitcoin's blockchain and, thus, potentially control the verification process; for example, if a country acquires 50% of the blockchain's computing power, it could reverse transactions or allow users to "double-spend" their bitcoin.

(ii) Seignorage Revenue

The possibility of lower revenue for the Bank of Canada and the federal government if digital currencies were to replace cash as a means of payment was mentioned. The Bank of Canada highlighted potentially lower revenue for it, and for the federal government, if the demand for digital currencies increases significantly. It explained that the proceeds from issuing banknotes are invested in Government of Canada bonds; the investment generates "seignorage revenue" that is used to pay the Bank's expenses, with the federal government receiving any excess revenue. The Bank said that, in 2013, seignorage revenue was $1.6 billion, and approximately $1.0 billion was remitted to the government. According to the Bank of Canada, a lower demand for cash resulting from increased use of digital currencies would reduce the amount of seignorage revenue available to it and remitted to the government; possibly, the Bank would be unable to finance its expenses, which would impair its ability to fulfil its mandate.

(iii) Access to Letters of Credit

Witnesses discussed the difficulties that some users of digital currencies may face when trying to obtain letters of credit that are based on these currencies. As no central authority exists with decentralized digital currencies and – thereby – letters of credit cannot be given, the Bank of Canada stated that the extent to which digital currencies can be used for business-to-business transactions may be limited.

That said, Andreas Antonopoulos suggested that organizations are going to provide global peer-to-peer lending with digital currencies; this model of lending could provide low-cost credit to individuals in the developing world.

CHAPTER 4: CONCLUSION

In the Committee's view, it is the case that legislators, governments, central banks, private-sector entities in a range of sectors, customers, merchants, investors and others are considering the opportunities and challenges that digital currencies present.

After hearing from a broad range of witnesses in Ottawa, and traveling to New York City for a fact-finding trip, the Committee has concluded that digital currencies and their technologies present a variety of opportunities. In the Committee's view, it is likely that the innovation underlying these currencies and technologies has applications that have not yet been imagined. There is evidence that they reduce transaction costs, increase the choices available to customers and merchants, protect users' identities and record all transactions. A key focus, then, is the actions that the federal government and other entities could take to maximize those opportunities.

Equally, the Committee acknowledges that digital currencies and their technologies present a range of challenges. Money laundering, terrorist financing, losses due to cyber-theft, bankruptcy of digital currency exchanges, price volatility, and a range of taxation issues are serious obstacles for a government whose primary duty is to protect its citizens.

Therefore, the Committee strongly believes that a balanced regulatory approach is needed in the digital currency sector. On one hand, the Committee is mindful that the government has the responsibility to protect consumers and root out illegal activity. On the other hand, it is critical that government action does not stifle innovation in digital currencies and its associated technologies that are in an early and delicate stage of development.

Having completed the study, the Committee is of the opinion that the opportunities presented by digital currencies, technologies and businesses outweigh the challenges. The Committee is confident that the implementation of our recommendations will have positive outcomes for consumers, merchants, digital currency-related businesses, Canada's financial services sector and others. The Committee looks forward to timely government action designed to maximize the opportunities and manage the challenges facing the digital currency sector.

APPENDIX A: WITNESSES

March 26, 2014	Department of Finance Canada	Rachel Grasham, Chief, Financial Crimes - Domestic, Financial Sector Division
March 26, 2014	Department of Finance Canada	David Karp, Economist, Financial Crimes - Domestic, Financial Sector Division
March 26, 2014	Department of Finance Canada	David Murchison, Director, Financial Sector Division
March 27, 2014	As an Individual	Joshua S. Gans, Professor and Area Coordinator of Strategic Management at Rotman School of Management, University of Toronto
March 27, 2014	As an Individual	Warren E. Weber, Economist
April 2, 2014	Bank of Canada	Grahame Johnson, Chief, Funds Management and Banking
April 2, 2014	Bank of Canada	Lukasz Pomorski, Assistant Director, Funds Management and Banking
April 3, 2014	As an Individual	Jeremy Clark, Assistant Professor, Concordia Institute for Information Systems Engineering, Concordia University
April 3, 2014	As an Individual	David Descôteaux, Associate Researcher, Montreal Economic Institute
April 9, 2014	Bit Access	Haseeb Awan, Co-founder
April 9, 2014	Canadian Virtual Exchange (CAVirtEx)	Joseph David, Chief Executive Officer
April 9, 2014	Bitcoin Strategy Group	Kyle Kemper, Partner
April 9, 2014	Canadian Virtual Exchange (CAVirtEx)	Larry O'Brien, Advisor
April 9, 2014	Bitcoin Strategy Group	Victoria van Eyk, Partner
April 10, 2014	Royal Bank of Canada	Jeremy Bornstein, Head, Emerging Payments
April 10, 2014	Royal Bank of Canada	Carolyn Burke, Vice-President, International Cards and Canadian Regulatory Payments
April 10, 2014	Canadian Bankers Association	Darren Hannah, Acting Vice-President, Policy and Operations
April 10, 2014	Canadian Payments Association	Doug Kreviazuk, Vice-President, Policy and Public Affairs
April 10, 2014	Canadian Payments Association	Carol Ann Northcott, Vice-President and Chief Risk Officer
June 5, 2014	Canada Revenue Agency	Michael Cooke, Manager, Income Tax Rulings Directorate

June 5, 2014	Canada Revenue Agency	Eliza Erskine, Director, Income Tax Rulings Directorate
June 12, 2014	BitPay	Tim Byun, Chief Compliance Officer
June 12, 2014	Interac Association	Caroline Hubberstey, Head, External Affairs, Enterprise Strategy
June 12, 2014	PayPal	Barry Murphy, Director, Government Relations, Canada and Latin America
October 1, 2014	Visa Canada Corporation	Derek Colfer, Head of Technology and Innovation
October 1, 2014	MasterCard	Jason Davies, Head of Emerging Payments, Canada
October 1, 2014	MasterCard	Sherri Haymond, Senior Vice President, Digital Channel Engagement, Emerging Payments
October 2, 2014	Bitcoin Foundation Canada	Guillaume Babin-Tremblay, Treasurer
October 2, 2014	Bitcoin Foundation Canada	Jillian Friedman, Legal Officer
October 2, 2014	Bitcoin Alliance of Canada	Stuart Hoegner, General Counsel
October 2, 2014	Bitcoin Alliance of Canada	Michael Perklin, Director
October 2, 2014	Bitcoin Embassy	Francis Pouliot, Director of Public Affairs
October 8, 2014	As an Individual	Andreas M. Antonopoulos, Author of *Mastering Bitcoin*
December 10, 2014	Dominion Bitcoin Mining Company	Jason Dearborn, Chair
December 10, 2014	Digital Finance Institute	Christine Duhaime, Co-founder and Executive Director
December 10, 2014	Digital Finance Institute	Manie Eagar, Co-founder and Chairman
January 28, 2015	Royal Canadian Mounted Police	Jean Cormier, Superintendent, Director, Federal Coordination Centres
January 28, 2015	Royal Canadian Mounted Police	Drew Kyle, Sergeant, Acting Officer in Charge, Financial Crime, Federal Policing Criminal Operations

January 28, 2015	Canadian Security Intelligence Service	Michael Peirce, Assistant Director, Intelligence
February 19, 2015	Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)	Bernard Gagné, Deputy Chief Compliance Officer, Compliance Relations and Support
February 19, 2015	Department of Finance Canada	Lisa Pezzack, Director, Financial Sector, Financial Sector Policy Branch
February 19, 2015	Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)	Martin Tabi, Manager, Research and Strategic Intelligence and International Relationships
February 19, 2015	Department of Finance Canada	Ian Wright, Chief, Financial Crimes - Domestic, Financial Sector Policy Branch
February 26, 2015	As an Individual	Elliot A. Greenstone, Lawyer, Davies Ward Phillips & Vineberg LLP
February 26, 2015	As an Individual	John Jason, Of Counsel, Norton Rose Fulbright Canada
February 26, 2015	Ripple Labs	Greg Kidd, Chief Risk Officer
March 11, 2015	TD Bank Financial Group	Paul Milkman, Senior Vice President and Head, Technology Risk Management and Information Security
March 12, 2015	Autorité des marchés financiers	Christian Desjardins, Manager, Market Surveillance, Enforcement Branch
March 12, 2015	Autorité des marchés financiers	Moad Fahmi, Financial Markets Specialist, Specialized Investigation Support Unit, Enforcement Branch
March 12, 2015	Autorité des marchés financiers	Jean-François Fortin, Executive Director, Enforcement Branch
March 12, 2015	Ontario Securities Commission	Paul Redman, Principal Economist, Strategy and Operations
March 12, 2015	Ontario Securities Commission	James Sinclair, General Counsel, General Counsel's Office
March 25, 2015	Bill & Melinda Gates Foundation	Rodger Voorhies, Director, Global Development, Financial Services for the Poor
March 26, 2015	MoneyGram International	Derek McMillan, Senior Director, Regional Compliance
March 26, 2015	As an Individual	Samir Saadi, Assistant Professor, Telfer School of Management, University of Ottawa

APPENDIX B: FACT-FINDING MISSION IN NEW YORK – FEBRUARY 2-4, 2015

February 2, 2015	Consulate General of Canada in New York	John F. Prato, Consul General
	As an Individual	Jeffrey Robinson, Financial Crime Journalist
	Circle Internet Financial Ltd.	John A. Beccia, General Counsel and Chief Compliance Officer
February 3, 2015	U.S. Department of the Treasury and the Financial Crimes Enforcement Network (FinCEN)	Sarah Runge, Director, Office of Strategic Policy for Terrorist Financing and Financial Crimes, U.S. Department of the Treasury
		Scott Rembrandt, Assistant Director, Office of Strategic Policy for Terrorist Financing and Financial Crimes, U.S. Department of the Treasury
		Jamal El-Hindi, Associate Director, Regulatory Policy and Programs Division, FinCEN
	U.S. Department of Homeland Security	Tate Jarrow, Special Agent, U.S. Secret Service
	Federal Reserve Bank of New York	Rodney Garratt, Vice President, Money and Payments Studies Function
		Vanessa Kagenian, Supervisory Associate
		Alex Entz, Policy and Markets Senior Analyst
		David A. Duttenhofer, Jr., Senior Vice President, Legal & Compliance Risk Function, Financial Institution Supervision Group
	New York State Department of Financial Services	Maria Filipakis, Executive Deputy Superintendent
		Dana Syracuse, Assistant General Counsel
		Colleen O'Brien, Senior Counsel
		Alexander Sand, Counsel
		Tom Eckmier, Snior Attorney

	New York Police Department	Lieutenant Kevin Yorke, Lieutenant Detective Commander Intelligence Division – Cyber intelligence & Analytical Programs
	Financial Crimes Enforcement Network (FinCEN)	Gary Novis, Director, Office of Strategic Policy
		Horacio Madinaveitia, Senior Regulatory Policy Officer
		Kevin Bleckley, Section Chief, Illicit Finance Methodologies
	U.S. Department of the Treasury (IRS)	Anne Wallmork, Senior Counselor, Strategic Policy, Office of Strategic Policy for Terrorist Financing and Financial Crimes
	Perkins Coie	Keith W. Miller, Partner and Firm-wide Chair
	As Individuals	Cameron Winklevoss Tyler Winklevoss
February 4, 2015	U.S. Internal Revenue Service	Gary L. Alford, Special Agent, Criminal Investigation, U.S. Internal Revenue Service
	Coin Comply	Brian Stoeckert, Managing Director and Chief Strategy Officer
	Bitcoin Centre NYC	Nick Spanos, CEO and Founder

APPENDIX C: GLOSSARY OF DIGITAL CURRENCY-RELATED TERMS

Bitcoin Blockchain (or Public Ledger): The public registry for all Bitcoin transactions, which are successively added in blocks once they have been validated through the mining process.

Centralized Digital Currency: A digital currency that has a single central authority that manages the supply, creates the rules for exchange and use, verifies transactions and maintains a central ledger of transactions.

Convertible Digital Currency: A digital currency that can be converted to a state-issued currency, and vice versa.

Cryptocurrency: A decentralized digital currency that is convertible and functions as both a currency and a decentralized payments system. Transactions are recorded on a public ledger, which is shared across a peer-to-peer network, and the validity of transactions is verified through cryptographic techniques. Bitcoin is an example.

Decentralized Digital Currency: A digital currency that is open-source, lacks a central authority and operates over an Internet-based peer-to-peer network; transactions using that currency are validated through that network.

Digital Currency: Electronic forms of exchange and their associated technologies that operate on the Internet and/or on mobile devices, and that are not issued or controlled by a government or central bank.

Digital Currency Exchange: A business that allows customers to convert fiat currency to digital currency and digital currencies to fiat currency or other digital currencies.

Mining: The process through which “miners” on the Bitcoin network compete to solve a “random hash algorithm” to validate and add a block of transactions to the public ledger, and for which they receive bitcoin as compensation.

Money Services Business: As defined by the Financial Transactions and Reports Analysis Centre of Canada, any Canadian business that offers foreign exchange dealing or money transferring services, or that cash or sell money orders, traveller's cheques or similar monetary instruments.

Non-Convertible Digital Currency: A digital currency that can only be used in relation to a particular retailer or virtual marketplace to purchase real or virtual goods and services; it cannot be converted to state-issued currency.

State-Issued Currency: A currency that is designated by a country as its legal tender, and that is customarily used and accepted as a medium of exchange in the issuing country.

Exhibit M

Advance Edited Version

Distr.: General
22 May 2015

Original: English

Human Rights Council
Twenty-ninth session
Agenda item 3
Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development

Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye*

Summary

In the present report, submitted in accordance with Human Rights Council resolution 25/2, the Special Rapporteur addresses the use of encryption and anonymity in digital communications. Drawing from research on international and national norms and jurisprudence, and the input of States and civil society, the report concludes that encryption and anonymity enable individuals to exercise their rights to freedom of opinion and expression in the digital age and, as such, deserve strong protection.

* Late submission.

Contents

I. Introduction

1. Contemporary digital technologies offer Governments, corporations, criminals and pranksters unprecedented capacity to interfere with the rights to freedom of opinion and expression. Online censorship, mass and targeted surveillance and data collection, digital attacks on civil society and repression resulting from online expression force individuals around the world to seek security to hold opinions without interference and seek, receive and impart information and ideas of all kinds. Many seek to protect their security through encryption, the scrambling of data so only intended recipients may access it, which may be applied to data in transit (e.g., e-mail, messaging, Internet telephony) and at rest (e.g., hard drives, cloud services). Others seek additional protection in anonymity, using sophisticated technologies to disguise their identity and digital footprint. Encryption and anonymity, today's leading vehicles for online security, provide individuals with a means to protect their privacy, empowering them to browse, read, develop and share opinions and information without interference and enabling journalists, civil society organizations, members of ethnic or religious groups, those persecuted because of their sexual orientation or gender identity, activists, scholars, artists and others to exercise the rights to freedom of opinion and expression.

2. Yet, just as the telephone may be used both to report a crime to the police and to conspire to commit one, so too may the Internet be abused to interfere with the rights of others, national security or public order. Law enforcement and intelligence services often assert that anonymous or encrypted communications make it difficult to investigate financial crimes, illicit drugs, child pornography and terrorism. Individuals express legitimate concerns about how bullies and criminals use new technologies to facilitate harassment. Some States restrict or prohibit encryption and anonymity on these and other grounds, while others are proposing or implementing means for law enforcement to circumvent these protections and access individual communications.

3. In the light of these challenges, the present report examines two linked questions. First, do the rights to privacy and freedom of opinion and expression protect secure online communication, specifically by encryption or anonymity? And, second, assuming an affirmative answer, to what extent may Governments, in accordance with human rights law, impose restrictions on encryption and anonymity? The present report seeks to answer these questions, review examples of State practice and propose recommendations. It does not purport to address every technical or legal question raised by digital technologies, but it identifies important ones for future reporting.

4. In preparing the report, the Special Rapporteur circulated a questionnaire to States, seeking relevant information on their domestic laws, regulations, policies and practices. As of 1 April 2015, 16 States had responded to this request.[1] The Special Rapporteur also issued a call for submissions from non-governmental stakeholders and convened a meeting of experts in Geneva in March 2015. The responses from Governments and the over 30 submissions by civil society organizations and individuals, which are available from the mandate holder's web page, contributed significantly to the preparation of the report.

5. A full review of the Special Rapporteur's activities since the beginning of his term in August 2014 may be found on the mandate holder's web page. This report, the current

[1] Responses were received from Austria, Bulgaria, Cuba, Germany, Greece, Guatemala, Ireland, Kazakhstan, Lebanon, Qatar, Republic of Moldova, Norway, Slovakia, Sweden, Turkey and the United States of America.

mandate holder's first, aims at furthering the work on the challenges to freedom of expression in the digital age.

II. Secure and private communication in the digital age

A. Contemporary encryption and anonymity

6. Modern approaches to private and secure communication draw on ideas that have been with humankind for millenniums. The rise of electronic data storage, the Internet and mass data collection and retention made clear that sophisticated means would be needed to protect individual, corporate and government data. As e-mail, instant-messaging, Voice-over-Internet Protocols, videoconferencing and social media moved from niche services to predominant and easily monitored modes of communication, individuals developed a need for security online, so that they could seek, receive and impart information without the risk of repercussions, disclosure, surveillance or other improper use of their opinions and expression.

7. Encryption — a mathematical "process of converting messages, information, or data into a form unreadable by anyone except the intended recipient" [2] — protects the confidentiality and integrity of content against third-party access or manipulation. Strong encryption, once the sole province of militaries and intelligence services, is now publicly accessible and often freely available to secure e-mail, voice communication, images, hard drives and website browsers. With "public key encryption", the dominant form of end-to-end security for data in transit, the sender uses the recipient's public key to encrypt the message and its attachments, and the recipient uses her or his own private key to decrypt them. Encryption may also be used to create digital signatures to ensure that a document and its sender are authentic, to authenticate and verify the identity of a server and to protect the integrity of communications between clients against tampering or manipulation of traffic by third parties (e.g., "man-in-the-middle" attacks). Since the encryption of data in transit does not ensure against attacks on unencrypted data when it is sitting at rest at either endpoint (nor protect the security of one's private key), one may also encrypt data at rest stored on laptops, hard drives, servers, tablets, mobile phones and other devices. Online practices may also be moving away from the system described here and towards "forward secrecy" or "off-the-record" technology in which keys are held ephemerally, particularly for uses such as instant messaging.

8. Some call for efforts to weaken or compromise encryption standards such that only Governments may enjoy access to encrypted communications. However, compromised encryption cannot be kept secret from those with the skill to find and exploit the weak points, whether State or non-State, legitimate or criminal. It is a seemingly universal position among technologists that there is no special access that can be made available only to government authorities, even ones that, in principle, have the public interest in mind. In the contemporary technological environment, intentionally compromising encryption, even for arguably legitimate purposes, weakens everyone's security online.

9. Notably, encryption protects the content of communications but not identifying factors such as the Internet Protocol (IP) address, known as metadata. Third parties may gather significant information concerning an individual's identity through metadata analysis if the user does not employ anonymity tools. Anonymity is the condition of avoiding identification. A common human desire to protect one's identity from the crowd,

[2] See SANS Institute, "History of encryption" (2001).

anonymity may liberate a user to explore and impart ideas and opinions more than she would using her actual identity. Individuals online may adopt pseudonyms (or, for instance, fake e-mail or social media accounts) to hide their identities, image, voice, location and so forth, but the privacy afforded through such pseudonyms is superficial and easily disturbed by Governments or others with the necessary expertise; in the absence of combinations of encryption and anonymizing tools, the digital traces that users leave behind render their identities easily discoverable. Users seeking to ensure full anonymity or mask their identity (such as hiding the original IP address) against State or criminal intrusion may use tools such as virtual private networks (VPNs), proxy services, anonymizing networks and software, and peer-to-peer networks.[3] One well-known anonymity tool, the Tor network, deploys more than 6,000 decentralized computer servers around the world to receive and relay data multiple times so as to hide identifying information about the end points, creating strong anonymity for its users.

10. A key feature of the digital age is that technology changes incessantly to sate user demands. Although the present report refers to contemporary technologies that facilitate encryption and anonymity, its analysis and conclusions apply generally to the concepts behind the current technologies and should be applicable as new technologies replace the old.

B. Uses of the technologies

11. The Internet has profound value for freedom of opinion and expression, as it magnifies the voice and multiplies the information within reach of everyone who has access to it. Within a brief period, it has become the central global public forum. As such, an open and secure Internet should be counted among the leading prerequisites for the enjoyment of the freedom of expression today. But it is constantly under threat, a space — not unlike the physical world — in which criminal enterprise, targeted repression and mass data collection also exist. It is thus critical that individuals find ways to secure themselves online, that Governments provide such safety in law and policy and that corporate actors design, develop and market secure-by-default products and services. None of these imperatives is new. Early in the digital age, Governments recognized the essential role played by encryption in securing the global economy, using or encouraging its use to secure Government-issued identity numbers, credit card and banking information, business proprietary documents and investigations into online crime itself.[4]

12. Encryption and anonymity, separately or together, create a zone of privacy to protect opinion and belief. For instance, they enable private communications and can shield an opinion from outside scrutiny, particularly important in hostile political, social, religious and legal environments. Where States impose unlawful censorship through filtering and other technologies, the use of encryption and anonymity may empower individuals to circumvent barriers and access information and ideas without the intrusion of authorities. Journalists, researchers, lawyers and civil society rely on encryption and anonymity to shield themselves (and their sources, clients and partners) from surveillance and harassment. The ability to search the web, develop ideas and communicate securely may be the only way in which many can explore basic aspects of identity, such as one's gender, religion, ethnicity, national origin or sexuality. Artists rely on encryption and anonymity to

[3] Proxy services send data through an intermediary, or "proxy server", that sends that data on behalf of the user, effectively masking the user's IP address with its own to the end recipient. Peer-to-peer networks partition and store data among interconnected servers and then encrypt that stored data so that no centralized server has access to identifying information. See, for example, Freenet.

[4] See OECD, *Guidelines for Cryptography Policy* (1997)..

safeguard and protect their right to expression, especially in situations where it is not only the State creating limitations but also society that does not tolerate unconventional opinions or expression.

13. The "dark" side of encryption and anonymity is a reflection of the fact that wrongdoing offline takes place online as well. Law enforcement and counter-terrorism officials express concern that terrorists and ordinary criminals use encryption and anonymity to hide their activities, making it difficult for Governments to prevent and conduct investigations into terrorism, the illegal drug trade, organized crime and child pornography, among other government objectives. Harassment and cyberbullying may rely on anonymity as a cowardly mask for discrimination, particularly against members of vulnerable groups. At the same time, however, law enforcement often uses the same tools to ensure their own operational security in undercover operations, while members of vulnerable groups may use the tools to ensure their privacy in the face of harassment. Moreover, Governments have at their disposal a broad set of alternative tools, such as wiretapping, geo-location and tracking, data-mining, traditional physical surveillance and many others, which strengthen contemporary law enforcement and counter-terrorism.[5]

III. Encryption, anonymity and the rights to freedom of opinion and expression and privacy

14. The human rights legal framework for encryption and anonymity requires, first, evaluating the scope of the rights at issue and their application to encryption and anonymity; and, second, assessing whether, and if so to what extent, restrictions may lawfully be placed on the use of technologies that promote and protect the rights to privacy and freedom of opinion and expression.

15. The rights to privacy[6] and freedom of opinion and expression[7] have been codified in universal and regional human rights instruments, interpreted by treaty bodies and regional courts, and evaluated by special procedures of the Human Rights Council and during universal periodic review. The universal standards for privacy, opinion and expression are found in the International Covenant on Civil and Political Rights, to which 168 States are party. Even for those remaining States that are not bound by it, the Covenant presents at the very least a standard for achievement and often reflects a customary legal norm; those that have signed but not ratified the Covenant are bound to respect its object and purpose under article 18 of the Vienna Convention on the Law of Treaties. National legal systems also protect privacy, opinion and expression, sometimes with constitutional or basic law or interpretations thereof. Several global civil society projects have also provided compelling demonstrations of the law that should apply in the context of the digital age, such as the International Principles on the Application of Human Rights to Communications

[5] See Center for Democracy and Technology, "'Going Dark' versus a 'Golden Age for Surveillance'" (2011).

[6] Article 12 of the Universal Declaration of Human Rights, article 17 of the International Covenant on Civil and Political Rights, article 16 of the Convention on the Rights of the Child, article 22 of the Convention on the Rights of Persons with Disabilities, article 14 of the Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, article 8 of the European Convention on Human Rights and article 11 of the American Convention on Human Rights protect the right to privacy.

[7] Article 19 of the Universal Declaration and the International Covenant on Civil and Political Rights, article 9 of the African Charter on Human and Peoples' Rights, article 13 of the American Convention on Human Rights and article 10 of the European Convention on Human Rights protect freedom of expression.

Surveillance and the Global Principles on National Security and the Right to Information. Although specific standards may vary from right to right, or instrument to instrument, a common thread in the law is that, because the rights to privacy and to freedom of expression are so foundational to human dignity and democratic governance, limitations must be narrowly drawn, established by law and applied strictly and only in exceptional circumstances. In a digital age, protecting such rights demands exceptional vigilance.

A. Privacy as a gateway for freedom of opinion and expression

16. Encryption and anonymity provide individuals and groups with a zone of privacy online to hold opinions and exercise freedom of expression without arbitrary and unlawful interference or attacks. The previous mandate holder noted that the rights to "privacy and freedom of expression are interlinked" and found that encryption and anonymity are protected because of the critical role they can play in securing those rights (A/HRC/23/40 and Corr.1). Echoing article 12 of the Universal Declaration of Human Rights, article 17 of the International Covenant on Civil and Political Rights specifically protects the individual against "arbitrary or unlawful interference with his or her privacy, family, home or correspondence" and "unlawful attacks on his or her honour and reputation", and provides that "everyone has the right to the protection of the law against such interference or attacks". The General Assembly, the United Nations High Commissioner for Human Rights and special procedure mandate holders have recognized that privacy is a gateway to the enjoyment of other rights, particularly the freedom of opinion and expression (see General Assembly resolution 68/167, A/HRC/13/37 and Human Rights Council resolution 20/8).

17. Encryption and anonymity are especially useful for the development and sharing of opinions, which often occur through online correspondence such as e-mail, text messaging, and other online interactions. Encryption provides security so that individuals are able "to verify that their communications are received only by their intended recipients, without interference or alteration, and that the communications they receive are equally free from intrusion" (see A/HRC/23/40 and Corr.1, para. 23). Given the power of metadata analysis to specify "an individual's behaviour, social relationships, private preferences and identity" (see A/HRC/27/37, para. 19), anonymity may play a critical role in securing correspondence. Besides correspondence, international and regional mechanisms have interpreted privacy to involve a range of other circumstances as well.[8]

18. Individuals and civil society are subjected to interference and attack by State and non-State actors, against which encryption and anonymity may provide protection. In article 17 (2) of the International Covenant on Civil and Political Rights, States are obliged to protect privacy against unlawful and arbitrary interference and attacks. Under such an affirmative obligation, States should ensure the existence of domestic legislation that prohibits unlawful and arbitrary interference and attacks on privacy, whether committed by government or non-governmental actors. Such protection must include the right to a remedy for a violation.[9] In order for the right to a remedy to be meaningful, individuals must be given notice of any compromise of their privacy through, for instance, weakened encryption or compelled disclosure of user data.

[8] Human Rights Committee, general comment No. 16 (1988) on the right to respect of privacy, family, home and correspondence, and protection of honour and reputation. See also European Court of Human Rights, factsheets on data protection (www.echr.coe.int/Documents/FS_Data_ENG.pdf) and right to protection of one's image (www.echr.coe.int/Documents/FS_Own_image_ENG.pdf).

[9] See Human Rights Committee general comment No.16 and general comment No. 31on the nature of the general legal obligation imposed on States parties to the Covenant; and CCPR/C/106/D/1803/2008.

B. Right to hold opinions without interference

19. The first article of the Universal Declaration of Human Rights recognizes that everyone is "endowed with reason and conscience", a principle developed further in human rights law to include, among other things, the protection of opinion, expression, belief, and thought. Article 19 (1) of the International Covenant on Civil and Political Rights, also echoing the Universal Declaration, provides that "everyone shall have the right to hold opinions without interference". Opinion and expression are closely related to one another, as restrictions on the right to receive information and ideas may interfere with the ability to hold opinions, and interference with the holding of opinions necessarily restricts the expression of them. However, human rights law has drawn a conceptual distinction between the two. During the negotiations on the drafting of the Covenant, "the freedom to form an opinion and to develop this by way of reasoning was held to be absolute and, in contrast to freedom of expression, not allowed to be restricted by law or other power".[10] The ability to hold an opinion freely was seen to be a fundamental element of human dignity and democratic self-governance, a guarantee so critical that the Covenant would allow no interference, limitation or restriction. Consequently, the permissible limitations in article 19 (3) expressly apply only to the right to freedom of expression in article 19 (2). Interference with the right to hold opinions is, by contrast, per se in violation of article 19 (1).

20. Commentators and courts have devoted much less attention to the right to hold opinions than to expression. Greater attention is warranted, however, as the mechanics of holding opinions have evolved in the digital age and exposed individuals to significant vulnerabilities. Individuals regularly hold opinions digitally, saving their views and their search and browse histories, for instance, on hard drives, in the cloud, and in e-mail archives, which private and public authorities often retain for lengthy if not indefinite periods. Civil society organizations likewise prepare and store digitally memoranda, papers and publications, all of which involve the creation and holding of opinions. In other words, holding opinions in the digital age is not an abstract concept limited to what may be in one's mind. And yet, today, holding opinions in digital space is under attack. Offline, interference with the right to hold an opinion may involve physical harassment, detention or subtler efforts to punish individuals for their opinion (see CCPR/C/78/D/878/1999, annex, paras. 2.5, 7.2 and 7.3). Interference may also include such efforts as targeted surveillance, distributed denial of service attacks, and online and offline intimidation, criminalization and harassment. Targeted digital interference harasses individuals and civil society organizations for the opinions they hold in many formats. Encryption and anonymity enable individuals to avoid or mitigate such harassment.

21. The right to hold opinions without interference also includes the right to form opinions. Surveillance systems, both targeted and mass, may undermine the right to form an opinion, as the fear of unwilling disclosure of online activity, such as search and browsing, likely deters individuals from accessing information, particularly where such surveillance leads to repressive outcomes. For all these reasons, restrictions on encryption and anonymity must be assessed to determine whether they would amount to an impermissible interference with the right to hold opinions.

[10] Manfred Nowak, *UN Covenant on Civil and Political Rights: CCPR Commentary* (1993), p. 441.

C. Right to freedom of expression

22. The right to freedom of expression under article 19 (2) of the International Covenant on Civil and Political Rights expands upon the Universal Declaration's already broad guarantee, protecting the "freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice". A significant accumulation of jurisprudence, special procedure reporting, and resolutions within the United Nations and regional human rights systems underscores that the freedom of expression "is essential for the enjoyment of other human rights and freedoms and constitutes a fundamental pillar for building a democratic society and strengthening democracy" (Human Rights Council resolution 25/2). The Human Rights Council, the General Assembly and individual States regularly assert that individuals enjoy the same rights online that they enjoy offline.[11] The present report will not repeat all the elements of this consensus. In the context of encryption and anonymity, three aspects of the text deserve particular emphasis (see paras. 23–26 below).

23. **Freedom to seek, receive, and impart information and ideas:** In environments of prevalent censorship, individuals may be forced to rely on encryption and anonymity in order to circumvent restrictions and exercise the right to seek, receive and impart information. Some States have curtailed access with a variety of tools. State censorship, for instance, poses sometimes insurmountable barriers to the right to access information. Some States impose content-based, often discriminatory restrictions or criminalize online expression, intimidating political opposition and dissenters and applying defamation and lese-majesty laws to silence journalists, defenders and activists. A VPN connection, or use of Tor or a proxy server, combined with encryption, may be the only way in which an individual is able to access or share information in such environments.

24. It bears emphasizing that human rights law also protects the right to seek, receive and impart scientific information and ideas. The Universal Declaration and the International Covenant on Economic, Social and Cultural Rights protect rights to education and "to share in scientific advancement and its benefits". Encryption and anonymity technologies enable individuals to share in such information in situations where they are otherwise denied, and they are themselves examples of scientific advancement. Their use empowers individuals to gain access to the benefits of scientific progress that might be curtailed by Government. The Special Rapporteur in the field of cultural rights noted that "the rights to science and to culture should both be understood as including a right to have access to and use information and communication and other technologies in self-determined and empowering ways" (see A/HRC/20/26, para. 19).

25. **Regardless of frontiers:** The major instruments guaranteeing freedom of expression explicitly acknowledge the transboundary scope of the right. Individuals enjoy the right to receive information from, and transmit information and ideas of all kinds to, places beyond their borders.[12] However, some States filter or block data on the basis of keywords, denying access by deploying technologies that rely on access to text. Encryption enables an individual to avoid such filtering, allowing information to flow across borders. Moreover, individuals do not control — and are usually unaware of — how or if their communications cross borders. Encryption and anonymity may protect information of all individuals as it transits through servers located in third countries that filter content.

[11] See, e.g., General Assembly resolution 68/167, Human Rights Council resolution 26/13 and Council of Europe recommendation CM/Rec (2014) 6 of the Committee of Ministers to member States on a guide to human rights for Internet users.

[12] The European Court of Human Rights has recognized this point. See *Ahmet Yildirim* v. *Turkey*,(2012); *Cox* v. *Turkey*, (2010); *Case of Groppera Radio AG and Others* v. *Switzerland* (1990).

26. **Through any media:** Articles 19 of the Universal Declaration and the International Covenant on Civil and Political Rights were drafted with the foresight to accommodate future technological advances (A/HRC/17/27). The States parties to the Covenant chose to adopt the general phrase "through any other media" as opposed to an enumeration of then-existing media. Partly on this basis, international mechanisms have repeatedly acknowledged that the protections of freedom of expression apply to activities on the Internet. Regional courts have likewise recognized that protections apply online.[13] The European Court of Human Rights, in discussing the similar protection of expression in the European Convention for the Protection of Human Rights and Fundamental Freedoms, has indicated that the forms and means through which information is transmitted and received are themselves protected, since any restriction imposed on the means necessarily interferes with the right to receive and impart information.[14] In this sense, encryption and anonymity technologies are specific media through which individuals exercise their freedom of expression.

D. Roles of corporations

27. Corporations in a variety of sectors play roles in advancing or interfering with privacy, opinion and expression, including encryption and anonymity. Much online communication (and virtually all of it in some countries) is carried on networks owned and operated by private corporations, while other corporations own and manage websites with substantial user-generated content. Others are active players in the surveillance and spyware markets, providing hardware and software to Governments to compromise the security of individuals online. Others develop and provide services for secure and private online storage. Telecommunications entities, Internet service providers, search engines, cloud services and many other corporate actors, often described as intermediaries, promote, regulate or compromise privacy and expression online. Intermediaries may store massive volumes of user data, to which Governments often demand access. Encryption and anonymity may be promoted or compromised by each of these corporate actors.

28. A full exploration of the role of corporations to protect their users' security online is beyond the scope of the present report, which is focused on State obligations. However, it remains important to emphasize that "the responsibility to respect human rights applies throughout a company's global operations regardless of where its users are located, and exists independently of whether the State meets its own human rights obligations" (see A/HRC/27/37, para. 43). At a minimum, corporations should apply principles such as those laid out in the Guiding Principles on Business and Human Rights, the Global Network Initiative's Principles on Freedom of Expression and Privacy, the European Commission's ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights and the Telecommunications Industry Dialogue Guiding Principles, which encourage corporations to commit to protect human rights, undertake due diligence to ensure the positive human rights impact of their work and remediate adverse impacts of their work on human rights. In the future, the Special Rapporteur will focus on the roles

[13] European Commission of Human Rights, *Neij and Sunde Kolmisoppi* v. *Sweden*, (2013); European Court of Human Rights, *Perrin* v. *United Kingdom*, (2005); African Court on Human and Peoples' Rights, *Zimbabwe Lawyers for Human Rights and Institute for Human Rights and Development (on behalf of Meldrum)* v. *Zimbabwe* (2009); *Case of Herrera Ulloa* v. *Costa Rica*, *Herrera Ulloa* v. *Costa Rica*, Preliminary Objections, Merits, Reparations and Costs, Series C No. 107, IHRL 1490 (IACHR 2004).

[14] See *Autronic AG* v. *Switzerland* (1990); *De Haes and Gijsels* v. *Belgium* (1997), para. 48; *News Verlags GmbH and Co.KG v. Austria* (2000).

corporations should play in preserving individual security to exercise freedom of opinion and expression.

IV. Evaluating restrictions on encryption and anonymity

A. Legal framework

29. The permissible limitations on the right to privacy should be read strictly, particularly in an age of pervasive online surveillance — whether passive or active, mass or targeted — regardless of whether the applicable standards are "unlawful and arbitrary" under article 17 of the International Covenant on Civil and Political Rights, "arbitrary" under article 12 of the Universal Declaration, "arbitrary or abusive" under article 11 of the American Convention on Human Rights, or "necessary in a democratic society" under article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (see A/HRC/13/37, paras. 14–19). Privacy interferences that limit the exercise of the freedoms of opinion and expression, such as those described in this report, must not in any event interfere with the right to hold opinions, and those that limit the freedom of expression must be provided by law and necessary and proportionate to achieve one of a handful of legitimate objectives.

30. No restrictions may be imposed on the right to hold opinions without interference; restrictions under article 19 (3) of the Covenant only apply to expression under article 19 (2). In environments where one's opinions, however held online, result in surveillance or harassment, encryption and anonymity may provide necessary privacy. Restrictions on such security tools may interfere with the ability of individuals to hold opinions.

31. Restrictions on encryption and anonymity, as enablers of the right to freedom of expression, must meet the well-known three-part test: any limitation on expression must be provided for by law; may only be imposed for legitimate grounds (as set out in article 19 (3) of the Covenant); and must conform to the strict tests of necessity and proportionality.

32. First, for a restriction on encryption or anonymity to be "provided for by law", it must be precise, public and transparent, and avoid providing State authorities with unbounded discretion to apply the limitation (see Human Rights Committee, general comment No. 34 (2011)). Proposals to impose restrictions on encryption or anonymity should be subject to public comment and only be adopted, if at all, according to regular legislative process. Strong procedural and judicial safeguards should also be applied to guarantee the due process rights of any individual whose use of encryption or anonymity is subject to restriction. In particular, a court, tribunal or other independent adjudicatory body must supervise the application of the restriction.[15]

33. Second, limitations may only be justified to protect specified interests: rights or reputations of others; national security; public order; public health or morals. Even where a State prohibits by law "advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence, as provided by Article 20 of the Covenant, any restrictions on expression must be consistent with Article 19(3) (A/67/357). No other grounds may justify restrictions on the freedom of expression. Moreover, because

[15] See International Covenant on Civil and Political Rights, article 2 (3)(b); CCPR/C/79/Add.110, para. 22; the Johannesburg Principles on National Security, Freedom of Expression and Access to Information.

legitimate objectives are often cited as a pretext for illegitimate purposes, the restrictions themselves must be applied narrowly.[16]

34. Third, the State must show that any restriction on encryption or anonymity is "necessary" to achieve the legitimate objective.[17] The European Court of Human Rights has concluded appropriately that the word "necessary" in article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms means that the restriction must be something more than "useful," "reasonable" or "desirable".[18] Once the legitimate objective has been achieved, the restriction may no longer be applied. Given the fundamental rights at issue, limitations should be subject to independent and impartial judicial authority, in particular to preserve the due process rights of individuals.

35. Necessity also implies an assessment of the proportionality of the measures limiting the use of and access to security online.[19] A proportionality assessment should ensure that the restriction is "the least intrusive instrument amongst those which might achieve the desired result".[20] The limitation must target a specific objective and not unduly intrude upon other rights of targeted persons, and the interference with third parties' rights must be limited and justified in the light of the interest supported by the intrusion. The restriction must also be "proportionate to the interest to be protected".[21] A high risk of damage to a critical, legitimate State interest may justify limited intrusions on the freedom of expression. Conversely, where a restriction has a broad impact on individuals who pose no threat to a legitimate government interest, the State's burden to justify the restriction will be very high.[22] Moreover, a proportionality analysis must take into account the strong possibility that encroachments on encryption and anonymity will be exploited by the same criminal and terrorist networks that the limitations aim to deter. In any case, "a detailed and evidence-based public justification" is critical to enable transparent public debate over restrictions that implicate and possibly undermine freedom of expression (see A/69/397, para. 12).

B. State practice: examples and concerns

36. The trend lines regarding security and privacy online are deeply worrying. States often fail to provide public justification to support restrictions. Encrypted and anonymous communications may frustrate law enforcement and counter-terrorism officials, and they complicate surveillance, but State authorities have not generally identified situations — even in general terms, given the potential need for confidentiality — where a restriction has been necessary to achieve a legitimate goal. States downplay the value of traditional non-digital tools in law enforcement and counter-terrorism efforts, including transnational

[16] See Human Rights Committee, general comment No. 34 on freedom of opinion and expression, para. 30, and general comment No. 31.

[17] See Human Rights Committee, general comment No. 34, para. 2, and communication No. 2156/2012, Views adopted on 10 October 2014.

[18] See *Case of The Sunday Times* v. *United Kingdom*, judgement of 26 April 1979, para. 59.

[19] See African Court Human and Peoples' Rights, *Lohe Issa Konate* v. *Burkina Faso*, application No. 004/2013, paras. 148 and 149 (2014); European Court of Human Rights, *Case of The Sunday Times*, para. 62.

[20] See Human Rights Committee, general comment No. 27 (1999) on freedom of movement, para. 14.

[21] See ibid., para. 14.

[22] See Inter-American Commission on Human Rights, OEA /Serv.L/V/II.149, para. 134.

cooperation.[23] As a consequence, the public lacks an opportunity to measure whether restrictions on their online security would be justified by any real gains in national security and crime prevention. Efforts to restrict encryption and anonymity also tend to be quick reactions to terrorism, even when the attackers themselves are not alleged to have used encryption or anonymity to plan or carry out an attack. Moreover, even where the restriction is arguably in pursuit of a legitimate interest, many laws and policies regularly do not meet the standards of necessity and proportionality and have broad, deleterious effects on the ability of all individuals to exercise freely their rights to privacy and freedom of opinion and expression.

37. It also bears noting that the United Nations itself has not provided strong communication security tools to its staff or to those who would visit United Nations websites, making it difficult for those under threat to securely reach the United Nations, human rights mechanisms online.[24]

1. Encryption

38. Some Governments seek to protect or promote encryption to ensure the privacy of communications. For instance,[25] the Marco Civil da Internet Law of Brazil, adopted in 2014, guarantees the inviolability and secrecy of user communications online, permitting exceptions only by court order. The E-Commerce Act and Telecommunication Act of Austria do not restrict encryption, and the Government has undertaken public awareness campaigns to educate the public about digital security. Greek law and regulations promote the effective use of both encryption and anonymity tools. Germany, Ireland and Norway permit and promote the use of encryption technologies and oppose any efforts to weaken encryption protocols. Similarly, Swedish and Slovak laws do not restrict the use of encryption online. The United States of America encourages the use of encryption, and the United States Congress should further consider a secure data act introduced in the Congress that would prohibit the Government from requiring companies to weaken product security or insert back-door access measures. Several Governments fund efforts to share or train in the use of encryption and anonymity technologies to help individuals evade censorship and protect their security online, including Canada, the Netherlands, Sweden, the United Kingdom of Great Britain and Northern Ireland and the United States. In addition, export regulations should facilitate the transfer of encryption technologies wherever possible. Although the present report does not provide an overall legal assessment of all national approaches to encryption, these noted elements — non-restriction or comprehensive protection, the requirement of court orders for any specific limitation, and public education — deserve wider application as means to protect and promote the rights to freedom of opinion and expression.

39. Nonetheless, the regulation of encryption often fails to meet freedom of expression standards in two leading respects. First, restrictions have generally not been shown to be necessary to meet a particular legitimate interest. This is especially the case given the breadth and depth of other tools, such as traditional policing and intelligence and transnational cooperation, that may already provide substantial information for specific law enforcement or other legitimate purposes. Second, they disproportionately impact the rights

[23] But see Centre for International Governance Innovation and Chatham House, *Toward a Social Compact for Digital Privacy and Security: Statement by the Global Commission on Internet Governance* (2015).

[24] For instance, staff of the Office of the United Nations High Commissioner for Human Rights (OHCHR) in Geneva do not have access to end-to-end e-mail encryption, and the OHCHR website is not encrypted.

[25] Many examples in this paragraph are taken from the relevant government submissions.

to freedom of opinion and expression enjoyed by targeted persons or the general population.

Bans on encryption for individual use

40. Outright prohibitions on the individual use of encryption technology disproportionately restrict the freedom of expression, because they deprive all online users in a particular jurisdiction of the right to carve out private space for opinion and expression, without any particular claim of the use of encryption for unlawful ends.

41. State regulation of encryption may be tantamount to a ban, such as rules (a) requiring licences for encryption use; (b) setting weak technical standards for encryption; and (c) controlling the import and export of encryption tools. By limiting encryption tools to government-approved standards and controlling the import or export of encryption technologies, States ensure encryption software maintains weaknesses that allow Governments to access the content of communications. For example, while the law may be in flux, India has provided that service providers may not deploy "bulk encryption" on their networks, while the law has also restricted individuals from using encryption greater than an easily breakable 40-bit key length without prior permission and required anyone using stronger encryption to provide the Government with a copy of the encryption keys.[26] Reports indicate that encryption products in China may be required to adhere to government-approved encryption algorithms that have not been peer-reviewed for security.[27] The Pakistan Telecommunication Authority requires prior approval for the use of VPNs and encryption.[28] Cuba requires regulatory authorization for those using encryption.[29] In Ethiopia, the Government has the power to set the technical standards of encryption and recently enacted regulation that criminalizes the manufacture, assembly or import of any telecommunications equipment without a permit.[30] Such regulations impermissibly interfere with the individual use of encryption in communications.

Intentional weakening of encryption

42. Some States have implemented or proposed implementing so-called back-door access in commercially available products, forcing developers to install weaknesses that allow government authorities access to encrypted communications. Some Governments have developed or purchased tools to allow such access for domestic surveillance purposes.[31] Senior officials in the United Kingdom and the United States appear to advocate requiring back-door access.[32] States supporting such measures often claim that a legal framework for back-door access is necessary to intercept the content of encrypted communications. Governments proposing back-door access, however, have not

[26] Government of India, Ministry of Communications and IT, Licence Agreement for Provision of Internet Services, (2007). Available from http://dot.gov.in/sites/default/files/internet-licence-dated%2016-10-2007_0.pdf. See especially sect. 2.2 (vii).

[27] See, e.g., Counter-terrorism Law, art. 15 (initial draft of 8 November 2014). Available from http://chinalawtranslate.com/en/ctldraft/.

[28] See www.ispak.pk/Downloads/PTA_VPN_Policy.pdf.

[29] Submission of Cuba.

[30] See Ethiopia Telecom Fraud Offence Proclamation 761/2012, sects. 3–10.

[31] See Morgan Maquis-Boire and others, *For Your Eyes Only* (2013, Citizen Lab).

[32] See the speech given by Prime Minister David Cameron on 12 January 2015 at the Conservative Party pledges conference for the 2015 general election and the speech given by James Comey, Director of the Federal Bureau of Investigation, on 16 October 2014, entitled "Going dark: are technology, privacy and public safety on a collision course?", at the Brookings Institution, Washington, D.C.

demonstrated that criminal or terrorist use of encryption serves as an insuperable barrier to law enforcement objectives. Moreover, based on existing technology, intentional flaws invariably undermine the security of all users online, since a backdoor, even if intended solely for government access, can be accessed by unauthorized entities, including other States or non-State actors. Given its widespread and indiscriminate impact, back-door access would affect, disproportionately, all online users.

43. The debate on this issue highlights a critical point: requiring encryption back-door access, even if for legitimate purposes, threatens the privacy necessary to the unencumbered exercise of the right to freedom of expression. Back-door access has practical limitations; the exploitation of intentional weaknesses could render encrypted content susceptible to attack, even if access is provided with the sole intention of allowing government or judicial control. Governments certainly face a dilemma when their obligation to protect freedom of expression is in conflict with their obligations to prevent violations of the right to life or bodily integrity, which are put at risk by terrorism and other criminal behaviour. But other recourses are available to States to request the disclosure of encrypted information, such as through judicial warrants. In such situations, States must demonstrate that general limitations on the security provided by encryption would be necessary and proportionate. States must show, publicly and transparently, that other less intrusive means are unavailable or have failed and that only broadly intrusive measures, such as backdoors, would achieve the legitimate aim. Regardless, measures that impose generally applicable restrictions on massive numbers of persons, without a case-by-case assessment, would almost certainly fail to satisfy proportionality.

Key escrows

44. A key escrow system permits individual access to encryption but requires users to store their private keys with the Government or a "trusted third party". Key escrows, however, have substantial vulnerabilities. For instance, the key escrow system depends on the integrity of the person, department or system charged with safeguarding the private keys, and the key database itself could be vulnerable to attack, undermining any user's communication security and privacy. Key escrow systems, rejected (along with back-door access) after significant debate in the United States in the so-called Crypto Wars of the 1990s, are currently in place in several countries and have been proposed in others. In 2011, Turkey passed regulations requiring encryption suppliers to provide copies of encryption keys to government regulators before offering their encryption tools to users.[33] The vulnerabilities inherent in key escrows render them a serious threat to the security to exercise the freedom of expression.

Mandatory key disclosure versus targeted decryption orders

45. In a situation where law enforcement or national security arguments may justify requests for access to communications, authorities may see two options: order either decryption of particular communications or, because of a lack of confidence that a targeted party would comply with a decryption order, disclosure of the key necessary for decryption. Targeted decryption orders may be seen as more limited and less likely to raise proportionality concerns than key disclosure, focusing on specific communications rather than an individual's entire set of communications encrypted by a particular key. Key disclosure, by contrast, could expose private data well beyond what is required by the exigencies of a situation.[34] Moreover, key disclosure or decryption orders often force

[33] Law No. 5651 on Regulating Broadcasting in the Internet and Fighting against Crimes Committed through Internet Broadcasting.

[34] The European Commission Counter-Terrorism Coordinator has urged consideration of mandatory key

corporations to cooperate with Governments, creating serious challenges that implicate individual users online. Key disclosure exists by law in a number of European countries.[35] In both cases, however, such orders should be based on publicly accessible law, clearly limited in scope focused on a specific target, implemented under independent and impartial judicial authority, in particular to preserve the due process rights of targets, and only adopted when necessary and when less intrusive means of investigation are not available. Such measures may only be justified if used in targeting a specific user or users, subject to judicial oversight.

Legal presumptions

46. Some States may identify the mere use of encryption technologies as illicit behaviour. For instance, charges against the Zone 9 blogger collective in Ethiopia included suggestions that the mere training in communication security was evidence of criminal behaviour.[36] Such presumptions fail to meet the standards for permissible restrictions. Similarly, States undermine the rights to privacy and freedom of expression when they penalize those who produce and distribute tools to facilitate online access for activists.

2. Anonymity

47. Anonymity has been recognized for the important role it plays in safeguarding and advancing privacy, free expression, political accountability, public participation and debate.[37] The Universal Declaration and the International Covenant on Civil and Political Rights do not address anonymity. During negotiation of the Covenant, it was proposed to include in article 19 (1) the phrase, "anonymity is not permitted". However, this was rejected "on the grounds, among others, that anonymity might at times be necessary to protect the author" and "that such a clause might prevent the use of pen names".[38] The Special Rapporteur on Freedom of Expression of the Inter-American Commission on Human Rights found that "the right to freedom of thought and expression and the right to private life protect anonymous speech from government restrictions".[39] Several States enjoy long traditions of celebrating anonymity in their political cultures, but very few provide general protection in law for anonymous expression. Some States exert significant pressure against anonymity, offline and online. Yet because anonymity facilitates opinion and expression in significant ways online, States should protect it and generally not restrict the technologies that provide it. Several States' judiciaries have protected anonymity, at least in limited instances. For instance, the Supreme Court of Canada recently struck down the warrantless acquisition of anonymous user identity online.[40] The Constitutional Court of the Republic of Korea struck down anti-anonymity laws as unconstitutional.[41] The Supreme

disclosure. See Council of the European Union, General Secretariat, meeting document D1035/15 (2015).

[35] See, e.g., United Kingdom, Regulation of Investigatory Powers Act (mandatory key disclosure); France, Law No. 2001-1062 (disclosure of encryption keys on authorization by a judge); Spain, Law on Telecommunications 25/2007 (key disclosure).

[36] See http://trialtrackerblog.org/2014/07/19/contextual-translation-of-the-charges-of-the-zone9-bloggers/.

[37] See, e.g., Inter-American Commission on Human Rights, OEA /Serv.L/V/II.149, para. 134; United States, *McIntyre* v. *Ohio Elections Commission* (1995); Lord Neuberger, speech to RB Conference on the Internet, entitled, "What's a name? Privacy and Anonymous Speech on the Internet" (2014).

[38] Marc J. Bossuyt, *Guide to the "Travaux Préparatoires" of the International Covenant on Civil and Political Rights* (1987), pp. 379-80.

[39] See Organization of American States, press release 17/15.

[40] *R.* v. *Spencer* (2014).

[41] Decision 2010 Hun-Ma 47, 252 (consolidated) announced 28 August 2012.

Court of the United States has consistently protected the right to anonymous expression.[42] The European Court of Human Rights has recognized anonymity as important to the freedom of expression but permits limitations in cases where necessary to achieve legitimate objectives.

48. Many States recognize the lawfulness of maintaining the anonymity of journalists' sources. The Mexican Supreme Court and Mexican Code of Criminal Procedures recognize the right of journalists to maintain the anonymity of their sources; yet pressures on journalists are in fact severe.[43] The Constitutions of Argentina, Brazil, Ecuador and Paraguay explicitly protect sources; Chile, El Salvador, Panama, Peru, Uruguay and Venezuela (Bolivarian Republic of) protect sources in law.[44] The Mozambique Constitution protects sources, while Angola purports to do so by statute.[45] Australia, Canada, Japan and New Zealand have established case-specific judicial balancing tests to analyse source protection, although pressure on journalists may undermine such protections over time.[46] States often breach source anonymity in practice, even where it is provided for in law.

Prohibition of anonymity

49. Prohibition of anonymity online interferes with the right to freedom of expression. Many States ban it regardless of any specific government interest. The Constitution of Brazil (art. 5) prohibits anonymous speech. The Constitution of the Bolivarian Republic of Venezuela (art. 57) similarly prohibits anonymity. In 2013, Viet Nam outlawed the use of pseudonyms, which forced individuals with personal blogs to publicly list their real name and address.[47] In 2012, the Islamic Republic of Iran required the registration of all IP addresses in use inside the country and cybercafe users to register their real names before using a computer.[48] Ecuadoran law requires commenters on websites and mobile phone owners to register under a real name.[49]

50. Certain States have passed laws that require real-name registration for online activity, a kind of ban on anonymity. In the Russian Federation, bloggers with 3,000 or more daily readers must register with the media regulator and identify themselves publicly, and cybercafe users reportedly must provide identification to connect to public wireless facilities.[50] China reportedly announced regulations requiring Internet users to register real

[42] *McIntyre* v. *Ohio Elections Commission* (1995), pp. 342 and 343.

[43] See new Federal Code of Criminal Procedures, art. 244.

[44] See Argentina, Constitution, art. 43; Brazil, Constitution, title II, chap. I, art. 5, XIV; Ecuador, Constitution, art. 20; Paraguay, Constitution, art. 29 (1). See also Chile, Law 19,733; El Salvador, Criminal Procedure Code; Panama, Law 67, art. 21; Peru, Criminal Procedure Code; Uruguay, Law 16.099; Bolivarian Republic of Venezuela, Law for Journalism 4.819, art. 8.

[45] See Mozambique, Constitution, art. 48(3); Angola, Press Law 7/06, art. 20(1).

[46] Australia Evidence Amendment (Journalists' Privilege) Act 2007; Canada, Court of Queen's Bench of Alberta, *Wasylyshen* v. *Canadian Broadcasting Corporation* (2005); Japan, Case 2006 (Kyo) No. 19 (2006); New Zealand Evidence Act, sect. 68 (2006).

[47] Human Rights Watch, "Vietnam: new decree punishes press", 23 February, 2011; Freedom House, "Vietnam: freedom of the press", 2012; Article 19, Comment on Decree No. 02 of 2011 on Administrative Responsibility for Press and Publication Activities of the Prime Minister of the Socialist Republic of Vietnam (June 2011).

[48] Islamic Republic of Iran, Bill 106, Communication Regulation Authority.

[49] See Ecuador, Organic Law on Communications (2013).

[50] Bill No. 428884-6 amending the Federal Law on Information, Information Technologies and Protection of Information and a number of legislative acts of the Russian Federation on streamlining the exchange of information with the use of information and telecommunication networks; Reuters, "Russia Demands Internet Users Show ID to Access Public Wifi," 8 August 2014.

names for certain websites and avoid spreading content that challenges national interests.[51] South Africa also requires real name registration for online and mobile telephone users.[52]

51. Likewise, Governments often require SIM card registration; for instance, nearly 50 countries in Africa require or are in the process of requiring the registration of personally identifiable data when activating a SIM card.[53] Colombia has had a mandatory mobile registration policy since 2011, and Peru has associated all SIM cards with a national identification number since 2010.[54] Other countries are considering such policies. Such policies directly undermine anonymity, particularly for those who access the Internet only through mobile technology. Compulsory SIM card registration may provide Governments with the capacity to monitor individuals and journalists well beyond any legitimate government interest.

52. States have also attempted to combat anonymity tools, such as Tor, proxies and VPNs, by denying access to them. China has long blocked access to Tor,[55] and Russian government officials reportedly offered more than $100,000 for techniques to identify anonymous users of Tor.[56] In addition, Ethiopia,[57] Iran (Islamic Republic of)[58] and Kazakhstan[59] have reportedly sought to block Tor traffic. Because such tools may be the only mechanisms for individuals to exercise freedom of opinion and expression securely, access to them should be protected and promoted.

Restrictions during public unrest

53. Anonymous speech has been necessary for activists and protestors, but States have regularly attempted to ban or intercept anonymous communications in times of protest. Such attempts to interfere with the freedom of expression unlawfully pursue an illegitimate objective of undermining the right to peaceful protest under the Universal Declaration and the International Covenant on Civil and Political Rights.

Intermediary liability

54. Some States and regional courts have moved towards imposing responsibilities on Internet service providers and media platforms to regulate online comments by anonymous users. Ecuador, for instance, in its Organic Communications Law, requires intermediaries to generate mechanisms to record personal data to allow the identification of those posting comments. In *Delfi* v. *Estonia* (application No. 64569/09), the European Court of Human Rights upheld an Estonian law that imposes liability on a media platform for anonymous defamatory statements posted on its site. Such intermediary liability is likely to result either in real-name registration policies, thereby undermining anonymity, or the elimination of posting altogether by those websites that cannot afford to implement screening procedures,

[51] China Copyright and Media, Internet User Account Name Management Regulations, article 5 (2015).

[52] South Africa, Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2003; see also Electronic Communications and Transactions Act of 2002 (requiring real name registration for service providers).

[53] Kevin P. Donovan and Aaron K. Martin, "The Rise of African SIM Registration", 3 February 2014.

[54] See Colombia, Decree 1630 of 2011; Perú 21, *Los celulares de prepago en la mira*, 27 May 2010.

[55] MIT Technology Review, *How China Blocks the Tor Anonymity Network*, 4 April 2012.

[56] The original offer is available from http://zakupki.gov.ru/epz/order/notice/zkk44/view/common-info.html?regNumber=0373100088714000008.

[57] Runa Sandvik, Ethiopia Introduces Deep Packet Inspection, The Tor Blog (31 May 2012); see also Article 19, 12 January 2015.

[58] "Phobos", "Iran partially blocks encrypted network traffic", The Tor Blog (10 February 2012).

[59] "Phobos", "Kazakhstan upgrades censorship to deep packet inspection", The Tor Blog (16 February 2012).

thus harming smaller, independent media. The recently adopted Manila Principles on Intermediary Liability, drafted by a coalition of civil society organizations, provide a sound set of guidelines for States and international and regional mechanisms to protect expression online.

Data retention

55. Broad mandatory data retention policies limit an individual's ability to remain anonymous. A State's ability to require Internet service and telecommunications providers to collect and store records documenting the online activities of all users has inevitably resulted in the State having everyone's digital footprint. A State's ability to collect and retain personal records expands its capacity to conduct surveillance and increases the potential for theft and disclosure of individual information.

V. Conclusions and recommendations

56. **Encryption and anonymity, and the security concepts behind them, provide the privacy and security necessary for the exercise of the right to freedom of opinion and expression in the digital age. Such security may be essential for the exercise of other rights, including economic rights, privacy, due process, freedom of peaceful assembly and association, and the right to life and bodily integrity. Because of their importance to the rights to freedom of opinion and expression, restrictions on encryption and anonymity must be strictly limited according to principles of legality, necessity, proportionality and legitimacy in objective. The Special Rapporteur therefore recommends the following.**

A. States

57. **States should revise or establish, as appropriate, national laws and regulations to promote and protect the rights to privacy and freedom of opinion and expression. With respect to encryption and anonymity, States should adopt policies of non-restriction or comprehensive protection, only adopt restrictions on a case-specific basis and that meet the requirements of legality, necessity, proportionality and legitimacy in objective, require court orders for any specific limitation, and promote security and privacy online through public education.**

58. **Discussions of encryption and anonymity have all too often focused only on their potential use for criminal purposes in times of terrorism. But emergency situations do not relieve States of the obligation to ensure respect for international human rights law. Legislative proposals for the revision or adoption of restrictions on individual security online should be subject to public debate and adopted according to regular, public, informed and transparent legislative process. States must promote effective participation of a wide variety of civil society actors and minority groups in such debate and processes and avoid adopting such legislation under accelerated legislative procedures. General debate should highlight the protection that encryption and anonymity provide, especially to the groups most at risk of unlawful interferences. Any such debate must also take into account that restrictions are subject to strict tests: if they interfere with the right to hold opinions, restrictions must not be adopted. Restrictions on privacy that limit freedom of expression — for purposes of the present report, restrictions on encryption and anonymity — must be provided by law and be necessary and proportionate to achieve one of a small number of legitimate objectives.**

59. **States should promote strong encryption and anonymity. National laws should recognize that individuals are free to protect the privacy of their digital communications by using encryption technology and tools that allow anonymity online. Legislation and regulations protecting human rights defenders and journalists should also include provisions enabling access and providing support to use the technologies to secure their communications.**

60. **States should not restrict encryption and anonymity, which facilitate and often enable the rights to freedom of opinion and expression. Blanket prohibitions fail to be necessary and proportionate. States should avoid all measures that weaken the security that individuals may enjoy online, such as backdoors, weak encryption standards and key escrows. In addition, States should refrain from making the identification of users a condition for access to digital communications and online services and requiring SIM card registration for mobile users. Corporate actors should likewise consider their own policies that restrict encryption and anonymity (including through the use of pseudonyms). Court-ordered decryption, subject to domestic and international law, may only be permissible when it results from transparent and publicly accessible laws applied solely on a targeted, case-by-case basis to individuals (i.e., not to a mass of people) and subject to judicial warrant and the protection of due process rights of individuals.**

B. International organizations, private sector and civil society

61. **States, international organizations, corporations and civil society groups should promote online security. Given the relevance of new communication technologies in the promotion of human rights and development, all those involved should systematically promote access to encryption and anonymity without discrimination. The Special Rapporteur urgently calls upon entities of the United Nations system, especially those involved in human rights and humanitarian protection, to support the use of communication security tools in order to ensure that those who interact with them may do so securely. United Nations entities must revise their communication practices and tools and invest resources in enhancing security and confidentiality for the multiple stakeholders interacting with the Organization through digital communications. Particular attention must be paid by human rights protection mechanisms when requesting and managing information received from civil society and witnesses and victims of human rights violations.**

62. **While the present report does not draw conclusions about corporate responsibilities for communication security, it is nonetheless clear that, given the threats to freedom of expression online, corporate actors should review the adequacy of their practices with regard to human right norms. At a minimum, companies should adhere to principles such as those laid out in the Guiding Principles on Business and Human Rights, the Global Network Initiative's Principles on Freedom of Expression and Privacy, the European Commission's ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights, and the Telecommunications Industry Dialogue Guiding Principles. Companies, like States, should refrain from blocking or limiting the transmission of encrypted communications and permit anonymous communication. Attention should be given to efforts to expand the availability of encrypted data-centre links, support secure technologies for websites and develop widespread default end-to-end encryption. Corporate actors that supply technology to undermine encryption and anonymity should be especially transparent as to their products and customers.**

63. **The use of encryption and anonymity tools and better digital literacy should be encouraged. The Special Rapporteur, recognizing that the value of encryption and anonymity tools depends on their widespread adoption, encourages States, civil society organizations and corporations to engage in a campaign to bring encryption by design and default to users around the world and, where necessary, to ensure that users at risk be provided the tools to exercise their right to freedom of opinion and expression securely.**

Exhibit N

Former Federal Agents Charged with Bitcoin Money Laundering and Wire Fraud

Agents were Part of Baltimore's Silk Road Task Force

U.S. Department of Justice
March 30, 2015

Office of Public Affairs
(202) 514-2007/TDD (202) 514-1888

Two former federal agents have been charged with wire fraud, money laundering and related offenses for stealing digital currency during their investigation of the Silk Road, an underground black market that allowed users to conduct illegal transactions over the Internet. The charges are contained in a federal criminal complaint issued on March 25, 2015, in the Northern District of California and unsealed today.

Assistant Attorney General Leslie R. Caldwell of the Justice Department's Criminal Division, U.S. Attorney Melinda Haag of the Northern District of California, Special Agent in Charge David J. Johnson of the FBI's San Francisco Division, Special Agent in Charge José M. Martinez of the Internal Revenue Service-Criminal Investigation's (IRS-CI) San Francisco Division, Special Agent in Charge Michael P. Tompkins of the Justice Department's Office of the Inspector General Washington Field Office and Special Agent in Charge Lori Hazenstab of the Department of Homeland Security's Office of the Inspector General in Washington D.C. made the announcement.

Carl M. Force, 46, of Baltimore, was a Special Agent with the Drug Enforcement Administration (DEA), and Shaun W. Bridges, 32, of Laurel, Maryland, was a Special Agent with the U.S. Secret Service (USSS). Both were assigned to the Baltimore Silk Road Task Force, which investigated illegal activity in the Silk Road marketplace. Force served as an undercover agent and was tasked with establishing communications with a target of the investigation, Ross Ulbricht, aka "Dread Pirate Roberts." Force is charged with wire fraud, theft of government property, money laundering and conflict of interest. Bridges is charged with wire fraud and money laundering.

According to the complaint, Force was a DEA agent assigned to investigate the Silk Road marketplace. During the investigation, Force engaged in certain authorized undercover operations by, among other things, communicating online with "Dread Pirate Roberts" (Ulbricht), the target of his investigation. The complaint alleges, however, that Force then, without authority, developed additional online personas and engaged in a broad range of illegal activities calculated to bring him personal financial gain. In doing so, the complaint alleges, Force used fake online personas, and engaged in complex Bitcoin transactions to steal from the government and the targets of the investigation. Specifically, Force allegedly solicited and received digital currency as part of the investigation, but failed to report his receipt of the funds, and instead transferred the currency to his personal account. In one such transaction, Force allegedly sold information about the government's investigation to the target of the investigation. The complaint also alleges that Force invested in and worked for a digital currency exchange company while still working for the DEA, and that he directed the company to freeze a customer's account with no legal basis to do so, then transferred the customer's funds to his personal account. Further, Force allegedly sent an unauthorized Justice Department subpoena to an online payment service directing that it unfreeze his personal account.

Bridges allegedly diverted to his personal account over $800,000 in digital currency that he gained control of during the Silk Road investigation. The complaint alleges that Bridges placed the assets into an account at Mt. Gox, the now-defunct digital currency exchange in Japan. He then allegedly wired funds into one of his personal investment accounts in the United States mere days before he sought a $2.1 million seizure warrant for Mt. Gox's accounts.

Bridges self-surrendered today and will appear before Magistrate Judge Maria-Elena James of the Northern District of California at 9:30 a.m. PST this morning. Force was arrested on Friday, March 27, 2015, in Baltimore and will appear before Magistrate Judge Timothy J. Sullivan of the District of Maryland at 2:30 p.m. EST today.

The charges contained in the complaint are merely accusations, and the defendants are presumed innocent unless and until proven guilty.

The case was investigated by the FBI's San Francisco Division, the IRS-CI's San Francisco Division, the Department of Justice Office of the Inspector General and the Department of Homeland Security Office of the Inspector General in Washington D.C. The Treasury Department's Financial Crimes Enforcement Network also provided assistance with the investigation of this case. The case is being prosecuted by Assistant U.S. Attorneys Kathryn Haun and William Frentzen of the Northern District of California and Trial Attorney Richard B. Evans of the Criminal Division's Public Integrity Section.

San Francisco Division Links

San Francisco Home

Contact Us
- Overview
- Territory/Jurisdiction

News and Outreach
- Press Room | Stories
- In Your Community

About Us
- Our People & Capabilities
- What We Investigate
- Our Partnerships
- San Francisco History

Wanted by the FBI - San Francisco

FBI Jobs

Close

Exhibit O

Suds for Drugs

Tide detergent: Works on tough stains. Can now also be traded for crack. A case study in American ingenuity, legal and otherwise.

By Ben Paynter Published Jan 6, 2013 Share 58 Comments

(Photo: Victor Prado/New York Magazine. Typography by Kevin Dresser.)

The call that came in from a local Safeway one day in March 2011 was unlike any the Organized Retail Crime Unit of the Prince George's County Police Department had fielded before. The grocery store, located in suburban Bowie, Maryland, had been robbed repeatedly. But in every incident the only products taken were bottles—many, many bottles—of the liquid laundry detergent Tide. "They were losing $10,000 to $15,000 a month, with people just taking it off the shelves," recalls Sergeant Aubrey Thompson, who heads the team. When Thompson and his officers arrived to investigate, they stumbled onto another apparent Tide theft in progress and busted two men who'd piled 100 or so of the bright-orange jugs into their Honda. The next day, Thompson returned to the store's parking lot to tape a television interview about the crimes. A different robber took advantage of the distraction to make off with twenty more bottles.

Later, Thompson reviewed weeks' worth of the Safeway's security footage. He found that more than two dozen thieves, working in crews, were regularly raiding the store's household-products aisle, sometimes returning more than once the same day and avoiding detection by timing their heists to follow clerks' shift changes. Owners and managers of other area stores, having seen Thompson on the news, reached out to him to report their own vanishing Tide bottles. Since then, the oddly brand-loyal crime wave has gone national, striking bodegas, supermarkets, and big-box discounters from Austin to West St. Paul, Minnesota. In New York, employees at the Penn Station Duane Reade nabbed a man trying to abscond with Tide bottles he'd stuffed into a suitcase. In Orange County, an attempted Tide theft led to a high-speed chase that included the thief crashing his SUV into an ambulance. Last year, for the first time, detergent made the National Retail Federation's list of most-targeted items. Says Joseph LaRocca, founder of the trade group RetailPartners, who helped compile the report: "Tide was specifically called out."

As the cases piled up after his team's first Tide-theft bust, Thompson sought an answer to the riddle at the center of the crimes: What did thieves want with so much laundry soap? To find out, he and his unit pored over security recordings to identify prolific perpetrators, whom officers then tracked down and detained for questioning. "We never promised to go easy on them, but they were willing to talk about it," Thompson says. "I guess they were bragging." It turned out the detergent wasn't being used as an ingredient in some new recipe for getting high, but instead to buy drugs themselves. Tide bottles have become ad hoc street currency, with a 150-ounce bottle going for either $5 cash or $10 worth of weed or crack cocaine. On certain corners, the detergent has earned a new nickname: "Liquid gold." The Tide people would never sanction that tag line, of course. But this unlikely black market would not have formed if they weren't so good at pushing their product.

Shoppers have surprisingly strong feelings about laundry detergent. In a 2009 survey, Tide ranked in the top three brand names that consumers at all income levels were least likely to give up regardless of the recession, alongside Kraft and Coca-Cola. That loyalty has enabled its manufacturer, Procter & Gamble, to position the product in a way that defies economic trends. At upwards of $20 per 150-ounce bottle, Tide costs about 50 percent more than the average liquid detergent yet outsells Gain, the closest competitor by market share (and another P&G product), by more than two to one. According to research firm SymphonyIRI Group, Tide is now a $1.7 billion business representing more than 30 percent of the liquid-detergent market.

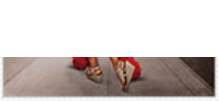
Before the advent of liquid detergent, the average American by one estimate owned fewer than ten

MOST POPULAR STORIES

Most Viewed Most Emailed

LAST 24 HOURS

1. Exclusive: Civil Suit to Be Filed Against Robert Durst by His Long-Missing Wife's Family
2. NYPD Doesn't Want to Talk About Its X-ray Vans
3. Why Are Republicans Suddenly Fixated With Urban Failure?
4. How Late Can Joe Biden Enter the 2016 Campaign?
5. Winter Is Coming, and So Is El Niño
6. Joe Biden Cryptically Lays Out Campaign Platform, Like a Guy Who's Decided to Run for President
7. Lamar Odom Has Reportedly Suffered Brain Damage After Passing Out in Nevada Brothel
8. Hillary Hints That Julian Castro Could Be Her VP Pick
9. Silicon Valley's Most Inspiring Company May Be a Fraud
10. Daniel Murphy, Jacob deGrom Carry the Mets Into the NLCS



outfits, wearing items multiple times (to keep them from getting threadbare too fast) before scrubbing them by hand using bars of soap or ground-up flakes. To come up with a less laborious way to do the laundry, executives at Procter & Gamble began tinkering with compounds called surfactants that penetrate dirt and unbond it from a garment while keeping a spot on a shirt elbow from resettling on the leg of a pant. When the company released Tide in 1946, it was greeted as revolutionary. "It took something that had been an age-old drudgery job and transformed it into something that was way easier and got better results," says Davis Dyer, co-author of *Rising Tide*, which charts the origins of the brand. "It was cool, kind of like the iPod of the day." Procter & Gamble, naturally, patented its formula, forcing competitors to develop their own surfactants. It took years for other companies to come up with effective alternatives.

While clothes were getting easier to clean, Americans were starting to own more of them. Today, journalist Elizabeth Cline reports in *Overdressed: The Shockingly High Cost of Cheap Fashion*, the average U.S. consumer buys 68 pieces of clothing a year—more than one purchase a week—much of it cheaply made. Launder those items with Tide, and they take on a uniform smell and feel that consumers have come to associate with quality. "It doesn't matter where the clothes come from, if you wash them with Tide, they do have almost this prestige wash to them," says Maru Kopelowicz, a global creative director at Saatchi & Saatchi, which researches consumer attitudes toward Tide as the brand's lead advertising firm.

Procter & Gamble spends heavily on research and development to continually refine the sensory by-products of doing the laundry with its leading detergent. Tide's original scent was "citruslike," in the words of Sundar Raman, the marketing director of Procter & Gamble's North American fabric-care division, but has evolved into a "citrus, floral, and fruity experience" with hints of lemon, orange, roses, lily, and apple. When combined in a complex perfume, these notes help cover up the odors of the cleaning agents that would otherwise waft out during the wash cycle. But P&G also chose each scent to do a specific job. The smell of citrus, for instance, has been shown to correlate strongly with perceptions of cleanliness. "That natural, fresh-and-clean smell is stimulating and creates an instantaneous mood of being happy," says Craig Warren, a former researcher for the firm International Flavors & Fragrances who, until the late nineties, did work with P&G. Floral scents, for their part, have been known to evoke strong feelings of maternal love and kinship. (Home visits by Saatchi researchers have found that very ardent Tide fans sometimes carry bottles as if cradling a baby.) The goal of all these efforts is to turn clothes-washing into more than a to-do; it's being a good parent, a good person. It's a message that may also explain why among some lower-income shoppers, according a 2012 newsletter by branding agency Daymon Worldwide, "being able to afford Tide laundry detergent is seen as a sign of success."

Once people pick a brand, their reasons for sticking with it are largely automatic. Read Montague is the director of the human-neuroimaging laboratory and computational-psychiatry unit at Virginia Tech's Carilion Research Institute, where he studies how people choose and value products using an fMRI machine. When shoppers are exposed to a brand they identify with, their ventral medial prefrontal cortex lights up—the same part of the brain associated with reward recognition in drug users. That neural pathway may have helped our ancestors remember, say, which plants were safe to eat or when a tribal marking meant a clan was worth avoiding. In the modern age, we use the same circuitry as a shortcut for more mundane decisions. "As long as it keeps paying you back the same way," Montague says, you buy the same brands. The feedback loop flashes: "It's worth the money."

The criminal cost-benefit analysis of a bottle of Tide is more straightforward. Most of the people stealing the detergent, Sergeant Thompson points out, are the same criminals who used to break into houses or mug pedestrians—male addicts whose need to feed their habits can foster a kind of innovative streak. "They are smart. They are creative. They want high reward and low risk," he says. Theft convictions can come with a maximum fifteen-year prison sentence, but the penalty for shoplifting is often just a small fine, with no jail time. For the most active thieves, says Thompson, stolen Tide has in some ways become more lucrative than the drugs it's traded for. "It's the new dope," he says. "You can get richer and have less chance of doing jail time."

For stores, stopping Tide shoplifting presents unique challenges. Most frequently stolen goods—GPS devices, smartphones, and other consumer electronics—are pricey, light, and easily concealed. They're also not routine purchases, which means they can be locked up until buyers ask for them. Bulk goods like detergent are harder to run off with, but they're also bought by dozens of customers daily—lock those products up, and a store manager adds more time to his customers' errand runs, potentially sending them to shop elsewhere. "Any time you secure something, it impacts the sale of that item at some level," says Jerry Biggs, the director of Walgreens' Organized Retail Crime Division.

Nor is relying on clerks to head off suspected thieves a realistic option. Cashiers and stockists, working for low pay, are often disinclined to confront a potential criminal. "People at the cash register don't stop you," says one of Thompson's informants, an ex-con who shoplifted for years. "They just let you go past." What's more, stolen bottles of Tide aren't easily traceable. Many merchants don't record the lot and batch numbers for most grocery-store products, because that takes precious man hours. And Procter & Gamble has not made its own database of that information publicly available. Some stores have tried attaching tracking stickers to bottles to

establish their provenance, only to find that thieves just wash them off.

In his investigation, Thompson realized that since the supply of Tide would be hard to curb, he had to figure out how to stem the illicit demand. Working from leads provided by inmates and parolees offering to share details about their own Tide dealings in exchange for a good word with their judge or parole officer, he and his fellow officers pieced together a loose network of middlemen—barbershops, nail salons, and drug houses that were taking in bottles to either sell on the side to their clients or at a deep discount to willing corner stores and pawn shops.

Despite its popularity, Tide is not a big moneymaker for stores. P&G's proprietary surfactants and enzymes are relatively expensive to produce, notes Bill Schmitz, a Deutsche Bank analyst, so Tide's wholesale cost is steep. Only so much of that can be passed on to customers. "It's so tight," says Schmitz of the profit margin. In general, a retailer clears just a few percentage points on a Tide purchase. A store that charges $19.99 for a 150-ounce bottle might claim $2 in profit. But if it buys stolen bottles for $5, that jumps to $15.

It's not just bodegas that hawk iffy product. Chain stores also wind up in resale schemes. Rather than stock large surpluses of popular items, those businesses often rely on so-called perpetual-inventory systems to electronically record sales data and relay it to manufacturers, which stagger deliveries accordingly. When a bottle of Tide is taken from a store without being rung up, a crucial step gets skipped, leading to shipment delays. And when that happens, some store managers place stopgap orders with local wholesalers who may be less than rigorous about where they obtain their products or from fencing rings that employ their own sales teams and maintain legitimate-looking websites. "Some stores might not recognize these goods as stolen, but others don't really care," says LaRocca. "There are [stores] who don't ask questions about where the goods originated. Plenty are just looking to fill their shelves."

To break that final link in the chain, Thompson and his unit needed to nail stores for buying and selling boosted product—and to prove they were moving enough of it to trigger sufficiently dissuasive penalties. Prosecutors have to base charges on the retail value of the stolen merchandise. In Maryland, if the total is less than $1,000, the crime is a misdemeanor. Above that threshold, it becomes a felony, and a perpetrator faces the possibility of years behind bars. After his team busted one area shop owner for taking in stolen Tide, the perpetrator struck a deal for a $250 fine and a form of probation—then turned around and raised the price his store charged for Tide by $3.

During a sting operation last June, Thompson tried a new tactic. On a muggy Friday, the sergeant, clad in a black tracksuit, pulled his unmarked cruiser into a run-down shopping center in Capitol Heights, a low-income neighborhood on the southwestern border of Prince George's County and Washington, D.C. The previous week, one of his tipsters called about seeing people lugging Tide into his target today, a salon called Star Nails.

Thompson watched as his team, two undercover cops in a Jeep Cherokee, pulled up to the shop, where a handful of people in ragged clothing were loitering under a faded red-and-white marquee. While the driver kept the car idling, a heavily tattooed, spiky-haired detective named Alexander Mallari jumped out holding a laundry bag filled with a few bottles of Tide and lots of bonus items—a dozen pairs of Philips earphones, a dozen or so bottles of Victoria's Secret perfume. Mallari's mission was simple: He'd enter the shop, disclose that the items were stolen, and try to unload them.

Ten minutes later, Mallari emerged with an empty bag and a small wad of money in his pocket. He was offered just $30—a pittance by the standards of the Tide trade. "That's a true crackhead price right there," Thompson said. Mallari could have haggled for more, but that's not the point, since it's the retail prices of the merchandise that will be making the police report, and the headphones and perfume helped to boost the total value into felony territory. "As long as they pay me, as long as they accept the stolen item, that's what matters," he said. A few weeks later, the team raided the salon and two houses and a pair of cars associated with Star Nails employees, arresting five workers and recovering roughly $20,000 in stolen property. While they had the salon under surveillance, Thompson's unit learned that the scope of Tide theft had broadened again. An officer overheard its employees talking about moving the Tide to stores "back home"—which in their case is Vietnam.

For its part, Procter & Gamble doesn't seem overly concerned about the black-market popularity of its product. "It's unfortunate that people are stealing Tide, and I don't think it's appropriate at all, but the one thing it reminds me of is that the value of the brand has stayed consistent," says Raman, the marketing director. Now the company's tactics for maintaining the brand's premium status are evolving. One recent commercial for the detergent shows a young couple watching TV. The boyfriend mentions that his girlfriend wanted him to use Tide with Downey to make his shirts soft. The punch line: She's fallen asleep on his stomach. "And was she right? The proof is in the snoring," he says. That promotion, part of a campaign called MyTide, is emblematic of the way Tide's target demographic has expanded since the brand's inception. Tide isn't just for stay-at-home moms anymore. It's for single guys—and, as other commercials show, for a woman who wants to resurrect her "nasty, vile" old tennis shoes, or the parents of triplets, folding clothes in a crowded bedroom, who consider their kids "such a blessing" but "not financially," or anyone looking to stretch their dollars. Says Kopelowicz of Saatchi & Saatchi: "Some people, just because they can't

afford Tide all the time, they might think the brand doesn't understand you. Of course we understand you."

Fashion trends might be ephemeral, but—if you buy into Tide's branding efforts—clean clothes, no matter what kind of clothes they are, are essential to your well-being, or even to your sense of self-worth. "It makes you feel prepared, like your priorities are straight," Kopelowicz says. It just happens that the high demand for Tide that message fuels also sustains criminal enterprises.

If all that makes Thompson's job harder, he doesn't blame Procter & Gamble. "I'm a No. 1 Tide fan," he says. "I don't know if it's all psychological, but you can tell the difference."

Exhibit P

BITLICENSE • BITSTAMP • COINBASE • COINSETTER • EXCHANGES • FEATURES

The Real Cost of Applying for a New York BitLicense

Yessi Bello Perez (@yessi_kbello) | Published on August 13, 2015 at 20:40 BST

FEATURE

In the aftermath of the BitLicense application deadline this week, a number of prominent bitcoin companies have ceased operations in New York.

Although the reasons behind startups' reluctance to apply for a license are varied, cost has played a significant part.

Of those who did apply – and fronted the $5,000 non-refundable application fee, most have alluded to an arduous process and high costs.

But just how much did their expenditure amount to?

CoinDesk has spoken to various companies in the space to breakdown the cost of the BitLicense application process both in monetary and non-monetary terms.

'Expensive and difficult'

"Applying for the BitLicense is an expensive and difficult process, as many have noted. Some other firms have chosen to abandon the New York market entirely, rather than comply. We do not fault them for doing so," said George Frost, executive VP and chief legal officer at Bitstamp.

Frost estimated the application cost Bitstamp roughly $100,000, including time allocation, legal and compliance fees.

"Our UK parent company has contributed a lot of time, expertise and money in the BitLicense effort, but much of this investment will benefit the entire Bitstamp group," said Frost.

Bitstamp, the world's third largest exchange in terms of BTC/USD trading volume, proceeded with the application for various reasons. Firstly, because, if approved, it would allow the company to offer a fully compliant trading platform for New York residents. Secondly, Frost said he expects to be able to offer a broader range of financial tools to customers – including Automatic Clearing House (ACH) deposits, domestic wire transfers and debit card transactions.

The application efforts, he added, included establishing a new operating subsidiary in the US, developing a business plan, establishing appropriate financial controls, hiring a US compliance officer – Lisa Dawson, former senior VP and compliance officer at Citi Group – and spending months "analysing and agonising over" the BitLicence's requirements and providing industry comments to the New York State Department of Financial Services (NYDFS).

He added:

> *"We drafted a detailed risk assessment of Bitstamp USA and the Bitstamp group overall, and more than 30 policies, training manuals and internal procedures guides that we believe are compliant with the New York regulatory regime ... These included hundreds and hundreds of pages of plans covering every aspect of our intended operations. All of this internal scrutiny and drafting has made us a lot smarter company, albeit one with corporate tunnel syndrome."*

FEATURES

Chainalysis: Barclays Deal is Start of Banks Opening Up to Bitcoin


Inside Multichain: A Build-Your-Own Blockchain Service for Banks


Blockchain Tech Reduces Corporations' Reliance on Humans

Meet Secco: The UK's 'Blockchain-Inspired' Challenger Bank

INDUSTRY PRESS RELEASES

Oct 15 | 14:45 **Crypti Foundation Announces Decentralized Application (Dapp) Hackathon Contest**

Oct 13 | 12:46 **Trading Platform OpenLedger Launches with BitShares 2.0 Release**

Oct 8 | 14:29 **Chroma.fund Conducts World's First "Blockchain IPO"**

Oct 8 | 14:04 **Crypti Foundation Open Sources Core Client and Announces Bug Bounty Program**

VIEW MORE SUBMIT RELEASE

Although a costly and cumbersome process, Frost said he believed greater regulation for the ecosystem is inevitable.

"Like others, we regret the loss of economic freedom occasioned by the onset of regulation. [But] by participating, we are better positioned to help create an industry – and regulatory environment – that achieves widespread adoption and preserves as much individual autonomy as possible."

Manning the effort

Unlike Bitstamp, which claims to employ up 50 people, bitcoin exchange MonetaGo is sizeably smaller.

Also unlike, Bitstamp, the New York-based company is a relative newcomer to the bitcoin scene, but by no means less eager to comply with the New York State's regulatory framework.

"Given that we are a new startup company we have been extremely diligent with our expenditures. In terms of hard costs we've spent approximately $50,000 ... by far the biggest costs have been the man-hours to date," said Patrick Manasse, chief compliance officer.

Manasse estimates that the team spent approximately 1,200 hours compiling the documentation for the BitLicense application, but noted that an additional 2,000 man hours had already been invested in developing MonetaGo's global compliance program.

Efforts were spent on providing compliance training to all of the officers and directors, working with lawyers and consultants in various regions and communicating with banks and other relevant authorities.

"Add to this programmers and developers putting in place systems and service providers, and you start to get a sense of the size and scope of the undertaking," he said, noting: "If all the hours were added up, the total would easily be upwards of a quarter million US dollars."

So, while putting the actual application together took MonetaGo's team members the better part of the past 45 days – the grace period following the publication of the BitLicense in New York's Register – the process, Manasse said, really began at the company's inception.

Manasse said the ongoing costs, should MonetaGo's submission be approved, are hard to estimate accurately. He believes they will depend on the approach taken by the NYDFS:

> *"The Department could easily make it completely unfeasible for startups to continue operating in the space, but that is not the sense that we have gotten from our interactions with them thus far. It is our hope that a measured approach will be taken."*

However, Manasse suggested that being a relatively new company could potentially work to MonetaGo's an advantage in terms of cost.

"A compliant company such as ours which is newly launched and has a limited operating history probably doesn't require the same amount of scrutiny as other players which have been around since the early days of bitcoin."

Significant undertaking

A spokesperson for Coinbase confirmed that the San Francisco-based company had submitted its BitLicense application.

Although they declined to divulge specific details, the spokesperson noted the process was a "significant undertaking", but one the company had no problem carrying out because it had sufficient internal resources.

Meanwhile, Jaron Lukasiewicz, CEO and founder of Coinsetter, noted his company had spent approximately $50,000 on BitLicense-related expenses over the past two years. "I think its bigger cost, though, has been in the uncertainty it created for investors looking to invest in our space – hopefully that will begin to reverse itself now."

Bittrex, a cryptocurrency exchange, also applied for the license. Bittrex founder Bill Shihara told CoinDesk he estimated the process to have cost his company between $18,000 and $20,000, whilst employees spent approximately 80 hours compiling and reviewing the paperwork.

"I am sure larger companies incurred much higher costs than we did ... we were lucky that we had a lot of the paperwork already available."

MUST READ MOST POPULAR


Bitcoin Firm Signs Compliance Deal With Banking Giant Barclays


Qiwi: Bitcoin Technology is 'Beyond' Russia's Proposed Ban


Blockstream to Launch First Sidechain for Bitcoin Exchanges


Ripple Sues Social App for $2 Million Over Trademark Infringement

Got a news tip or guest feature?

What is Bitcoin?
It's a decentralized digital currency

How Can I Buy Bitcoins?
From an exchange or an individual

Although he noted the BitLicense was a significant undertaking for companies, he said customers should welcome it:

> *"Ultimately, I think customers should be happy about the BitLicense. While it is burdensome for us, the core of the paperwork involved consumer protection. The BitLicense requires background checks on the principals who handle your funds; detailed information of how the funds are stored and credited to our users; proof that the company is profitable; as well as security and incident response plans."*

"If the BitLicense reviewers do their jobs right, passing the application process means the company holding your funds is a legitimate business that you should want to work with," he concluded.

Legal perspective

Marco Santori, counsel at Pillsbury Winthrop Shaw Pittman LLP, described the application process as "consultative and iterative".

"The NYDFS will not simply take your $5,000 and deny you without ceremony. They will certainly accept the application fee, but if the staff takes issues with some of the applicant's responses, or find deficiencies, they will address them with the applicant. Their objective is to bring businesses into the BitLicense regime, not to block them out of it," he added.

The NYDFS, Santori said, has 90 days to grant or deny a BitLicense application, but the Superintendent may extend that period for a reasonable amount of time sufficient to enable compliance with the BitLicense regime. "It is not clear whether that means compliance by NYDFS or the applicant. I expect that – certainly during the early stages – applications will take longer than 90 days to be approved."

If an application does not satisfy all the criteria, the authorities may decide to grant a conditional license, which will entail periodic review. "This is an amorphous thing. The are no criteria set forth in the regulation for what kind of company might qualify for a conditional license or what conditions might be attached for that license."

"Unilateral discretion in that regard," Santori added, "is left to the Superintendent. Those seeking a conditional license should submit their application along with a cover letter explaining why they believe one should be granted, and what conditions they believe should attach. It will likely take a bit of advocacy."

New York image via Shutterstock.

BitLicense Bitstamp Coinbase Marco Santori MonetaGo New York NYDFS

Exhibit Q

NEW YORK STATE DEPARTMENT OF FINANCIAL SERVICES

APPLICATION FORMS FOR:
LICENSE TO ENGAGE IN VIRTUAL CURRENCY BUSINESS ACTIVITY

2015.06.24 Version

APPLICATION FOR LICENSE TO ENGAGE IN VIRTUAL CURRENCY BUSINESS ACTIVITY

(Before filling out this form read the instructions carefully. All answers should be printed or typed. If additional space is required to complete any statement, prepare and annex a rider. Write "none" or "not applicable" where appropriate.)

_____, 20____

To the Superintendent of Financial Services of the State of New York:

The undersigned, desiring to engage in Virtual Currency Business Activity pursuant to the provisions of 23 NYCRR 200, does hereby make application for a license in accordance with 23 NYCRR §200.

1. The name and full address of the applicant is (include any trade name, under assumed name (UAN) or doing business as (DBA) name):

_____
_____
_____

2. Type of Application is: (Check type)

De Novo (new licensee) [ ] Other (specify) _____ [ ]

3. Form of Organization of Applicant is: (Check type of entity in which business will be conducted)

Individual (Sole Proprietor) [ ] Partnership [ ] Corporation [ ]
Limited Partnership [ ] Association [ ]
Limited Liability Company [ ] Other (specify) _____

4. Is the applicant also applying for a money transmission license with the Department at this time? If yes, the applicant must *also* submit an Application for a License to Engage in the Business of Issuing Travelers Checks, Money Orders, Prepaid/Stored Value Cards, and/or Transmitting Money (available at the Department's website). Additionally, note that information or documents recently submitted in connection with an application for a money transmitter license may be used to cross-satisfy information requested as part of this application. Please see section III of the application instructions for more information.

Yes [ ] No [ ]

5. Is the applicant currently licensed with the Department as a New York money transmitter?

Yes [ ] No [ ]

The documents and information attached hereto are hereby referred to and by this reference incorporated herein.

_____
(Authorized Signature)

_____ _____
(Name of Applicant) (Print Name and Title)

_____ _____ _____
(Telephone Number) (Fax Number) (E-Mail Address)

VERIFICATION

The undersigned swears or affirms that the information contained in this application, including the attached information and documents, is true and correct. FALSE WRITTEN STATEMENTS IN THIS APPLICATION ARE PUNISHABLE UNDER SECTION 210.45 OF THE NEW YORK PENAL LAW (making a punishable false written statement). Also, as per the New York Financial Services Law and regulations, the Superintendent of Financial Services may initiate regulatory actions against the licensee.

The undersigned further verifies that he/she is the named person below and that he/she is authorized to attest to and submit this application on behalf of the Applicant.

This application is executed at _____, New York (or insert name of other jurisdiction) _____on _____, 20_____.

_____
(Applicant Name)

_____
(Authorized Signature)

_____
(Print Name and Title)

INSTRUCTIONS

For License to Engage in Virtual Currency Business Activity

I. INTRODUCTION

The following instructions are for filing an application pursuant to the provisions of 23 NYCRR 200 for a license to engage in Virtual Currency Business Activity.

II. DEFINITIONS

As used in this document, the following definitions apply:

i. *Affiliate* means any Person that directly or indirectly controls, is controlled by, or is under common control with, another Person;

ii. *Person* means an individual, partnership, corporation, association, joint stock association, trust, or other entity, however organized;

iii. *Principal Officer* means an executive officer of an entity, including, but not limited to, the chief executive, financial, operating, and compliance officers, president, general counsel, managing partner, general partner, controlling partner, and trustee, as applicable;

iv. *Principal Stockholder* means any Person that directly or indirectly owns, controls, or holds with power to vote ten percent or more of any class of outstanding capital stock or other equity interest of an entity or possesses the power to direct or cause the direction of the management or policies of the entity; and

v. *Principal Beneficiary* means any Person entitled to ten percent or more of the benefits of a trust.

vi. *Virtual Currency Business Activity* means the conduct of any one of the following types of activities involving New York or a New York Resident:

1. receiving virtual currency for transmission or transmitting virtual currency, except where the transaction is undertaken for non-financial purposes and does not involve the transfer of more than a nominal amount of virtual currency;

2. storing, holding, or maintaining custody or control of virtual currency on behalf of others;

3. buying and selling virtual currency as a customer business;

4. performing exchange services as a customer business; or

5. controlling, administering, or issuing a virtual currency.

The development and dissemination of software in and of itself does not constitute Virtual Currency Business Activity.

III. GENERAL APPLICATION PROCEDURES

i. The license application shall be made, to the extent applicable, upon forms issued by the Superintendent of Financial Services of the State of New York. The application forms are available on the Department's website.

ii. All parts of the application, including documents submitted with the application, must be in the English language.

iii. The Application Form, Individual Questionnaires and other related forms shall be filled under oath or affirmation.

iv. A separate Application Form is required for each new (de novo) operation seeking to engage in activity under the provisions of 23 NYCRR 200.

v. All forms are to be printed or typed and fully completed. Type "none" or "not applicable" where appropriate. If additional space is required, prepare and annex a signed rider.

vi. Full names and addresses must be given, including zip codes and counties, where requested.

vii. To the extent that information or documents requested below have previously or concurrently been submitted to the Department in connection with an application for a money transmission license, the applicant may provide a cross-reference to the already submitted material in lieu of re-submitting the same information or material in response to the below requests. Cross-references must refer to the specific date and title of the referenced submission and, to the extent applicable, the specific portion of the prior or concurrent submission that addresses the requested information (*e.g.,* exhibit number or page number).

viii. The competed application shall be submitted together with any required fees to:

New York State Department of Financial Services
Virtual Currency Applications
One State Street
New York, NY 10004-1511

IV. *Application Processing*

Upon receipt, each application is reviewed by the Department to determine if it is substantially complete. Applicants/licensees submitting incomplete applications will receive written notification of the reason(s) their application was found incomplete and an itemized list of its deficiencies. In cases where the deficiencies are substantial, the entire application package, except for the application fee, will be returned to the applicant.

In addition to the application materials and information discussed below, the Superintendent may require additional information deemed necessary to adequately and efficiently assess the applicant within the intent of 23 NYCRR 200.

V. CONTENTS

In addition to a completed application form, the application must include the information and documents discussed below.

A. Information Regarding Corporate Matters

i. Provide the exact name of the applicant, including any doing business as name, the form of organization, the date of organization, and the jurisdiction where organized or incorporated. Attach a copy of applicant's Articles of Incorporation (or equivalent documentation if the applicant is not a corporation) as amended to the date of filing the application, certified by the applicable agency of the applicant's domiciliary jurisdiction. Attach a copy of the applicant's By-Laws, certified as current and accurate by the corporate secretary, or equivalent documentation if the applicant is not a corporation.

1. If the applicant is a corporation organized under New York Law, submit a copy of the Certificate of Incorporation certified by the Secretary of State of New York, or equivalent documentation if the applicant is not a corporation.

2. Foreign entities must submit a copy of their Application for Authority and Foreign Bid Certificate, certified by the Secretary of State of New York, as proof of their qualification to do business in this State.

ii. Provide the name, mailing address, telephone number and facsimile telephone number for: (a) the applicant's head office; (b) the office where applicant's books and records are kept; and (c) each subsidiary or affiliated company engaged in Virtual Currency Business Activity.

iii. Provide the name and title of: (a) the individual to whom all communications from the Department should be addressed; and (b) the individual to whom all consumer inquiries and complaints should be addressed.

iv. In the case of any Person who has made a commitment to extend credit to the applicant and such commitment is outstanding, identify such Person(s) and the terms of the commitment(s).

v. Provide a list of all of the applicant's Affiliates and an organization chart illustrating the relationship among the applicant and such Affiliates;

vi. Provide a verification from the New York State Department of Taxation and Finance that the applicant is compliant with all New York State tax obligations.

B. Fees

A non-refundable check, payable to the order of the Superintendent of Financial Services, for the $5,000 application fee must be sent with each new license application.

C. Information Regarding History and Business

i. A description of the proposed, current, and historical business of the applicant and all Affiliates, including detail on the products and services provided and to be provided, all associated website addresses, the jurisdictions in which the applicant and its Affiliates are engaged in business, the principal place of business, the primary market of operation, the projected customer base, any specific marketing targets, and the physical address of any operation in New York.

ii. If the applicant or its Affiliates have been or currently are engaged in Virtual Currency Business Activity without first obtaining a license to do so from the Superintendent, provide details as to: (a) the length of time engaged in such activity; (b) the amount and number of virtual currency transactions transmitted, exchanged, or held; and (c) the reason for not obtaining a license.

iii. Provide a list of the jurisdictions in which the applicant is licensed or otherwise authorized to engage in virtual currency-related activity, money transmission, or other financial services activity and the amount of any bond or deposit furnished in each such jurisdiction. In each case, please also specify the type of activity for which the applicant is licensed or otherwise authorized.

iv. List all jurisdictions, both domestic and foreign, in which the applicant or any Affiliate of the applicant has applied for a license or other authorization to engage in virtual currency-related activity, money transmission, or other financial services activity and has not been issued such license or authorization. State the reason(s) provided for why such license or authorization was not or has not yet been issued.

v. List all jurisdictions, both domestic and foreign, in which the license or other authorization of the applicant or its Affiliate to engage in virtual currency-related activity, money transmission, or other financial services was revoked, suspended, or refused renewal. State the reason(s) provided for why the revocation, suspension, or refusal occurred.

vi. Indicate whether the applicant or any Affiliate of the applicant has ever been the subject of a regulatory or enforcement action in any jurisdiction. If answered in the affirmative, describe the nature, and outcome, of all such regulatory or enforcement action(s).

vii. Provide, as applicable, a copy of any insurance policies maintained for the benefit of the applicant, its directors or officers, or its customers.

D. Information Regarding Directors, Principal Officers, Principal Stockholders and Principal Beneficiaries

i. Provide a list of, and detailed biographical information for, each individual applicant and each director, Principal Officer, Principal Stockholder, and Principal Beneficiary of the applicant, as applicable, including such individual's name, citizenship, title, social security number or alien identification number, as applicable, and physical and mailing addresses.

ii. Describe the amount and type of equity interests of the applicant owned by each Director, Principal Officer, Principal Stockholder, and Principal Beneficiary. Complete a sworn statement of ownership form for the applicant.

iii. For each Principal Stockholder and Principal Beneficiary who is a natural Person, and each director and Principal Officer, describe all material occupations, positions, offices or employment during the preceding 15 years. Include: (a) the name, address, and principal activities of any business, corporation, or other entity in which each occupation, position, office or employment was carried on; (b) the starting and ending dates of each; and (c) a statement as to whether within such period s/he was discharged from such occupation, position, office or employment and, if so, for what reason. Such information must be accompanied by a form of authority, executed by such individual, to release information to the Department.

iv. In the case any Person other than a natural Person is a Principal Stockholder or Principal Beneficiary of the applicant, provide the name, address, and date and place of incorporation or organization of any such Person. Also provide an organization chart to show the beneficial ownership relationship between the parties.

v. In the case of any owner that is not a natural Person but an investment company or equity fund, provide the following.

For each investment company, provide: (a) a general description of the company; (b) a listing of all funds managed by the company; (c) a listing of all directors and officers of the company; and (d) audited financial statements for the past two years. If audited financial statements are not available, provide a statement explaining why they are not required.

For each fund managed by an investment company, provide: (a) a general description of the Fund, the date formed, and the purpose of the fund; (b) a statement of whether the fund is opened or closed to new investors; (c) a list of any investors in the fund who hold more than a 10% interest; (d) a list of any investors in the fund who have any control over the management or policies of the fund; (e) indication of whether the investors in the fund are indirect, passive owners and, if so, attach a copy of the applicable pages from the investment agreement evincing said restriction; (f) a listing of all directors and officers of the fund; and (g) the BSA/AML and compliance policies in place for the screening of all potential investors in the fund.

vi. Describe the amount and type of equity interests of applicant, owned, either directly or indirectly through ownership of another entity, by any such Person or the Person's associates.

vii. Indicate whether any director, Principal Officer, Principal Stockholder, or Principal Beneficiary of the applicant ever applied for a license or other authorization, in this State or otherwise, to engage in virtual currency-related activity, money transmission, or other financial services activity. If answered in the affirmative, state whether such license was granted. If granted, state whether such license was ever suspended, revoked, or refused renewal.

viii. The exhibits marked "Questionnaire" and "Litigation Affidavit" in the enclosed material must be completed by each director, Principal Officer, Principal Stockholder, and Principal Beneficiary of the applicant.

ix. Provide an organization chart, including the applicant and all Affiliates. Indicate Principal Stockholders and Principal Beneficiaries.

E. Information Regarding Operations

i. List the jurisdictions in which the applicant proposes to operate. If applicable, list the locations in other countries in which the applicant proposes to engage in virtual currency-related activities. List any other virtual currency, money transmitter, or other entities routinely used to facilitate transactions.

ii. Provide an organization chart of the applicant and its management structure, including its Principal Officers or senior management, indicating lines of authority and the allocation of duties among its principal officers or senior management.

iii. Describe, in detail, the proposed operations for conducting the Virtual Currency Business Activity. This description should include information on the staffing and internal organization of the applicant, its systems and procedures, and details of all banking arrangements. Include letters from bank compliance officers that the bank is aware that the applicant's accounts are being used to facilitate virtual currency-related activity.

iv. Provide an explanation of the methodology used to calculate the value of virtual currency in fiat currency.

v. Provide a specimen form of all agreements, documents, receipts, disclosures, and contracts that the applicant plans to issue or use with customers in this State.

vi. Provide a flow of funds narrative, including a flow chart, specifying all flows of funds that will occur in the normal operation of the applicant. Specify who directs the flow and how it is done; the name and address of each entity the funds flow through; the title of each

account; ownership or control of the accounts and addresses and who or what entity is liable for the funds at all points.

F. Information Regarding Other Agreements

Provide copies of any other agreements the applicant has entered into (or will enter into) in anticipation of Virtual Currency Business Activity.

G. Information Regarding Legal Proceedings

Describe (a) any criminal action brought against the applicant or any director, Principal Officer, Principal Stockholder or Principal Beneficiary of the applicant; (b) any civil action brought against the applicant or any director, Principal Officer, Principal Stockholder or Principal Beneficiary of the applicant (excluding any civil action in which the amount in controversy was less than $25,000 or which terminated more than 15 years prior to submission of this application); and (c) any proceeding brought to declare the applicant, or any director, Principal Officer, Principal Stockholder or Principal Beneficiary of the applicant, bankrupt and the disposition of such action or proceeding.

H. Information Regarding Financial Statements

i. Provide a current audited financial statement for the applicant prepared by an independent certified public accountant and a projected balance sheet and income statement for the following year of the applicant's operation. The projected balance sheet and income statement must include the assumptions used in making the projections. If audited financial statements are unavailable, include an explanation of why. If the applicant's fiscal year ends more than 60 days prior to the date of application, provide a supplemental financial statement for a period ending not more than 60 days prior to the date of application (which may be prepared by applicant). All financial statements must include a balance sheet, profit and loss statement, and a statement of retained earnings. Where the applicant has wholly owned subsidiaries, financial statements for applicant alone, as well as consolidated financial statements, must be filed. Any exhibited losses must be explained and a projected date for the return to or achieving profitability must be included.

ii. Applicants that are not able to provide current financial statements must provide a pro forma balance sheet and profit and loss statement. Include retained earnings for the business as of the close of each of the first two years of operation. Include the assumptions used in making the projections. Any projected losses must be explained and an estimate of time to achieve profitability should be given.

iii. Financial statements of foreign-owned applicants must be presented in both the applicable foreign currency and in United States Dollars. The date and basis of conversion must be stated.

iv. Complete the enclosed Personal Financial Statement for each director, Principal Officer, Principal Stockholder and Principal Beneficiary of the applicant. Alternatively, a different format may be used provided it contains substantially similar information; but in either case the statement must be dated and certified as complete and correct by the party submitting it.

v. Provide audited financial statements for the most recent two fiscal years of any Person, other than a natural person, which directly or indirectly owns 10% or more of the equity interests of the applicant. Such financial statements must include a balance sheet, profit and loss statement, and a statement of retained earnings. Any exhibited losses must be explained and a projected date for the return to or achieving profitability must be included.

I. Required Affidavits

Provide affidavits describing any pending or threatened administrative, civil, or criminal action, litigation, or proceeding before any governmental agency, court, or arbitration tribunal against the applicant or any of its directors, Principal Officers, Principal Stockholders, and Principal Beneficiaries, as applicable, including the names of the parties, the nature of the proceeding, and the current status of the proceeding.

J. Anti-Money Laundering (BSA/AML)

i. Provide written BSA/AML policies and procedures that meet the requirements set forth in 23 NYCRR 200.15, including the applicant's risk assessment.

ii. Identify the individual or individuals who will be responsible for coordinating and monitoring day-to-day compliance with the applicant's anti-money laundering program and provide background information and materials demonstrating that the identified individual(s) is qualified to carry out such functions.

K. Surety Bond or Trust Account

i. Indicate how the applicant proposes to comply with the requirements of 23 NYCRR 200.9(a), including the general manner, the proposed amount of the bond or trust account, and why the applicant believes such an amount is sufficient for the protection of customers.

ii. To the extent the applicant purposes to use a trust account, identify the qualified custodian at which the account will be maintained.

L. Fingerprints

Applicants must provide, for each individual applicant; for each Principal Officer, Principal Stockholder, and Principal Beneficiary of the applicant, as applicable; and for all

individuals to be employed by the applicant who have access to any customer funds, whether denominated in fiat currency or virtual currency:

i. a set of completed fingerprints, or a receipt indicating the vendor at which, and the date when, the fingerprints were taken, for submission to the State Division of Criminal Justice Services and the Federal Bureau of Investigation; and

ii. two portrait-style photographs of each such individual measuring not more than two inches by two inches.

iii. fingerprints must be submitted according to the procedures available on our website at http://www.dfs.ny.gov/banking/iafpplfs.htm.

M. Background Investigation Reports

Provide an investigative background report prepared by an independent investigatory agency for each individual applicant, and each Principal Officer, Principal Stockholder, and Principal Beneficiary of the applicant, as applicable. It is the responsibility of the applicant (and its, Principal Officers, Principal Stockholders, and Principal Beneficiaries, as applicable) to order such reports at their own expense, from an independent licensed private investigation company.

All background investigation reports must be provided directly to the Department by the licensed private investigation company. Note that the failure to promptly order the reports may delay application processing.

These reports should be sent to:

New York State Department of Financial Services
Virtual Currency Applications
One State Street, 20th Floor
New York, NY 10004-1511

The following list specifies information that must be included in a submitted background report. No background report will be considered complete unless all the information requested below is included in the investigation report.

i. Comprehensive credit report/history (include the actual report as well as summary).

ii. Civil Court and Bankruptcy Court records for the past 10 years. Include federal, state, and local courts. Such reports shall contain, at a minimum, court dates from courts located in counties in which the applicant both worked and resided and all counties contiguous to those counties.

iii. Criminal records, including felonies, misdemeanors, and violations. Include federal, state, and local courts. Such reports shall contain, at a minimum, court dates from courts located in counties in which the applicant worked and/or resided and all counties contiguous to those counties.

iv. Education records.

v. Employment history.

vi. Personal and professional references (at least three of each, excluding relatives), which must be furnished in writing.

vii. Media history, if applicable (include electronic search of national and local newspapers, wire services, and business publications).

viii. Regulatory history, if applicable (HUD, FREDDIE MAC, State Regulators, OCC, FINRA, etc.).

ix. Department of Motor Vehicles records.

x. All judgments and liens filed with the county clerk (within the past ten years) (such reports shall contain, at a minimum, information on judgments and liens filed with the county clerk in counties where the applicant worked and resided and all counties contiguous to those counties).

xi. Licenses granted by any governmental agency or judicial body (indicate if they are still in good standing).

xii. Listing of all credit relationships by the applicant (such as revolving credit and established credit facilities) and indication of any credit extensions, including loans, on which the applicant is in default (more than 90 days past due).

N. FinCEN Registration

To the extent applicable, the applicant is required to submit evidence that it has registered with FinCEN as a Money Service Business. A copy of FinCEN's confirmation or acknowledgment letter will be sufficient. If the applicant believes it is not required to register with FinCEN, the applicant must provide an explanation and supporting documentation for that conclusion.

O. Written Policies and Procedures

Provide copies of all written policies and procedures required by, or related to, the requirements of 23 NYCRR 200, including but not limited to policies and procedures addressing:

i. compliance;
ii. anti-fraud;
iii. cyber security;
iv. privacy and information security;
v. business continuity and disaster recovery;
vi. complaints and complaint resolution.

P. Miscellaneous

Provide the name, address, telephone number and facsimile telephone number of applicant's counsel and independent certified public accountant, to the extent applicable.

VI. FILED APPLICATIONS

For any questions concerning the preparation and filing of an application, submit questions to VCLicenseQuestions@dfs.ny.gov. Question submissions should include contact information that the Department may use to contact you regarding your question.

ENCLOSURES

For a License to Engage in Virtual Currency Business Activity

As applicable, the following individual forms must be filled out by the applicant and submitted with the application:

- Authority to Release Information
- Background Report Certification
- Personal Financial Statement
- Litigation Affidavit – Individual
- Litigation Affidavit – Licensee/Applicant
- Questionnaire
- Statement of Ownership
- Taxpayer ID

These forms are provided below.

AUTHORITY TO RELEASE INFORMATION

TO WHOM IT MAY CONCERN:

I hereby authorize any duly authorized representative of the New York State Department of Financial Services (DFS) bearing this release, or copy thereof, within one year of its date, to obtain any information in your files pertaining to any professional license awarded to me (including any grievance records), employment, military, educational records (including, but not limited to academic achievement, attendance, athletic, personal history, and disciplinary records), credit records, and law enforcement records (including, but not limited to any record of charge, prosecution or conviction for criminal or civil offenses). I hereby direct you to release such information upon request to the bearer. This release is executed with full knowledge and understanding that the information is for the official use of the DFS. Consent is granted for the DFS to furnish such information, as is described above, to third parties in the course of fulfilling its official responsibilities. I hereby release you, as the custodian of such records, your employers, officers, employees, and related personnel, both individually and collectively, from any and all liability for damages of whatever kind, which may at any time result to me, my heirs, family or associates because of compliance with this authorization and request to release information, or any attempt to comply with it. I am furnishing my Social Security Account Number on a voluntary basis with the understanding such is not required by statute or regulation. I understand that the DFS will use the number only to assist the Superintendent of Financial Services in making a determination as to whether I meet the standards set forth pursuant to the Financial Services Law and regulations for receiving the license for which I am applying. Should there be any question as to the validity of this release, you may contact me as indicated below:

I have read the above release and agree to the terms and conditions therein.

Social Security Account Number: _____

Date of Birth: _____

Signature of Parent or Guardian (if required): _____

Date: _____

Current Address:_____

Telephone Number:_____

CPA/Bar Membership(s) State:_____

Registration Number:_____

Full Name (Signature):_____

Full Name (Typed or Printed):_____

(Include maiden and any other previously-used name(s)):_____

STATE OF _____} ss.:
COUNTY OF_____}

Before me, a Notary Public in and for said County and State, personally appeared the above-named who acknowledged that s/he did sign the foregoing instrument and that the same is his/her free and voluntary act and deed. IN TESTIMONY WHEREOF, I have hereunto set my hand and official seal at, _____ this _____day of_____, 20_____ .

_____
Notary Public

BACKGROUND REPORT CERTIFICATION

Re:_____
(Subject of Report)

I, _____, do certify that a background report

on_____, _____
(Name) (Title)

of _____ was ordered
(Applicant's Name)

from _____
(Name of Company)

on_____. If ordered by telephone, the report
(Date Report Was Ordered)

was ordered from_____.
(Name of Person Taking Order)

_____
(Signature)

_____
(Title)

_____
(Date)

THIS FORM MAY BE REPRODUCED

2015.06.24 Version

PERSONAL FINANCIAL STATEMENT

NAME_____
(APPLICANT, OFFICER, DIRECTOR, STOCKHOLDER, OR INDIVIDUAL, AS APPLICABLE)

ADDRESS_____

To: THE NEW YORK STATE DEPARTMENT OF FINANCIAL SERVICES (DFS)

The undersigned make(s) the following statement of (my)(our)(its) assets and liabilities at the close of business of the _____ day of _____, _____.

PLEASE ANSWER ALL QUESTIONS USING "NO" OR "NONE" WHERE NECESSARY.

ASSETS		LIABILITIES AND NET WORTH	
Cash on Hand and in Banks (Sch 1)		Notes Payable Banks (Sch 1)	
Finance Agreements		Notes Payable Others (Sch 4)	
Finance Agreements-Pledged		Due to Principals (Sch 4)	
Notes Receivable		Notes Rec., Discounted (Contra)	
Notes Rec., Discounted (Contra)		Accounts Payable	
Accts and Loans Receivable		Accrued Expenses Payable	
Cash		Accrued Interest Payable	
Securities (Sch 2)		Accrued Taxes and Asses Pay.	
Due from Part, Stkhrs, Off, Empl.		Brokers Margin Account Pay	
Inv. And Adv. –Affil. Or Subsid. Co.		Mortgages Payable (Sch 3)	
Mortgages Owned		Unearned Income	
Real Estate (Sch 3)		Valuation Reserve-Bad Debts	
Furn, Fix, and Equip (Net of Depr)		Valuation Reserve-Contingencies	
Other Assets (Itemize)		Other Liabilities (Itemize)	

		Total Liabilities	
		Preferred Stock	
		Common Stock	
		Surplus	
		Net Worth (Indiv. Or Part.)	
Total Assets		Total Liabilities and Net Worth	

SUPPLEMENTARY SCHEDULES

Sch. 1. Banking Relations (A list of all bank accounts, including savings)

Name and Address of Bank	Balance	Loans, if any	Endorsed, Guaranteed or Secured

Sch.2. Securities Owned (Stocks, Bonds, etc., but not mortgages)

Par Val. Or Shs.	Description	Cost	Pres. Mkt. Val	To Whom Pledged

Sch.3. Real Estate Owned – Mortgage Payable

Location and Description	Cost	Asses. Val.	Est. Val.	Mortgage Balance	Maturity

Sch.4. Notes Payable – Due to Principals (Partners, Stockholders, Officers and Others)

Due To	Amount	Due Date	Due To	Amount	Due Date

CONTINGENT LIABILITY. The undersigned has (have) no contingent liabilities as endorser, guarantor, or otherwise, except the following: (Give details.)

SUITS, JUDGMENTS AND OTHER LEGAL ACTIONS. There are no suits, judgments, or other legal actions outstanding or pending against the undersigned and to the best of the undersigned's knowledge no legal actions are to be started against undersigned, except as follows: (Give details.)

PLEDGE ASSIGNMENT, AND TRANSFER OF TITLE OR ASSETS. As of the date of the statement of assets and liabilities, included in this financial statement, the undersigned has (have) not pledged, assigned, hypothecated, or transferred the title of any of the assets as listed above, except as noted in the various schedules of this financial statement; and the undersigned has (have) not pledged, assigned, hypothecated, or transferred the title of any such assets, except as follows: (Give details.)

INSURANCE COVERAGE. - Fidelity Bond: Partners, Officers, Employees $ _____;
Indemnity Coverage: Robbery and Holdup $ _____; Burglary $ _____;
Misplacement $ _____; Forgery $ _____;
Errors and Omissions $ _____; Public Liability $ _____;
Fire Insurance: Furn., Fix., and Equip. $ _____
Other Insurance (describe):

ACCOUNTING DATA. - If books are kept or audited please give name of accountant _____; Indicate if Certified Public Accountant _____; Frequency of Audits _____; Date of Last Audit _____; Date of Fiscal Year-End _____; Did the accountant prepare the financial statement submitted herewith? _____ Are the figures shown the same as the auditor's figures? _____If not, how do the figures differ (give details):

The undersigned has (have) carefully read the foregoing statements, and all printed and written matter therein, and hereby certifies that all the statements are known to me (us) to be true and give a correct showing of the undersigned financial conditions, and that the undersigned has (have) no liabilities, direct, or contingent, business or accommodation, except as set forth in said complete statement, and that the legal and equitable title to all assets therein set forth is in the name of the undersigned solely, except as otherwise noted therein.

Signed this_____ day of _____, 20___ .

_____
Name of Entity

By:_____ By:_____

Title: _____ Title: _____

By:_____ By:_____

Title: _____ Title: _____

LITIGATION AFFIDAVIT
FOR INDIVIDUALS

STATE OF NEW YORK, **}**
}
} **ss:**
}

County of

I, _____, being duly sworn, depose and say:

That there are no arrests, indictments, criminal information or other criminal proceedings now pending against me as an individual, partner, director or officer of a corporation; that I have never been convicted of a crime in any jurisdiction in any of these capacities, that I have never been sued nor has any judgment been obtained against me in any of these capacities in any civil action in any jurisdiction; and that I have never been the subject of any administrative or disciplinary proceedings initiated by a regulatory or governmental agency in any of these capacities.

_____
Signature

Subscribed and sworn to before me this _____ day of _____, 20_____.

_____
Notary Public

LITIGATION AFFIDAVIT
FOR LICENSEE/APPLICANT

I, _____, the _____ of
(Print or type name) (Title)

_____ ,

being duly sworn, depose and say:

There are no indictments, criminal information or other criminal proceedings now pending against the licensee/applicant, that it has never been sued nor has any judgment been obtained against it in any civil action in any jurisdiction; and that it has never been the subject of any administrative or disciplinary proceedings initiated by a regulatory or governmental agency except as noted below.

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

_____
(Signature)

Subscribed and sworn to before me this _____ day of _____, 20_____.

_____
Notary Public

NEW YORK STATE DEPARTMENT OF FINANCIAL SERVICES
PERSONAL QUESTIONNAIRE
(Please Print or Type)

Please answer all questions, using "No," "None" or "Not Applicable" where necessary

1. Full Name: _____ Soc. Sec. No.: _____
First, Middle, Last
Have you ever been known by, or used, any other name? If so, list such name(s):

2. Home Address:_____

_____

How long at this address: _____

3. Previous Home Address(es) (immediately prior to present address for the last 15 years):

_____

How long at this address: _____

4. Present Occupation:

Firm Name:_____

Business Address: _____

Nature of Business:_____

Title: _____

Telephone Number: _____

Email Address: _____

Name of Immediate Superior: _____

5. Date of Birth: _____ Place of Birth: _____

Citizenship:_____ Right-to-Work in USA: Yes ( ) No ( )

Passport No.: _____ Visa Type:_____

Country of Issue: _____ Expiration Date: _____

6.

Education Awarded	Name and Address of School	Dates of Attendance	Major Area of Study	Degree Granted and Date
High School				
College, University (Undergraduate)				
College, University (Graduate)				
Professional or Technical School				

7. Do you have a license to practice any profession: Yes ( ) No ( )

If "yes" give details:

(a) Nature of License: _____

(b) Date Issued: _____ Number of license (if any): _____

(c) Licensing Agency and Address: _____

8. Employment Record for the last 15 years. Account for all gaps in employment. (Use additional sheets if necessary.)

Name & Address of Employer	Dates of Employment	Position Held & Duties	Immediate Supervisor	Reason for Leaving

9. If self-employed, describe each enterprise, including the name, address, state of incorporation, your percentage of ownership and the type of business of each corporate or other entity which you own or control. (Control means ownership of 10% or more of the stock or the ability to effectively control the management of the corporation or other entity.)

List names, addresses and percentage of control and/or ownership of other incorporators, partners, directors or officers of the entity referred to above.

10. Are you employed in any professional capacity, or do you perform any services for or have any business connections with any institution which is subject to the supervision of the Department, or any agency or authority of the State of New York?

Yes ( ) No ( )

If "yes," indicate name of institution, address and nature of your work.

11. Have you had, or do you now have, any financial interest, direct or indirect, in any institution under the supervision of any authority or agency in New York State, or any other state?

Yes ( ) No ( )

If "yes," give the name of the institution, address and nature of interest.

12. References:

(a) List the names and addresses of three personal references who can attest to your character, fitness and reputation. (State how long you have known each person; do not include relatives or current business associates.)

(b) List the names and addresses of three professional references who can attest to your character, fitness, reputation, professional competence and business skills.

13. List of checking, savings and any borrowing relationships in excess of $10,000, for both personal and business purposes. (Use additional sheets if necessary.)

Name and address of Creditor/ Financial Institution	Account Number	Type of relationship (checking, savings, Personal/ business borrowing and so on)	Account balance / loan outstanding

14. Answer yes to any of these questions if they apply to you as an individual, or as partner, director or officer of a corporation.

Except for minor traffic violations:

	Yes	No
(a) Are any arrests, indictments, criminal information or other criminal proceedings now pending against you?	( )	( )
(b) Were you ever convicted for any violation of law?	( )	( )
(c) Have you or has any partnership of which you were a member or any corporation of which you were a principal officer or major stockholder ever been adjudged a bankrupt or involved in a civil action either as a defendant or plaintiff (within the past 10 years)?	( )	( )
(d) Have you ever initiated or been named in any administrative or disciplinary proceedings?	( )	( )
(e) Has your salary ever been garnished (within the past 10 years)?	( )	( )

If your answer to any of the above questions is "Yes", on a separate sheet of paper list the dates, name and location of the court of jurisdiction or administrative agency and a brief description of each action or charge and its disposition. Report all legal actions, regardless of disposition. Include copies of documents you have which provide information on any matters listed.

15. Has any enterprise in which you were a partner, director or officer been the subject of federal or state administrative proceedings, criminal indictment, criminal information or other criminal proceeding?	( )	( )

If your answer is "Yes", on a separate sheet of paper provide a description of each administrative or disciplinary proceeding and its disposition. Report all matters, regardless of disposition. Include copies of documents you have which provide information on any matters listed.

16. Have you and/or any enterprise in which you are a partner failed to file required federal, state and local tax returns for the previous three calendar years?

Yes	No
( )	( )

If your answer is "yes", on a separate sheet of paper, please explain the circumstances and include the date on which any applications for extension have been filed.

The undersigned affirms that the statements made and answers given herein are accurate and complete, and hereby authorizes the New York State Department of Financial Services to make any inquiry it deems appropriate in connection with processing this questionnaire. FALSE WRITTEN STATEMENTS IN THIS QUESTIONNAIRE ARE PUNISHABLE UNDER SECTION 210.45 OF THE NEW YORK PENAL LAW (making a punishable false written statement) and also as per the New York Financial Services Law and regulations, the Superintendent of Financial Services may initiate regulatory actions against the licensee.

Date _____ Signature _____

STATEMENT OF OWNERSHIP
OF LICENSED ENTITY ENGAGED IN VIRTUAL CURRENCY BUSINESS ACTIVITY

I, _____, being duly sworn, depose and state:

I. That I am an officer of the _____ Corporation,

namely _____.
(Title)

II. That in my capacity as such I have applied in the name of the corporation for a license to engage in Virtual Currency Business Activity.

III. That the stock ownership of the _____ Corporation is distributed as follows:

_____ %
_____ %
_____ %
_____ %

and that no other persons will invest any funds in the Corporation nor share in the management or profits of the Corporation, either directly or indirectly.

IV. That I understand that false statements made in this affidavit under oath may result in the revocation of the Virtual Currency Business Activity license of _____ (entity name) and in prosecution for perjury.

_____
Applicant

Subscribed and sworn to before me this _____day of _____, 20 _____.

_____
Notary Public

TAXPAYER IDENTIFICATION INFORMATION

Disclosure of this information by you is mandatory in order to complete the processing of your application. The authority to request personal information from you, including identifying numbers, and the authority to maintain such information from you, including identifying numbers, and the authority to maintain such information is found in Section 5 of the Tax Law. The principal purpose for which the information is collected is to enable the Department of Taxation and Finance to identify individuals, businesses and others who have been delinquent in filing tax returns or may have understated their tax liabilities and to generally identify persons affected by the taxes administered by the Commissioner of Taxation and Finance. The information will be used for tax administration purposes and for any other purpose authorized by the Tax Law.

(Print or Type information) (This form may be reproduced as necessary)

1. Social Security Number (complete only if applicant is other than a corporation. A separate form must be completed for each partner or associate).

_____

2. Employer Identification Code (for reporting wages of employees)

_____

3. Legal Name (individual, partner or associate)

_____

4. Trade Name (Doing business as D/B/A in license or application)

_____

5. Street Address of Business (to be licensed or authorized)

_____

6. City _____ 7. State_____

8. Zip and 4 Digit Code _____

9. County _____

Exhibit R

RULE MAKING ACTIVITIES

Each rule making is identified by an I.D. No., which consists of 13 characters. For example, the I.D. No. AAM-01-96-00001-E indicates the following:

AAM -the abbreviation to identify the adopting agency
01 -the *State Register* issue number
96 -the year
00001 -the Department of State number, assigned upon receipt of notice.
E -Emergency Rule Making—permanent action not intended (This character could also be: A for Adoption; P for Proposed Rule Making; RP for Revised Rule Making; EP for a combined Emergency and Proposed Rule Making; EA for an Emergency Rule Making that is permanent and does not expire 90 days after filing.)

Italics contained in text denote new material. Brackets indicate material to be deleted.

Office of Alcoholism and Substance Abuse Services

PROPOSED RULE MAKING NO HEARING(S) SCHEDULED

Implementation of a Program for the Designation of Vital Access Providers

I.D. No. ASA-29-14-00002-P

PURSUANT TO THE PROVISIONS OF THE State Administrative Procedure Act, NOTICE is hereby given of the following proposed rule:

Proposed Action: This is a consensus rule making to add Part 802 to Title 14 NYCRR.

Statutory authority: Mental Hygiene Law, sections 19.09(b), 19.20, 19.20-a, 19.40, 32.02; L. 2014, ch. 53

Subject: Implementation of a program for the designation of Vital Access providers.

Purpose: To ensure preservation of access to essential services in economically challenged regions of the state.

Text of proposed rule: *PART 802*
VITAL ACCESS PROGRAM and PROVIDERS
802.1 Background and Intent.
The Purpose of this Part is to provide a means to support the stability and geographic distribution of substance use disorder treatment services throughout all geographic and economic regions of the state. A designation of Vital Access Provider denotes the state's determination to ensure patient access to a provider's essential services otherwise jeopardized by the provider's payer mix or geographic isolation. Vital Access Providers in the OASAS system are limited to eligible OASAS certified inpatient rehabilitation facilities, or such other programs as may be designated by the commissioner.

802.2 Legal Base
(a) Section 19.07(e) of the Mental Hygiene Law authorizes the Commissioner ("Commissioner") of the Office to adopt standards including necessary rules and regulations pertaining to chemical dependence services.
(b) Section 19.09(b) of the Mental Hygiene Law authorizes the Commissioner to adopt regulations necessary and proper to implement any matter under his or her jurisdiction.
(c) Section 19.40 of the Mental Hygiene Law authorizes the Commissioner to issue operating certificates for the provision of chemical dependence services.
(d) Section 25.09 of the Mental Hygiene Law authorizes the Office to establish limits on the amount of financial support which may be advanced or reimbursed to a program for the administration of such program.
(e) Section 32.01 of the Mental Hygiene Law authorizes the Commissioner to adopt any regulation reasonably necessary to implement and effectively exercise the powers and perform the duties conferred by Article 32 of the Mental Hygiene Law.
(f) Section 32.07(a) of the Mental Hygiene Law authorizes the Commissioner to adopt regulations to effectuate the provisions and purposes of Article 32 of the Mental Hygiene Law.
(g) Section 43.02 of the Mental Hygiene Law authorizes the establishment of rates or methods of payment for services at facilities subject to licensure or certification by the Office.
(h) Section 23 of part C of chapter 58 of the laws of 2009, authorizes the commissioner, with the approval of the Commissioner of Health and the Director of the Budget, to promulgate regulations pursuant to Article 32 of the Mental Hygiene Law utilizing the APG methodology described in subdivision (c) of section 841.14 of this Part for the purpose of establishing standards and methods of payments made by government agencies pursuant to title 11 of article 5 of the Social Services Law for chemical dependence outpatient clinic services.
(i) Chapter 53 of the Laws of 2014 authorizes the commissioner to provide special funding to certain designated providers.
802.3 Definitions.
(a) "Vital Access Program" means a program of supplemental state funding and/or temporary rate adjustments available to designated vital access providers pursuant to Part 841 of this Title and the provisions of this Part.
(b) "Vital Access Provider" ("VAP") means an OASAS certified program that is designated by the commissioner as essential but not financially viable because of its service to financially vulnerable populations and/or provision of essential services in an otherwise underserved region.
802.4 Vital Access Program.
(a) Program. The Vital Access Program is a program of ongoing supplement to the non-capital component of service reimbursement rates calculated pursuant to Part 841 of this Title, or exemption from payment reductions, as long as the designation as a vital access provider, as determined pursuant to this section, applies.
(b) Eligibility. The commissioner may grant approval of temporary adjustments to OASAS certified inpatient rehabilitation (IPRs) programs, or such other programs as may be designated by the commissioner, which demonstrate through submission of a written application that the additional resources provided by a temporary rate adjustment will achieve one or more of the following:
(1) protect or enhance access to care;
(2) protect or enhance quality of care;
(3) improve the cost effectiveness of the delivery of health care services; or
(4) otherwise protect or enhance the health care delivery system, as determined by the commissioner.
(c) Application. (1) The written application pursuant to subdivision (a) shall be submitted to the commissioner at least sixty (60) days prior to the requested effective date of the temporary rate adjustment and shall include a proposed budget to achieve the goals of the proposal.

The revised proposed amendment defines a traditional standardized assessment as a systematic method of gathering information from objectively scored items that allow the test taker to select one or more of the given options or choices as their response. Examples include multiple-choice, true-false, and matching items. Traditional standardized assessments are those that require the student (and not the examiner/assessor) to directly use a ''bubble'' answer sheet. Traditional standardized assessments do not include performance assessments or assessments in which students perform real-world tasks that demonstrate application of knowledge and skills; assessments that are otherwise required to be administered by federal law; and/or assessments used for diagnostic or formative purposes. Therefore, if these assessments are used for diagnostic purposes and the superintendent, district superintendent, or chancellor of a school district/BOCES that chooses to use such assessment certifies in its APPR plan that the assessment is a not a traditional standardized assessment and that the assessment meets the minimum requirements prescribed by the Commissioner in guidance, these assessments may be used in grades K-2 for APPR purposes.

2. COMMENT: The provision that no APPR plan for the 2014-15 school year will be approved if it includes ''traditional standardized third party or vendor assessments to students in kindergarten through grade two.'' Not knowing what your definition of ''traditional third party, standardized assessments will be'' I have a few concerns.

First, our district chose to use AISMweb Reading & Math for our Growth sub-component for K-2 teachers in our APPR plan. We made this decision so that we would be able to use an assessment that was already in place for our students. Simply said, we wouldn't be adding or creating a new assessment on top of what we already use for RTI/DIagnostic/Formative purposes.

Secondly, it would seem that the exclusion of RTI/Diagnostic/Formative assessments such as AIMSweb, which are used to meet the state mandate of implementing an RTI approach to identifying students with learning disabilities, would have the opposite effect of reducing testing for K-2 students. For example, since we have a K-2 building we would need to create a new (and likely longer, less reliable) assessment to use for our K-2 teacher's growth sub-component. This would add to the time we utilize for assessments and end up adding an assessment that is primarily used for APPR purposes.

RESPONSE: See response to Comment #1.

3. COMMENT: Our district uses two of the approved K-2 assessment products: Aimsweb and STAR (Renaissance Learning) as diagnostic and instructional tools while also using the assessment to meet APPR requirements. The possibility of removing these options for our districts will actually INCREASE the amount of testing necessary for K-2 students instead of decreasing it as the adjustment to the regulation intends. Please consider this carefully before a decision is finalized.

RESPONSE: See response to Comment #1.

4. COMMENT: Our district has, for many years, used AIMSWeb as a diagnostic test for students K-8. We were certainly pleased when SED approved AIMSWeb for use with APPRs, as we were able to limit testing of students for APPR purposes by using this test both for diagnostic and for APPR purposes. The recommendations to the BOR will force disapproval of the use of these tests for the APPR. Consequently, our district will be forced to either use a group/building metric for the APPR or find another test which can be used. In the case of the latter, we will indeed be ADDING tests for the K-2 students as we will no longer be able to use AIMSWeb for both purposes. Again, AIMSWeb has been used in this district for years as a diagnostic. As well, the time spent on this assessment is well under the 1% cap. It is working and we are concerned about a change simply for the sake of change, or a change that is responsive to political pressures rather than a consideration of what is actually happening in schools.

While a group metric is another option, as a district, we have chosen to avoid that route, particularly as the results of the 3rd grade ELA and Math assessments would be used for the group metric. We believe that a teacher's score for their APPR should as closely as possible reflect the current work they are doing with their current classes. Certainly, the work that a K-2 teacher does will eventually contribute to a student's score in 3rd grade, but issues of cohorts and student population within any given year may not accurately represent the work that they are currently doing.

So, we are asking for clarification. If we are using AIMSWeb for diagnostic purposes, in the interest of avoiding double testing, can the results of that test be used for APPR purposes? If the answer currently is no, we respectfully ask you to reconsider this decision which will not only negatively impact districts but, most importantly, will negatively impact children.

RESPONSE: See response to Comment #1.

5. COMMENT: Although I, too, support eliminating K-2 standardized assessments for APPR purposes, I propose that districts have the ability to continue using AIMSweb (included on the State approved list) for APPR purposes. First, AIMSweb houses data for short (1 - 8 minutes) reading, writing, and math probes (assessments). These probes are better described as formative/interim assessments typically used for Response to Interventions (RtI) decision-making. What is more, the early literacy probes such as letter naming measures and letter sound measures are performance tasks. In essence, AIMSweb probes are similar in nature to the Dynamic Indicators of Basic Early Literacy Skills (DIBELS).

I bring this to your attention because we have been using AIMSweb probes two ways in grades K-5. First way, as universal screenings for RTI and second, to meet APPR guidelines for our K-5 student population. I'm thinking that districts who have double-dipped would appreciate having the ability to make a local decision regarding AIMSweb use for K-2 APPR purposes.

RESPONSE: See response to Comment #1.

Department of Environmental Conservation

NOTICE OF ADOPTION

Recreational Harvest Regulations for Summer Flounder (Fluke) and Black Sea Bass

I.D. No. ENV-19-14-00020-A

Filing No. 595

Filing Date: 2014-07-08

Effective Date: 2014-07-23

PURSUANT TO THE PROVISIONS OF THE State Administrative Procedure Act, NOTICE is hereby given of the following action:

Action taken: Amendment of Part 40 of Title 6 NYCRR.

Statutory authority: Environmental Conservation Law, sections 11-0303, 13-0105, 13-0340-b and 13-0340-f

Subject: Recreational harvest regulations for summer flounder (fluke), and black sea bass.

Purpose: To maximize recreational angler opportunities for popular finfish species while staying in compliance with ASMFC.

Text or summary was published in the May 14, 2014 issue of the Register, I.D. No. ENV-19-14-00020-EP.

Final rule as compared with last published rule: No changes.

Text of rule and any required statements and analyses may be obtained from: Stephen Heins, Department of Environmental Conservation, 205 N. Belle Mead Rd, Suite 1, East Setauket, NY 11733, (631) 444-0435, email: swheins@gw.dec.state.ny.us

Additional matter required by statute: Pursuant to the State Environmental Quality Review Act, a negative declaration is on file with the Department.

Initial Review of Rule

As a rule that requires a RFA, RAFA or JIS, this rule will be initially reviewed in the calendar year 2017, which is no later than the 3rd year after the year in which this rule is being adopted.

Assessment of Public Comment

The agency received no public comment.

Department of Financial Services

PROPOSED RULE MAKING
NO HEARING(S) SCHEDULED

Arbitration

I.D. No. DFS-29-14-00003-P

PURSUANT TO THE PROVISIONS OF THE State Administrative Procedure Act, NOTICE is hereby given of the following proposed rule:

Proposed Action: Amendment of Subpart 65-4 of Title 11 NYCRR.

Statutory authority: Financial Services Law, sections 202 and 302; Insurance Law, sections 301 and 5201 and art. 51

the Department of Financial Services ("Department"), it is not known how many of them are small businesses, but it is believed that a significant number of them may be small businesses.

Persons affiliated with title insurance agents or title insurance corporations would not, by definition, be independently owned and would thus not be small businesses.

The rule does not impose any impacts, including any adverse impacts, or reporting, recordkeeping, or other compliance requirements on any local governments.

2. Compliance requirements: The proposed rules conform and implement requirements regarding title insurance agents and placement of title insurance business with Chapter 57 of the Laws of 2014, which made title insurance agents subject to licensing in New York for the first time. A number of the rules will make title insurance agents subject to the same requirements that apply to other insurance producers. There are also disclosure requirements unique to title insurance.

3. Professional services: This amendment does not require any person to use any professional services.

4. Compliance costs: Title insurance agents will need to provide new disclosures in accordance with the regulation if they are not already making such disclosures but they already have an obligation to make changes to notices pursuant to the legislation. There are also new reporting requirements to the Department but these are the same that apply with respect to other licensees. In any event, the costs of these new disclosures and reporting requirements should not be significant. The proposed rules now subject title insurance agents to requirements regarding the maintenance of fiduciary accounts that already apply to other insurance producers. The cost impact on title insurance agents will likely vary from agent to agent but should not be significant.

5. Economic and technological feasibility: Small businesses that may be affected by this amendment should not incur any economic or technological impact as a result of this amendment.

6. Minimizing adverse impact: This rule should have no adverse impact on small businesses.

7. Small business participation: Interested parties, including an organization representing title insurance agents, were given an opportunity to comment on draft proposed rules.

Rural Area Flexibility Analysis

The Department of Financial Services ("Department") finds that this rule does not impose any additional burden on persons located in rural areas, and will not have an adverse impact on rural areas. This rule applies uniformly to regulated parties that do business in both rural and non-rural areas of New York State.

Rural area participation: Interested parties, including those located in rural areas, were given an opportunity to review and comment on draft versions of these rules.

Job Impact Statement

The Department of Financial Services finds that these rules should have no negative impact on jobs and employment opportunities. The rules conform to and implement the requirements of, with respect to title insurance agents and the placement of title insurance business, Chapter 57 of the Laws of 2014, which make title insurance agents subject to licensing in New York for the first time and, by establishing a regulated marketplace, may lead to increased employment opportunity.

PROPOSED RULE MAKING
NO HEARING(S) SCHEDULED

Regulation of the Conduct of Virtual Currency Businesses

I.D. No. DFS-29-14-00015-P

PURSUANT TO THE PROVISIONS OF THE State Administrative Procedure Act, NOTICE is hereby given of the following proposed rule:

Proposed Action: Addition of Part 200 to Title 23 NYCRR.

Statutory authority: Financial Services Law, sections 102, 104, 201, 206, 301, 302, 309 and 408

Subject: Regulation of the conduct of virtual currency businesses.

Purpose: To regulate retail-facing virtual currency business activity in order to protect New York consumers and users and ensure the safety and soundness of New York licensed providers of virtual currency products and services. This regulation complements the Department of Financial Services' Order of March 11, 2014, which provides for the regulation, pursuant to the Banking Law, of exchanges that interact primarily with institutions.

Substance of proposed rule (Full text is posted at the following State website: www.dfs.ny.gov): The following is a summary of the proposed regulation:

Section 200.1, "Introduction," sets forth the statutory authority for the rule.

Section 200.2, "Definitions," defines terms used throughout the proposed regulation. Most significantly this Section defines "virtual currency" and "virtual currency business activity".

Section 200.3, "License," prohibits any Person from engaging in virtual currency business activity without a license.

Section 200.4, "Application," sets forth the information to be included in a prospective licensee's application.

Section 200.5, "Application fees," requires applicants to pay an application fee to the Department of Financial Services (the "Department") and provides that licensees may need to pay fees for the processing of additional applications related to the license.

Section 200.6, "Action by superintendent," provides for the superintendent to approve or deny an application and, if approved, to suspend or revoke a license on specified grounds after a hearing.

Section 200.7, "Compliance," requires licensees to comply with all applicable federal and state law, designate a compliance officer, and maintain and enforce various written compliance policies.

Section 200.8, "Capital requirements," sets forth minimum capitalization requirements and a list of permissible investments.

Section 200.9, "Custody and protection of customer assets," requires licensees to establish a bond or trust account for the benefit of their customers, requires licensees to hold virtual currency in the same type and amount as any virtual currency owed by the licensee, and prohibits licensees from encumbering customer assets.

Section 200.10, "Material change to business," requires licensees to seek prior approval by written application to introduce a new, or materially change an existing, product or service.

Section 200.11, "Change of control; mergers and acquisitions," requires licensees to seek prior approval by written application before executing a change of control or merger or acquisition.

Section 200.12, "Books and records," requires licensees to maintain certain records pertaining to each transaction and make such records available to the Department upon request.

Section 200.13, "Examinations," requires licensees to permit the superintendent to examine the licensee, including the licensee's books and records, at least once every two years and to make special investigations as deemed necessary by the superintendent.

Section 200.14, "Reports and financial disclosures," requires licensees to file quarterly financial statements and audited annual financial statements, to make special reports upon request, and to notify the Department upon discovery of any breach of law or upon a proposed change to the methodology used to calculate the value of virtual currency in fiat currency.

Section 200.15, "Anti-money laundering program," requires licensees to establish and implement an anti-money laundering program, which includes customer identification and transaction monitoring, to maintain records, and to make reports as required by applicable federal anti-money laundering law.

Section 200.16, "Cyber security program," requires licensees to design a cyber security program and written policy, designate a chief information security officer, make reports, and conduct audits.

Section 200.17, "Business continuity and disaster recovery," requires licensees to establish and maintain a written business continuity and disaster recovery plan to address disruptions to normal business operations.

Section 200.18, "Advertising and marketing," requires licensees to display a legend regarding its licensure by the Department, maintain all advertising and marketing materials, comply with all applicable federal and state disclosure requirements, and not make any false or misleading representations or omissions.

Section 200.19, "Consumer protection," requires licensees to disclose material risks and terms and conditions to customers and to establish an anti-fraud policy.

Section 200.20, "Complaints," requires licensees to disclose the licensee's and the Department's contact information and other information pertaining to the resolution of complaints.

Section 200.21, "Transitional period," requires Persons already engaged in virtual currency business activity to apply for a license with the Department within 45 days of the effective date of the regulation.

Text of proposed rule and any required statements and analyses may be obtained from: Office of General Counsel - Dana V. Syracuse, New York State Department of Financial Services, One State Street, New York, NY 10004, (212) 709-1663, email: dana.syracuse@dfs.ny.gov

Data, views or arguments may be submitted to: Same as above.

Public comment will be received until: 45 days after publication of this notice.

This rule was not under consideration at the time this agency submitted its Regulatory Agenda for publication in the Register.

Regulatory Impact Statement

1. Statutory Authority.

Section 102 of the Financial Services Law (FSL) states the legislature's

intent that the superintendent of Financial Services regulate "new financial services products," and "ensure the continued safety and soundness of New York's banking, insurance and financial services industries, as well as the prudent conduct of the providers of financial products and services, through responsible regulation and supervision." The definition of "financial product or service" in FSL section 104(a)(2) includes "any financial product or service offered or sold to consumers" other than those regulated under the exclusive jurisdiction of a federal or other New York state agency or where such regulation of such financial product or service would be preempted by federal law. Virtual currency meets the definition of "financial product or service," and is therefore subject to regulation by the superintendent.

Moreover, the superintendent has the explicit power under FSL section 301(c) "to protect users of financial products and services," and, under FSL section 302(a)(1), to "prescribe. . . rules and regulations. . . effectuating any power given to the superintendent under the provisions of this chapter." The superintendent therefore has statutory authority to prescribe regulations regarding virtual currency for the purpose of protecting users of virtual currency and virtual currency-related services.

Other statutory authority includes: Financial Services Law, sections 201, 202, 206, 302, 303, 304-a, 305, 306, 309, 404, 408; State Administrative Procedures Act, section 102; Banking Law, sections 10, 14, 36, 37, 39, 40, 44, 44-a, 78, 128, 225-a, 600, 601-a, 601-b; and Executive Law, section 63.

2. Legislative Objectives.

FSL section 201 is entitled "Declaration of policy" and states:

(a) It is the intent of the legislature that the superintendent shall supervise the business of, and the persons providing, financial products and services, including any persons subject to the provisions of the insurance law and the banking law.

(b) The superintendent shall take such actions as the superintendent believes necessary to:

(1) foster the growth of the financial industry in New York and spur state economic development through judicious regulation and vigilant supervision;

(2) ensure the continued solvency, safety, soundness and prudent conduct of the providers of financial products and services;

(3) ensure fair, timely and equitable fulfillment of the financial obligations of such providers;

(4) protect users of financial products and services from financially impaired or insolvent providers of such services;

(5) encourage high standards of honesty, transparency, fair business practices and public responsibility;

(6) eliminate financial fraud, other criminal abuse and unethical conduct in the industry; and

(7) educate and protect users of financial products and services and ensure that users are provided with timely and understandable information to make responsible decisions about financial products and services.

Virtual currency business activity is currently in its infancy and is almost entirely unregulated. The current lack of regulation, along with the dangers associated with virtual currency, may subject consumers and the businesses themselves to undue risk. The proposed regulation is intended to protect members of the public by imposing regulatory standards on virtual currency transactions and services that involve New York or New York residents, ensure the solvency, safety, soundness, and prudent conduct of persons or entities engaged in virtual currency business activity, and to foster the growth of the financial industry in New York by setting forth clear guidelines that will inspire confidence and allow for the establishment of legal virtual currency business activity.

3. Needs and Benefits.

Extensive research and analysis by the Department of Financial Services (the "Department"), including a two-day hearing held in January 2014, has made clear the need for a new and comprehensive set of regulations that address the novel aspects and risks of virtual currency. Existing laws and regulations do not cover proposed or current virtual currency business activity. The proposed regulation is therefore necessary to ensure that: (a) persons or entities engaged in virtual currency business activity operate in a safe and sound manner; (b) New York consumers and other residents are protected from the risks posed by virtual currency business activity; and (c) persons or entities engaged in new virtual currency business activity have a framework within which they can grow.

4. Costs.

Persons licensed under the proposed regulation will be responsible for ensuring that they are in compliance with this regulation, which will impose some costs on their operations. The Department will develop procedures to effectuate the licensing and examination of regulated persons or entities engaged in virtual currency business activity. In addition, the Department's operating expenses will be assessed in accordance with the provisions of FSL section 206. There should be no costs to any local governments as a result of the proposed regulation.

5. Local Government Mandates.

The proposed regulation does not impose any new programs, services, duties, or responsibilities upon any county, city, town, village, school district, fire district or other special district.

6. Paperwork.

Persons licensed under the proposed regulation will be required to keep and maintain books and records, make quarterly financial reports to the superintendent, and provide written applications for the initial license, and to seek approval for changes in control of, or material changes to, their businesses.

7. Duplication.

The proposed regulation does not duplicate, overlap, or conflict with any other regulations.

8. Alternatives.

The Department considered amending existing laws or regulations, particularly under the Banking Law, to include virtual currency. The Department decided not to pursue that alternative because of the widespread and potentially unforeseen ramifications such modification could have on the financial services industry and currently regulated entities. The Department also considered not acting at all, but concluded that failure to regulate virtual currency business activity will place the public at risk.

9. Federal Standards.

There are no applicable federal standards.

10. Compliance Schedule.

Persons or entities engaging in virtual currency business activity as of the effective date of the regulation must file an application for a license within 45 days of the effective date of the regulation.

Regulatory Flexibility Analysis

1. Effect of the rule.

Local governments do not engage in the virtual currency business activity covered by the proposed regulation. This regulation will not impose any adverse economic impact or any reporting, recordkeeping, or other compliance requirements on local governments. To the extent a small business engages in any of the conduct specified in the proposed regulation, it will be required to comply with the requirements of the regulation. At this time, because virtual currency technology is relatively new, there exists no comprehensive estimate of the number of small businesses in New York that would be impacted by the proposed regulation.

2. Compliance requirements.

Small businesses, like all businesses licensed under the proposed regulation, will be required to make quarterly financial reports to the superintendent of Financial Services, keep and maintain accurate books and records, be subject to examinations, and provide written applications for the initial license and to seek approval for changes in control or material changes to their businesses.

3. Professional services.

Small businesses, like all businesses licensed under the proposed regulation, will be required to satisfy an annual audit requirement, which will require the retention of qualified professionals to perform the audit.

4. Compliance costs.

Persons licensed under the proposed rule will be responsible for ensuring that they are in compliance with the regulation, which will impose some costs on their operations. Although the cost of compliance, particularly with regard to anti-money laundering and cyber security, could be significant for small businesses, the overwhelming need for such compliance to protect New York residents outweighs such costs. In addition, very few, if any, small businesses currently engage in the conduct that is subject to regulation under the proposed rule. For small businesses that do not engage in virtual currency business activity, the regulation will impose no adverse impact or increased costs.

5. Economic and technological feasibility.

The Department of Financial Services (the "Department") believes it will be economically and technologically feasible for small businesses to comply with the requirements of the proposed regulation.

6. Minimizing adverse impact.

To minimize any adverse economic impact of the proposed regulation on small businesses, the Department will adjust small businesses' capital requirements to reflect the size of their operations. Small businesses generally will have lower capital requirements than large businesses.

7. Small business participation.

The proposed regulation will be published publicly, including on the Department's website, for notice and comment, which will provide small businesses with the opportunity to participate in the rule making process. Further, prior to drafting this regulation the Department held a two day public hearing and sought input from dozens of virtual currency businesses, venture capital companies, and academics.

Rural Area Flexibility Analysis

1. Types and estimated numbers of rural areas.

Persons subject to the licensing requirements of the proposed regulation could possibly operate anywhere in this state, including rural areas.

2. Reporting, recordkeeping and other compliance requirements; and professional services.

Persons licensed under the proposed regulation will be will be required to make quarterly financial reports to the superintendent of Financial Services, keep and maintain accurate books and records, be subject to examinations, and must provide written applications for the initial license and to seek approval for changes in control or material changes to their businesses.

3. Costs.

Persons licensed under the proposed regulation will be responsible for ensuring that they are in compliance with this regulation, which will impose some costs on their operations. The costs are not expected to be any higher for entities in rural areas than for any other entity in the state.

4. Minimizing adverse impact.

The proposed regulation is not expected to have an adverse impact on public or private sector interests in rural areas. This regulation is specifically tailored to the pressing need to regulate virtual currency business activity involving New York or New York residents and is likely to have a positive impact on interests in rural areas by increasing the financial services available to them.

5. Rural area participation.

The proposed regulation will be published publicly, including on the Department's website, for notice and comment, which will provide public and private interests in rural areas with the opportunity to participate in rule making.

Job Impact Statement

A Job Impact Statement is not being submitted with this proposed regulation because it is evident from the subject matter of the regulation that it will not have an adverse impact on jobs and employment opportunities in New York State. The proposed regulation is intended to protect members of the public by imposing a regulatory framework on persons or entities that wish to engage in virtual currency business activity involving the State of New York or New York residents and to provide the market with guidance and clarity with regard to the use of virtual currency. Based on the feedback the Department of Financial Services (the "Department") has received from virtual currency businesses to date, the Department believes that the proposed regulation will have a positive impact on jobs and employment opportunities in New York by allowing for the establishment and growth of legitimate virtual currency businesses.

Department of Health

PROPOSED RULE MAKING
NO HEARING(S) SCHEDULED

State Aid for Public Health Services: Counties and Cities

I.D. No. HLT-29-14-00012-P

PURSUANT TO THE PROVISIONS OF THE State Administrative Procedure Act, NOTICE is hereby given of the following proposed rule:

Proposed Action: Repeal of Parts 39 and 40; and addition of new Part 40 to Title 10 NYCRR.

Statutory authority: Public Health Law, sections 201, 602, 603, 619, 2201, 2202 and 2276

Subject: State Aid for Public Health Services: Counties and Cities.

Purpose: To modernize certain regulations, including standards of performance for eligible public health services.

Substance of proposed rule (Full text is posted at the following State website: www.health.ny.gov): Article 6 of the Public Health Law (PHL) sets forth the statutory framework for the Departments' State Aid program, which partially reimburses local health departments (LHDs) for eligible expenses related to specified public health services. The objectives of these amendments is to conform the State Aid regulations to recent statutory changes to PHL Article 6; clarify, simplify, and reorganize all of the regulations; and to modernize certain regulations, including standards of performance for eligible public health services.

The Department does not expect the non-conformance amendments to result in any significant increased costs. The proposed regulations were developed with considerable input from New York State Association of County Officials (NYSACHO), through numerous meetings. NYSACHO has not indicated that these regulations, which aim to reduce administrative burdens on LHDs, will result in any significant increased costs.

The regulations implementing the State Aid program are set forth in 10 NYCRR Part 39 and Subparts 40-1 and 40-2. Part 39 and Subpart 40-1 establish the administrative aspects of State Aid, including the application and payment mechanisms. Subpart 40-2 establishes the standards of performance for eligible public health services.

These regulations repeal Part 39 and Subparts 40-1 and 40-2 in their entirety. New Subparts 40-1 and 40-2 are issued. The relevant provisions of Part 39 are incorporated into a new Subpart 40-1; accordingly, Part 39 is not being reissued.

With this in mind, these regulatory amendments can be organized into three categories:

- Conformance Changes, for changes necessary to conform the regulations to the recent statutory changes to Article 6 of the PHL;
- Non-conformance Changes – Administrative, for changes to the administrative aspects of State Aid, currently set forth in Part 39 and Subpart 40-1, and now provided solely in Subpart 40-1; and
- Non-conformance changes – Standards of Performance, for changes to the performance standards for core public health services, set forth in Subpart 40-2.

The conformance changes can be summarized as follows:

- All references to the "Municipal Public Health Services Plan" (MPHSP) and Fee and Revenue Plan are removed.
- The regulations describing the State Aid Application (SAA) are amended to reflect that the SAA is now comprised of the following sections: an organizational chart and list of the number of employees providing public health services; a proposed budget; a description of how the LHD will provide public health services; an attestation by the chief executive officer of the municipality that sufficient funds have been appropriated to provide public health services; an attestation by the public health commissioner or director that the LHD has exercised due diligence in reviewing the SAA and that the application seeks State Aid only for eligible public health services; a list of public health services provided by the LHD that are not eligible for State Aid; a projection of fees and revenues to be collected for public health services eligible for State Aid and any other information or documents required by the commissioner.
- The regulation describing the duties of the local commissioner of health or public health director is revised to reflect that such official may serve as the head of a merged agency or multiple agencies if approved by the commissioner, or serve as the local commissioner of health or public health director of additional counties when authorized pursuant to section 351 of the PHL.
- The definition of "maintenance of effort"—i.e., the funding level at which an LHD must maintain services—and the calculation of the penalty for failing to comply, have been simplified.
- Subpart 40-2, which provides the standards of performance for public health services required for State Aid eligibility, is updated to include the following six core public health services: Family Health, Communicable Disease Control, Chronic Disease Prevention, Community Health Assessment, Environmental Health, and Emergency Preparedness and Response. In particular, Chronic Disease Prevention and Emergency Preparedness, which had been a subset of "Disease Control", are now distinct core services. Public Health Education, which was a distinct core service, has been eliminated and the activities incorporated into each of the core services.

The non-conformance administrative changes to Subpart 40-1 involve significant simplification, clarification, and reorganization of all related provisions. For example, the existing sections relating to fees and revenues are updated and clarified. The regulations clarify that LHDs must make reasonable efforts to collect fees and revenue. The provisions setting forth the activities that are ineligible for State Aid is moved to Subpart 40-2, reorganized and clarified. These and other administrative changes to Subpart 40-1 are described in more detail in the Regulatory Impact Statement.

The non-conformance changes to the performance standards in Subpart 40-2 can be summarized as follows:

- The Family Health core service is amended to focus services in the following areas: Child Health, Maternal and Infant Health, and Reproductive Health sections.
- The requirements of the Chronic Disease Prevention core service are revised to focus LHDs on working with community partners to implement policy rather than on providing direct patient care.
- In the Communicable Disease Prevention core service, the section relating to General Communicable Disease control is amended to reflect best practices, which include requiring LHDs to provide communications to health care providers, clinics and laboratories on how to decrease the spread of communicable disease. The sections on Sexually Transmitted Diseases and Human Immunodeficiency Virus are consolidated.
- The Community Health Assessment section now requires LHDs to create a Community Health Improvement Plan.

Exhibit S

RULE MAKING ACTIVITIES

Each rule making is identified by an I.D. No., which consists of 13 characters. For example, the I.D. No. AAM-01-96-00001-E indicates the following:

AAM -the abbreviation to identify the adopting agency
01 -the *State Register* issue number
96 -the year
00001 -the Department of State number, assigned upon receipt of notice.
E -Emergency Rule Making—permanent action not intended (This character could also be: A for Adoption; P for Proposed Rule Making; RP for Revised Rule Making; EP for a combined Emergency and Proposed Rule Making; EA for an Emergency Rule Making that is permanent and does not expire 90 days after filing.)

Italics contained in text denote new material. Brackets indicate material to be deleted.

Department of Corrections and Community Supervision

PROPOSED RULE MAKING
NO HEARING(S) SCHEDULED

Rochester Correctional Facility

I.D. No. CCS-08-15-00002-P

PURSUANT TO THE PROVISIONS OF THE State Administrative Procedure Act, NOTICE is hereby given of the following proposed rule:

Proposed Action: This is a consensus rulemaking to amend section 100.92(a) of Title 7 NYCRR.

Statutory authority: Correction Law, section 70

Subject: Rochester Correctional Facility.

Purpose: To correct the address for Rochester Correctional Facility.

Text of proposed rule: Amend section 100.92 of 7 NYCRR, as follows:

(a) There shall be in the department a facility to be known as the Rochester Correctional Facility, which shall be located at Rochester, in Monroe County, New York, and which shall consist of the land and buildings at *470 Ford Street* [55 Greig Street], formerly occupied by a Division for Youth center.

(b) Rochester Correctional Facility shall be a correctional facility for males of the age of 16 years or older.

(c) Rochester Correctional Facility shall be classified as a minimum security correctional facility, to be used for the following functions:

(1) residential treatment facility; and

(2) work release facility.

Text of proposed rule and any required statements and analyses may be obtained from: Kevin Bruen, Deputy Commissioner and Counsel, NYS Department of Corrections and Community Supervision, 1220 Washington Avenue - Harriman State Campus - Building 2, Albany, NY 12226-2050, (518) 457-4951, email: Rules@Doccs.ny.gov

Data, views or arguments may be submitted to: Same as above.

Public comment will be received until: 45 days after publication of this notice.

Consensus Rule Making Determination

The Department of Correctional and Community Supervision (DOCCS) has determined that no person is likely to object to the proposed action. The amendment of this section corrects the address of Rochester Correctional Facility. The street where the original front entrance to the facility was located has been closed. A new front entrance has been located on an adjacent street and a new address was assigned. See SAPA Section 102(11)(a).

The Department's authority resides in section 70 of Correction Law, which mandates that each correctional facility must be designated in the rules and regulations of the Department and assigns the Commissioner the duty to classify each facility with respect to the type of security maintained and the function as specified. See Correction Law § 70(6).

Job Impact Statement

A job impact statement is not submitted because this proposed rulemaking will merely correct the address for Rochester Correctional Facility. This has no adverse impact on jobs or employment opportunities. Additionally, there is no adverse impact on jobs or employment.

Education Department

EMERGENCY
RULE MAKING

New York State Common Core Learning Standards (CCLS) in Mathematics

I.D. No. EDU-48-14-00007-E
Filing No. 101
Filing Date: 2015-02-10
Effective Date: 2015-02-14

PURSUANT TO THE PROVISIONS OF THE State Administrative Procedure Act, NOTICE is hereby given of the following action:

Action taken: Amendment of section 100.5(g)(1)(ii)(*a*) of Title 8 NYCRR.

Statutory authority: Education Law, sections 101(not subdivided), 207(not subdivided), 208(not subdivided), 209(not subdivided), 305(1), (2), 308(not subdivided), 309(not subdivided) and 3204(3)

Finding of necessity for emergency rule: Preservation of general welfare.

Specific reasons underlying the finding of necessity: The proposed amendment is necessary to implement Regents policy to provide additional flexibility in the transition to the Common Core Regents Examination in Algebra I by allowing, at the local school district's discretion, an additional opportunity for certain specified students to take the Regents Examination in Integrated Algebra in addition to the Regents examination in Algebra I (Common Core) at the June 2015 test administration, and meet the mathematics requirement for graduation by passing either examination.

The proposed amendment was adopted by emergency action at the November 17-18, 2014 Regents meeting, effective November 18, 2014. A Notice of Emergency Adoption and Proposed Rule Making was published in the State Register on December 3, 2014.

Subsequently, the proposed amendment was revised to clarify, consis-

NOTICE OF ADOPTION

New York State Common Core Learning Standards (CCLS) in Mathematics

I.D. No. EDU-48-14-00007-A
Filing No. 100
Filing Date: 2015-02-10
Effective Date: 2015-02-25

PURSUANT TO THE PROVISIONS OF THE State Administrative Procedure Act, NOTICE is hereby given of the following action:

Action taken: Amendment of section 100.5(g)(1)(ii)(*a*) of Title 8 NYCRR.

Statutory authority: Education Law, sections 101(not subdivided), 207(not subdivided), 208(not subdivided), 209(not subdivided), 305(1), (2), 308(not subdivided), 309(not subdivided) and 3204(3)

Subject: New York State Common Core Learning Standards (CCLS) in mathematics.

Purpose: To provide additional flexibility in the transition to the Common Core-Aligned Regents Examination in Algebra I by allowing, at the discretion of the local school district, students receiving Algebra I (common core) instruction to take the Regents Examination in Integrated Algebra in addition to the Regents examination in Algebra I (common core) at the June 2015 test administration, and meet the requirement for graduation by passing either examination.

Text or summary was published in the December 3, 2014 issue of the Register, I.D. No. EDU-48-14-00007-EP.

Final rule as compared with last published rule: No changes.

Text of rule and any required statements and analyses may be obtained from: Kirti Goswami, State Education Department, Office of Counsel, State Education Building, Room 148, 89 Washington Ave., Albany, NY 12234, (518) 474-6400, email: legal@nysed.gov

Initial Review of Rule

As a rule that requires a RFA, RAFA or JIS, this rule will be initially reviewed in the calendar year 2020, which is the 4th or 5th year after the year in which this rule is being adopted. This review period, justification for proposing same, and invitation for public comment thereon, were contained in a RFA, RAFA or JIS.

An assessment of public comment on the 4 or 5-year initial review period is not attached because no comments were received on the issue.

Assessment of Public Comment

Since publication of a Notice of Emergency Adoption and Proposed Rule Making in the State Register on December 3, 2014, the State Education Department received the following comments:

1. COMMENT:

The proposed rule appears to suggest that 9th and 10th graders will have the opportunity to take the Integrated Algebra Regents in June 2015 because both started high school with Algebra I Common Core Math. Can 11th and 12th graders who have not passed the Integrated Algebra Regents exam sit for these Regents also, even though they did not start with Algebra I Common Core Math?

DEPARTMENT RESPONSE:

All students who began their first commencement-level course of study in algebra (2005 standard) prior to September 2013 and who have completed that course of study, albeit successfully or not, are eligible to participate in the June 2015 Regents Examination in Integrated Algebra.

NOTICE OF ADOPTION

Professional Development Requirements for Teachers, Level III Teaching Assistants and Administrators

I.D. No. EDU-48-14-00009-A
Filing No. 102
Filing Date: 2015-02-10
Effective Date: 2015-02-25

PURSUANT TO THE PROVISIONS OF THE State Administrative Procedure Act, NOTICE is hereby given of the following action:

Action taken: Amendment of sections 80-3.6, 100.2 and 154-2.3 of Title 8 NYCRR.

Statutory authority: Education Law, sections 207(not subdivided), 215(not subdivided), 305(1), (2), 2117(1), 3001(2), 3003(1), 3004(1), 3006(1)(b) and 3009(1)

Subject: Professional development requirements for teachers, level III teaching assistants and administrators.

Purpose: To establish professional development requirements for teachers, holders of a level III teaching assistant certificate, and administrators, in language acquisition that specifically addresses the needs of students who are English Language Learners (ELLs) and integrating language and content instruction for such ELL students.

Text or summary was published in the December 3, 2014 issue of the Register, I.D. No. EDU-48-14-00009-P.

Final rule as compared with last published rule: No changes.

Text of rule and any required statements and analyses may be obtained from: Kirti Goswami, State Education Department, Office of Counsel, State Education Building, Room 148, 89 Washington Ave., Albany, NY 12234, (518) 474-6400, email: legal@mail.nysed.gov

Initial Review of Rule

As a rule that requires a RFA, RAFA or JIS, this rule will be initially reviewed in the calendar year 2020, which is the 4th or 5th year after the year in which this rule is being adopted. This review period, justification for proposing same, and invitation for public comment thereon, were contained in a RFA, RAFA or JIS.

An assessment of public comment on the 4 or 5-year initial review period is not attached because no comments were received on the issue.

Assessment of Public Comment

COMMENT: One comment expressed concern about certificate holders who are not employed by a public school in New York State. The commenter indicated that while it is easy for teachers in public schools to meet the professional development requirements, private schools and out of state schools are not subject to these requirements. The commenter has asked that we revisit the requirements for certificate holders working in private or an out of state school and either modify or eliminate the requirements for those teachers.

RESPONSE: Section 80-3.6(b)(2) of the Commissioner's regulations already provides for a 10% adjustment of the professional development requirement per year for a certificate holder that is not regularly employed in a public school in New York. This adjustment will also apply to the minimum professional development requirements in language acquisition for English language learners, as added under the proposed amendment. In an effort to ensure the quality of teaching and learning by ensuring that teachers participate in professional development in order to remain current with their profession, the Department does not believe any further changes are needed.

Department of Financial Services

EMERGENCY RULE MAKING

Unfair Claims Settlement Practices and Claim Cost Control Measures

I.D. No. DFS-08-15-00001-E
Filing No. 97
Filing Date: 2015-02-04
Effective Date: 2015-02-04

PURSUANT TO THE PROVISIONS OF THE State Administrative Procedure Act, NOTICE is hereby given of the following action:

Action taken: Amendment of Part 216 (Regulation 64) of Title 11 NYCRR.

Statutory authority: Financial Services Law, sections 202 and 302; Insurance Law, sections 301 and 2601

Finding of necessity for emergency rule: Preservation of public health, public safety and general welfare.

Specific reasons underlying the finding of necessity: Insurance Law § 2601 prohibits an insurer doing business in New York State from engaging in unfair claims settlement practices and sets forth a list of acts that, if committed without just cause and performed with such frequency as to indicate a general business practice, will constitute unfair claims settlement practices. Insurance Regulation 64 sets forth the standards insurers are expected to observe to settle claims properly.

On October 26, 2012, in anticipation of extensive power outages, loss of life and property, and ongoing harm to public health and safety expected to result from then-Hurricane Sandy, Governor Andrew M. Cuomo issued Executive Order 47, declaring a State of Disaster Emergency for all 62

tered in rural areas, because they will need to pay the costs of mediation and provide representatives to send to the mediations. However, by providing an alternative to litigation, the insurers may also realize savings from mediations that result in settlements because the cost to mediate a claim is significantly less than the cost to defend against civil litigation brought by insureds. The actual cost effect of the rule is difficult to quantify because it is dependent upon unknown variables such as how many claims will be subject to litigation, how many insureds will select the mediation option, and how many claims that are mediated will be successfully resolved without the insured resorting to litigation. Nothing in this rule requires insurers to reach a settlement in the course of a mediation.

4. Minimizing adverse impact: The Department considered the approaches suggested in SAPA § 202-bb(2) for minimizing adverse economic impacts. Because the public health, safety, or general welfare has been endangered, establishment of differing compliance or reporting requirements or timetables based upon whether or not the damage occurred in a rural area is not appropriate. However, the rule applies only in the counties of New York, Bronx, Kings, Richmond, Queens, Nassau, Suffolk, Westchester, Rockland, and Orange, the areas that suffered the greatest storm damage, and thus the impact of the rule on rural areas is minimized, since none of those counties are rural areas.

5. Rural area participation: Public and private interests in rural areas have had a continual opportunity to participate in the rule making process since the first publication of the emergency measure in the State Register on March 13, 2013, which was published again in the State Register on November 26, 2014. The emergency measure also has been posted on the Department's website continually since March 13, 2013.

Job Impact Statement

The Department of Financial Services does not believe that this rule will have any adverse impact on jobs or employment opportunities, including self-employment opportunities. This rule provides insureds with open or denied claims for loss or damage to personal and real property, except damage to automobiles, arising in New York, Bronx, Kings, Richmond, Queens, Nassau, Suffolk, Westchester, Rockland, and Orange counties between October 26, 2012 and November 15, 2012, with an option to participate in a mediation program to facilitate the negotiation of their claims with their insurers.

REVISED RULE MAKING NO HEARING(S) SCHEDULED

Regulation of the Conduct of Virtual Currency Businesses

I.D. No. DFS-29-14-00015-RP

PURSUANT TO THE PROVISIONS OF THE State Administrative Procedure Act, NOTICE is hereby given of the following revised rule:

Proposed Action: Addition of Part 200 to Title 23 NYCRR.

Statutory authority: Financial Services Law, sections 102, 104, 201, 206, 301, 302, 309 and 408

Subject: Regulation of the conduct of virtual currency businesses.

Purpose: To regulate virtual currency businesses to ensure the protection of New York consumers and to ensure the safety and soundness of providers of virtual currency products and services. The Department of Financial Services proposes this regulation as a complement to its Order of March 11, 2014, which provides for the regulation, pursuant to the Banking Law, of exchanges that exercise fiduciary powers.

Substance of revised rule: The following is a summary of the proposed regulation:

Section 200.1, "Introduction," sets forth the statutory authority for the rule.

Section 200.2, "Definitions," defines terms used throughout the proposed regulation. Most significantly this Section defines "virtual currency" and "virtual currency business activity" and specifies conduct that is not covered by the proposed regulation.

Section 200.3, "License," prohibits any Person from engaging in virtual currency business activity without a license.

Section 200.4, "Application," sets forth the information to be included in a prospective licensee's application and provides for the granting of a conditional license, in certain circumstances.

Section 200.5, "Application fees," requires applicants to pay an application fee of $5000.00 to the Department of Financial Services (the "Department") and provides that licensees may need to pay fees for the processing of additional applications related to the license.

Section 200.6, "Action by superintendent," provides for the superintendent to approve or deny an application and, if approved, to suspend or revoke a license on specified grounds after a hearing.

Section 200.7, "Compliance," requires licensees to comply with all applicable federal and state law, designate a compliance officer, and maintain and enforce various written compliance policies.

Section 200.8, "Capital requirements," requires that licensees maintain minimum amounts of capital as determined by the superintendent based on a number of factors.

Section 200.9, "Custody and protection of customer assets," requires licensees to establish a bond or trust account for the benefit of their customers, requires licensees to hold virtual currency in the same type and amount as any virtual currency owed by the licensee, and prohibits licensees from encumbering customer assets.

Section 200.10, "Material change to business," requires licensees to seek prior approval by written application to introduce a new, or materially change an existing, product or service.

Section 200.11, "Change of control; mergers and acquisitions," requires licensees to seek prior approval by written application before executing a change of control or merger or acquisition.

Section 200.12, "Books and records," requires licensees to maintain certain records pertaining to each transaction and make such records available to the Department upon request.

Section 200.13, "Examinations," requires licensees to permit the superintendent to examine the licensee, including the licensee's books and records, at least once every two years and to make special investigations as deemed necessary by the superintendent.

Section 200.14, "Reports and financial disclosures," requires licensees to file quarterly financial statements and audited annual financial statements, to make special reports upon request, and to notify the Department upon discovery of any breach of law or upon a proposed change to the methodology used to calculate the value of virtual currency in fiat currency.

Section 200.15, "Anti-money laundering program," requires licensees to establish and implement an anti-money laundering program, which includes customer identification and transaction monitoring, to maintain records, and to make reports as required by applicable federal anti-money laundering law.

Section 200.16, "Cyber security program," requires licensees to design a cyber security program and written policy, designate a chief information security officer, make reports, and conduct audits.

Section 200.17, "Business continuity and disaster recovery," requires licensees to establish and maintain a written business continuity and disaster recovery plan to address disruptions to normal business operations.

Section 200.18, "Advertising and marketing," requires licensees to display a legend regarding its licensure by the Department, maintain all advertising and marketing materials, comply with all applicable federal and state disclosure requirements, and not make any false or misleading representations or omissions.

Section 200.19, "Consumer protection," requires licensees to disclose material risks and terms and conditions to customers and to establish an anti-fraud policy.

Section 200.20, "Complaints," requires licensees to disclose the licensee's and the Department's contact information and other information pertaining to the resolution of complaints.

Section 200.21, "Transitional period," requires Persons already engaged in virtual currency business activity to apply for a license with the Department within 45 days of the effective date of the regulation.

Section 200.22, "Severability," states that in the event a specific provision of the regulation is adjudged invalid, such judgment will not impair the validity of the remainder of the regulation.

Revised rule compared with proposed rule: Substantive revisions were made in sections 200.2, 200.3, 200.4, 200.5, 200.6, 200.8, 200.9, 200.10, 200.11, 200.12, 200.13, 200.14, 200.15, 200.16, 200.18, 200.19, 200.21 and 200.22.

Text of revised proposed rule and any required statements and analyses may be obtained from Office of General Counsel - Dana V. Syracuse, New York State Department of Financial Services, One State Street, New York, NY 10004, (212) 709-1663, email: VCRegComments@dfs.ny.gov

Data, views or arguments may be submitted to: Same as above.

Public comment will be received until: 30 days after publication of this notice.

Revised Regulatory Impact Statement, Regulatory Flexibility Analysis, Rural Area Flexibility Analysis and Job Impact Statement

A Revised Regulatory Impact Statement, Regulatory Flexibility Analysis, Rural Area Flexibility Analysis and Job Impact Statement is not required because the revisions to the proposed regulation do not change the conclusions set forth in the previously published Regulatory Impact Statement, Regulatory Flexibility Analysis, Rural Area Flexibility Analysis and Job Impact Statement.

Assessment of Public Comment

The New York State Department of Financial Services (the "Department") received over 3000 comments on proposed rule 23 NYCRR 200

from virtual currency businesses, other financial services businesses, merchants, retailers, researchers, academics, policy centers, governmental agencies, and private individuals. Many commenters addressed more than one provision of the proposed regulation, and several requested specific changes. Every comment has been processed and considered by the Department, as reflected in the full text of the Assessment of Public Comment, which is available at www.dfs.ny.gov. This summary is intended to provide an overview of the categories of comments received by the Department and the changes the Department has made to the proposed regulation in response to those comments.

Many comments requested clarification over who is, and is not, required to obtain a virtual currency license. Several of those commenters requested that the Department specify that certain activities, such as software development, non-financial uses of virtual currency technology, and investment in virtual currency, and certain programs, such as gift cards and customer loyalty programs, are exempt from the regulation. The Department has revised the definitions of virtual currency and virtual currency business activity accordingly to exclude certain activities and programs. In particular, the Department has clarified that virtual currency business activity does not include transactions that are undertaken for non-financial purposes and that do not involve the transfer of more than a nominal amount of virtual currency, and that virtual currency does not include digital units used in gift cards. The Department has also revised the regulation to clarify that the development and dissemination of software in and of itself does not constitute virtual currency business activity. (Section 200.2)

The Department also received many comments requesting an on-ramp or more flexible set of licensing requirements for small and start-up businesses. The Department has addressed those comments by providing that the superintendent may grant a conditional license to conduct virtual currency business activity. The Department set forth in the revised proposed regulation a list of factors that the superintendent may consider in determining whether to issue or renew a conditional license. (Section 200.4)

Commenters also requested that the Department set forth the fee that applicants will be required to pay for a virtual currency license. The revised proposed regulation sets the fee at $5000.00. (Section 200.5)

Another large source of comment related to the capital requirements set forth in the proposed regulation. The Department considered those comments and revised the requirements to allow licensees to hold capital in the form of cash, virtual currency, and high quality, highly liquid, investment-grade assets in a proportion that is acceptable to the superintendent. (Section 200.8)

Some commenters expressed concern that requiring the superintendent's approval prior to permitting changes in control could limit start-up firms' ability to attract investors and raise capital. To address that concern, the Department revised the regulation to provide licensees with the ability to apply for a determination that a given party will not be considered a control party by the Department, based on several factors relating to the party's ability to manage or exercise control over the licensee. (Section 200.11)

Several commenters also requested that the Department reduce the burden associated with the proposed regulation's recordkeeping requirements. In response, the Department revised the proposed regulation to reduce the recordkeeping requirement from ten years to seven years (Section 200.12) and require that licensees maintain, only to the extent practicable, specific identifying information regarding parties to the transaction that are not customers or accountholders of the licensee. (Sections 200.12 and 200.15)

The Department also received comments requesting that the regulations include more detail in certain areas, including the addition of specific formulas for setting capital requirements and further technical specifications with respect to cyber security. The Department has considered those comments but has concluded that the factors and principles set forth in the proposed regulation provide the appropriate level of specificity.

While a number of commenters expressed support for the proposed regulation, others rejected the regulation in its entirety, stating that virtual currency should be regulated under existing money transmission law or not at all. The Department has extensively considered the need to regulate virtual currency business activity and the appropriate way to do so, and it has concluded that a new regulation under the Financial Services Law is necessary to protect New York consumers and users of virtual currency-related services.

Similarly, some commenters called for the Department to heighten the proposed regulations and add to it new requirements, while others contested the need for regulatory requirements relating to money laundering, cyber security, and recordkeeping, among other specific provisions. The Department has considered both sets of comments and has determined that the proposed regulation adequately addresses the risks associated with virtual currency business activity.

Department of Health

EMERGENCY/PROPOSED RULE MAKING NO HEARING(S) SCHEDULED

Opioid Overdose Programs

I.D. No. HLT-08-15-00005-EP
Filing No. 99
Filing Date: 2015-02-06
Effective Date: 2015-02-06

PURSUANT TO THE PROVISIONS OF THE State Administrative Procedure Act, NOTICE is hereby given of the following action:

Proposed Action: Amendment of section 80.138 of Title 10 NYCRR.

Statutory authority: Public Health Law, section 3309

Finding of necessity for emergency rule: Preservation of public health.

Specific reasons underlying the finding of necessity: The regulatory revisions are necessary for emergency implementation to safeguard the lives and well-being of New Yorkers who are otherwise at increasing risk for opioid-associated harm including death.

In New York State substantial mortality is associated with opioids. In 2012, there were 875 deaths where the toxicology reports indicated opioid analgesics. In addition, 478 overdose deaths occurred that year associated with heroin and 150 deaths for which the toxicology report indicated an unspecified opioid. The heroin-related deaths for 2012 represent an almost-threefold increase from two years earlier. Although there are not yet consolidated reports for more recent years, there is reason to believe, based on information shared by local jurisdictions as well as from legislative hearings, that this trend has not only continued, but has grown at an alarming rate.

Similarly, costly hospitalizations in which opioids have been identified among the diagnostic codes have risen substantially. In 2012, there were more than 75,000 hospital discharges in which opioids were identified. This is an increase of approximately 4,000 from four years earlier. Although a broad range of opioid-related diagnoses is represented in these figures, they indicate the growing problem associated with this class of drugs.

There is a broad-based interest in—and commitment to—resolving New York State's opioid crisis. Part of that response includes providing law enforcement and firefighting personnel with the training and the naloxone necessary to save lives when they are the first to arrive on the scene of a suspected overdose. The Division of Criminal Justice Services, working with the Department of Health, Albany Medical Center, the Harm Reduction Coalition, local health departments and other community partners has initiated training of law enforcement officers, with a goal of 5,000 trained in the first year. There have been immediate benefits from these trainings, including overdose reversals successfully carried out within hours of a training. This initiative is currently severely hampered in its implementation by a requirement that each officer have his or her own rescue kit and that the officer cannot share it with colleagues. The revised regulation will address that. The revised regulation allowing for non-patient specific prescriptions of naloxone—something now authorized under the law—will eliminate the de facto requirement that prescribers be physically present every time that naloxone is furnished or dispensed. This will provide immediate relief not only in training public safety personnel, but also for more community-oriented programs, in which prescriber availability is extremely limited.

Subject: Opioid Overdose Programs.

Purpose: Modification of the rule consistent with new statutory language and with the emergency nature of opioid overdose response.

Substance of emergency/proposed rule (Full text is posted at the following State website:www.health.ny.gov): The regulatory changes accomplish the following:

- authorize clinical directors and affiliated prescribers to prescribe an opioid antagonist to trained overdose responders, and for those prescriptions to be either patient-specific or non-patient-specific;
- require clinical directors to designate those individuals by name or by description who will be furnishing or dispensing naloxone pursuant to a non-patient specific prescription;
- allow for trained overdose responders to have shared access to, and use of, an opioid antagonist so long as the following conditions are met:

Exhibit T

RULE MAKING ACTIVITIES

Each rule making is identified by an I.D. No., which consists of 13 characters. For example, the I.D. No. AAM-01-96-00001-E indicates the following:

AAM -the abbreviation to identify the adopting agency
01 -the *State Register* issue number
96 -the year
00001 -the Department of State number, assigned upon receipt of notice.
E -Emergency Rule Making—permanent action not intended (This character could also be: A for Adoption; P for Proposed Rule Making; RP for Revised Rule Making; EP for a combined Emergency and Proposed Rule Making; EA for an Emergency Rule Making that is permanent and does not expire 90 days after filing.)

Italics contained in text denote new material. Brackets indicate material to be deleted.

Department of Agriculture and Markets

NOTICE OF ADOPTION

Incorporation by Reference of the 2013 Edition of the Grade A Pasteurized Milk Ordinance (''PMO'')

I.D. No. AAM-05-15-00002-A
Filing No. 462
Filing Date: 2015-06-05
Effective Date: 2015-06-24

PURSUANT TO THE PROVISIONS OF THE State Administrative Procedure Act, NOTICE is hereby given of the following action:

Action taken: Amendment of section 2.1 of Title 1 NYCRR.

Statutory authority: Agriculture and Markets Law, sections 16, 18, 46, 46-a, 50-k, 71-a, 71-n and 214.6

Subject: Incorporation by reference of the 2013 edition of the Grade A Pasteurized Milk Ordinance (''PMO'').

Purpose: To require certain producers, processors and manufacturers of milk and milk products to comply with the 2013 edition of the PMO.

Text of final rule: Paragraph (1) of subdivision (b) of section 2.1 of 1 NYCRR is amended to read as follows:

(1) The sanitation provisions of this Part shall not apply to dairy farms or dairy farmers, or to milk plants and persons who operate milk plants, that have a sanitation compliance rating of 90 or better, as set forth in the latest Sanitation Compliance and Enforcement Ratings of interstate milk shippers list (IMS List), except as set forth in paragraph (2) of this subdivision. Dairy farms and dairy farmers, and milk plants and persons who operate milk plants, that have such a sanitation compliance rating shall comply with the sanitation requirements set forth in the Grade A Pasteurized Milk Ordinance, [2011] *2013* edition, published by the United States Department of Health and Human Services, Washington, DC (PMO) except to the extent that any provision of the PMO is in conflict with a provision of State and/or Federal law and except as provided in paragraph (2) of this subdivision. A copy of the PMO is available for public inspection at the Division of Milk Control and Dairy Services, Department of Agriculture and Markets, 10B Airline Drive, Albany, NY 12235, and at the Department of State, [41 State Street] *99 Washington Avenue*, Albany, NY 12231.

Subdivision (c) of section 2.1 of 1 NYCRR is amended to read as follows:

(c) Every term used in subdivision (b) of this section that is defined in the Grade A Pasteurized Milk Ordinance, [2011] *2013* edition, shall have the meaning ascribed to such term therein.

Final rule as compared with last published rule: Nonsubstantive changes were made in section 2.1(b)(1).

Text of rule and any required statements and analyses may be obtained from: Casey McCue, Director, Division of Milk Control, NYS Dept. of Agriculture and Markets, 10B Airline Drive, Albany, NY 12235, (518) 457-1772, email: Casey.McCue@agriculture.ny.gov

Revised Job Impact Statement

The express terms of the proposed rule were changed to provide that a copy of the 2013 edition of the Pasteurized Milk Ordinance, incorporated by reference in 1 NYCRR section 2.1(b)(1), is available at the Department of State's current address, i.e., 99 Washington Avenue, Albany, New York 12231. As such, the change made to the last published rule does not necessitate that the previously published statement in lieu of job impact statement be revised.

Assessment of Public Comment

The agency received no public comment.

Office of Children and Family Services

PROPOSED RULE MAKING
NO HEARING(S) SCHEDULED

Expansion of the Business Enterprise Program Priority in Accordance with Chapter 532 of the Laws of 2010

I.D. No. CFS-25-15-00004-P

PURSUANT TO THE PROVISIONS OF THE State Administrative Procedure Act, NOTICE is hereby given of the following proposed rule:

Proposed Action: Amendment of sections 729.1, 729.2(b), (e), 729.18, 729.19 and 729.20(b) of Title 18 NYCRR.

Statutory authority: Social Services Law, sections 20, 34 and 38; Unconsolidated Law, section 8714-a

Subject: Expansion of the Business Enterprise Program priority in accordance with chapter 532 of the Laws of 2010.

Purpose: To allow the Business Enterprise Program to expand opportunities for employment of blind and visually impaired individuals.

Substance of proposed rule (Full text is posted at the following State website:http://ocfs.ny.gov): Amendment of 18 NYCRR Part 729

Section 729.1 of Title 18 is amended pursuant to Chapter 532 of the

nesses and facilities, and describing key provisions of the START-UP NY program.

NEEDS AND BENEFITS:

The emergency rule is necessary in order to implement the statute contained in Article 21 of the Economic Development Law, creating the START-UP NY program. The statute directs the Commissioner of Economic Development to establish procedures for the implementation and execution of the START-UP NY program.

Upstate New York has faced longstanding economic challenges due in part to the departure of major business actors from the region. This divestment from upstate New York has left the economic potential of the region unrealized, and left many upstate New Yorkers unemployed.

START-UP NY will promote economic development and job creation in New York, particularly the upstate region, through tax benefits conditioned on locating business facilities in Tax-Free NY Areas. Attracting start-ups and high-tech industries is critical to restoring the economy of upstate New York, and to positioning the state as a whole to be competitive in a globalized economy. These goals cannot be achieved without first establishing procedures by which to admit businesses into the START-UP NY program.

The proposed regulation establishes procedures and standards for the implementation of the START-UP program, especially rules for the creation of Tax-Free NY Areas, application procedures for the admission of businesses into the program, and eligibility requirements for continued receipt of START-UP NY benefits for admitted businesses. These rules allow for the prompt and efficient commencement of the START-UP NY program, ensure accountability of business participants, and promote the general welfare of New Yorkers.

COSTS:

I. Costs to private regulated parties (the business applicants): None. The proposed regulation will not impose any additional costs to eligible business applicants.

II. Costs to the regulating agency for the implementation and continued administration of the rule: None.

III. Costs to the State government: None.

IV. Costs to local governments: None.

LOCAL GOVERNMENT MANDATES:

The rule establishes certain property tax benefits for businesses locating in Tax-Free NY Areas that may impact local governments. However, as described in the accompanying statement in lieu of a regulatory flexibility analysis for small businesses and local governments, the program is expected to have a net-positive impact on local government.

PAPERWORK:

The rule establishes application and eligibility requirements for Tax-Free NY Areas proposed by universities and colleges, and participating businesses. These regulations establish paperwork burdens that include materials to be submitted as part of applications, documents that must be submitted to maintain eligibility, and information that must be retained for auditing purposes.

DUPLICATION:

The proposed rule will create a new section of the existing regulations of the Commissioner of Economic Development, Part 220 of 5 NYCRR. Accordingly, there is no risk of duplication in the adoption of the proposed rule.

ALTERNATIVES:

No alternatives were considered in regard to creating a new regulation in response to the statutory requirement. The regulation implements the statutory requirements of the START-UP NY program regarding the application process for creation of Tax-Free NY Areas and certification as an eligible business. This action is necessary in order to clarify program participation requirements and is required by the legislation establishing the START-UP NY program.

FEDERAL STANDARDS:

There are no federal standards applicable to the START-UP NY program; it is purely a State program that offers tax benefits to eligible businesses and their employees. Therefore, the proposed rule does not exceed any federal standard.

COMPLIANCE SCHEDULE:

The affected State agency (Department of Economic Development) and the business applicants will be able to achieve compliance with the regulation as soon as it is implemented.

Regulatory Flexibility Analysis

Participation in the START-UP NY program is entirely at the discretion of qualifying business that may choose to locate in Tax-Free NY Areas. Neither statute nor the proposed regulations impose any obligation on any business entity to participate in the program. Rather than impose burdens on small business, the program is designed to provide substantial tax benefits to start-up businesses locating in New York, while providing protections to existing businesses against the threat of tax-privileged start-up companies locating in the same community. Local governments may not be able to collect tax revenues from businesses locating in certain Tax-Free NY Areas. However, the regulation is expected to have a net-positive impact on local governments in light of the substantial economic activity associated with businesses locating their facilities in these communities.

Because it is evident from the nature of the proposed rule that it will have a net-positive impact on small businesses and local government, no further affirmative steps were needed to ascertain that fact and none were taken. Accordingly, a regulatory flexibility analysis for small businesses and local government is not required and one has not been prepared.

Rural Area Flexibility Analysis

The START-UP NY program is open to participation from any business that meets the eligibility requirements, and is organized as a corporation, partnership, limited liability company, or sole proprietorship. A business's decision to locate its facilities in a Tax-Free NY Area associated with a rural university or college would be no impediment to participation; in fact, START-UP NY allocates space for Tax-Free NY Areas specifically to the upstate region which contains many of New York's rural areas. Furthermore, START-UP NY specifically calls for the balanced allocation of space for Tax-Free NY Areas between eligible rural, urban, and suburban areas in the state. Thus, the regulation will not have a substantial adverse economic impact on rural areas, and instead has the potential to generate significant economic activity in upstate rural areas designated as Tax-Free NY Areas. Accordingly, a rural flexibility analysis is not required and one has not been prepared.

Job Impact Statement

The regulation establishes procedures and standards for the administration of the START-UP NY program. START-UP NY creates tax-free areas designed to attract innovative start-ups and high-tech industries to New York so as to stimulate economic activity and create jobs. The regulation will not have a substantial adverse impact on jobs and employment opportunities; rather, the program is focused on creating jobs. Because it is evident from the nature of the rulemaking that it will have either no impact or a positive impact on job and employment opportunities, no further affirmative steps were needed to ascertain that fact and none were taken. Accordingly, a job impact statement is not required and one has not been prepared.

Department of Financial Services

NOTICE OF ADOPTION

Regulation of the Conduct of Virtual Currency Businesses

I.D. No. DFS-29-14-00015-A

Filing No. 505

Filing Date: 2015-06-10

Effective Date: 2015-06-24

PURSUANT TO THE PROVISIONS OF THE State Administrative Procedure Act, NOTICE is hereby given of the following action:

Action taken: Addition of Part 200 to Title 23 NYCRR.

Statutory authority: Financial Services Law, sections 102, 104, 201, 202, 206, 301, 302, 303, 304-a, 305, 306, 309, 404 and 408; Banking Law, sections 10, 14, 36, 37, 39, 40, 44, 44-a, 78, 128, 225-a, 600, 601-a and 601-b; and Executive Law, section 63

Subject: Regulation of the conduct of virtual currency businesses.

Purpose: Regulate retail-facing virtual currency business activity in order to protect New York consumers and users and ensure the safety and soundness of New York licensed providers of virtual currency products and services.

Substance of final rule: The following is a summary of the proposed regulation:

Section 200.1, "Introduction," sets forth the statutory authority for the rule.

Section 200.2, "Definitions," defines terms used throughout the proposed regulation. Most significantly this Section defines "virtual currency" and "virtual currency business activity" and specifies conduct that is not covered by the proposed regulation.

Section 200.3, "License," prohibits any Person from engaging in virtual currency business activity without a license.

Section 200.4, "Application," sets forth the information to be included

in a prospective licensee's application and provides for the granting of a conditional license, in certain circumstances.

Section 200.5, "Application fees," requires applicants to pay an application fee of $5000.00 to the Department of Financial Services (the "Department") and provides that licensees may need to pay fees for the processing of additional applications related to the license.

Section 200.6, "Action by superintendent," provides for the superintendent to approve or deny an application and, if approved, to suspend or revoke a license on specified grounds after a hearing.

Section 200.7, "Compliance," requires licensees to comply with all applicable federal and state law, designate a compliance officer, and maintain and enforce various written compliance policies.

Section 200.8, "Capital requirements," requires that licensees maintain minimum amounts of capital as determined by the superintendent based on a number of factors.

Section 200.9, "Custody and protection of customer assets," requires licensees to establish a bond or trust account for the benefit of their customers, requires licensees to hold virtual currency in the same type and amount as any virtual currency owed by the licensee, and prohibits licensees from encumbering customer assets.

Section 200.10, "Material change to business," requires licensees to seek prior approval by written application to introduce a materially new, or materially change an existing, product or service.

Section 200.11, "Change of control; mergers and acquisitions," requires licensees to seek prior approval by written application before executing a change of control or merger or acquisition.

Section 200.12, "Books and records," requires licensees to maintain certain records pertaining to each transaction and make such records available to the Department upon request.

Section 200.13, "Examinations," requires licensees to permit the superintendent to examine the licensee, including the licensee's books and records, at least once every two years and to make special investigations as deemed necessary by the superintendent.

Section 200.14, "Reports and financial disclosures," requires licensees to file quarterly financial statements and audited annual financial statements, to make special reports upon request, and to notify the Department upon discovery of any breach of law or upon a proposed change to the methodology used to calculate the value of virtual currency in fiat currency.

Section 200.15, "Anti-money laundering program," requires licensees to establish and implement an anti-money laundering program, which includes customer identification and transaction monitoring, to maintain records, and to make reports as required by applicable federal anti-money laundering law.

Section 200.16, "Cyber security program," requires licensees to design a cyber security program and written policy, designate a chief information security officer, make reports, and conduct audits.

Section 200.17, "Business continuity and disaster recovery," requires licensees to establish and maintain a written business continuity and disaster recovery plan to address disruptions to normal business operations.

Section 200.18, "Advertising and marketing," requires licensees to display a legend regarding its licensure by the Department, maintain all advertising and marketing materials, comply with all applicable federal and state disclosure requirements, and not make any false or misleading representations or omissions.

Section 200.19, "Consumer protection," requires licensees to disclose material risks and terms and conditions to customers and to establish an anti-fraud policy.

Section 200.20, "Complaints," requires licensees to disclose the licensee's and the Department's contact information and other information pertaining to the resolution of complaints.

Section 200.21, "Transitional period," requires Persons already engaged in virtual currency business activity to apply for a license with the Department within 45 days of the effective date of the regulation.

Section 200.22, "Severability," states that in the event a specific provision of the regulation is adjudged invalid, such judgment will not impair the validity of the remainder of the regulation.

Final rule as compared with last published rule: Nonsubstantive changes were made in sections 200.2, 200.10, 200.11, 200.13, 200.14, 200.15 and 200.19.

Revised rule making(s) were previously published in the State Register on February 25, 2015.

Text of rule and any required statements and analyses may be obtained from: Dana Syracuse - Office of General Counsel, New York State Department of Financial Services, 1 State Street, New York, NY 10004, (212) 709-1663, email: VCLicenseQuestions@dfs.ny.gov

Revised Regulatory Impact Statement, Regulatory Flexibility Analysis, Rural Area Flexibility Analysis and Job Impact Statement

A Revised Regulatory Impact Statement, Regulatory Flexibility Analysis, Rural Area Flexibility Analysis and Job Impact Statement is not required because the revisions to the proposed regulation do not change the substance or conclusions set forth in the previously published Regulatory Impact Statement, Regulatory Flexibility Analysis, Rural Area Flexibility Analysis and Job Impact Statement.

Initial Review of Rule

As a rule that requires a RFA, RAFA or JIS, this rule will be initially reviewed in the calendar year 2018, which is no later than the 3rd year after the year in which this rule is being adopted.

Assessment of Public Comment

The New York State Department of Financial Services (the "Department") initially released proposed rule 23 NYCRR 200 in July 2014 and received over 3700 comments to that proposed rulemaking from virtual currency businesses, other financial services businesses, merchants, retailers, researchers, academics, policy centers, governmental agencies, and private individuals. Every comment was processed and considered by the Department and in February 2015 the Department issued a revised proposed rule 23 NYCRR 200, which incorporated a number of substantial changes made in response to those comments. In response to that revised proposed rulemaking the Department received more than 30 substantive comments from many of the same commenters. Many commenters addressed more than one provision of the proposed regulation, and several requested specific changes. The Department has processed and considered every comment and has made several clarifications to the regulation. This summary is intended to provide an overview of the categories of comments received by the Department, the clarifications the Department has made to the proposed regulation in response to those comments, and, where applicable, the reasons for not making additional changes or clarifications.

The Department received comments concerning the potentially broad applicability of the exemption provided to gift card programs. In response, the Department now uses the term "Prepaid Card" instead of "Gift Card" and amended the definition of that term to clarify that the exemption only applies to cards that are issued and redeemable for fiat currency. (Section 200.2)

Some commenters have expressed concern that licensees should not be required to seek approval from the Department prior to making changes to their business or introducing new products. Commenters have stated that this requirement is burdensome and may deter innovation by not allowing licensees to offer new products without prior approval and would require approval for even minor releases of new products or software. The Department has clarified the regulation to state that prior approval is only needed where a licensee is offering a materially new product, service or activity or is making a material change to an existing product service or activity for which it is already licensed. (Section 200.10)

Several commenters have stated that the 10% threshold for creating a presumption of a change of control should be raised as it could present an obstacle to fundraising and may impair a licensee's ability to attract new funding and new board members. The Department has considered this comment and has determined that the 10% threshold is appropriate and consistent with the threshold for other entities regulated by the Department. The Department has, however, added clarifying language stating that no person shall be deemed to control another person solely by reason of his or her being an officer or director of the licensee. (Section 200.11)

Some commenters have stated that virtual currency companies should not be subject to anti-money laundering and know your customer requirements. The Department has not made any changes in response to these comments. Any entity engaged in a virtual currency business activity, including those that provide hosted wallet services, should be subject to anti-money laundering and know your customer requirements. (Section 200.15)

Several commenters have expressed concern that the regulation creates a new state level requirement that calls for licensees to report when they are involved in a virtual currency transaction or series of transactions that exceeds a US Dollar value of $10,000. While no such federal requirement currently exists for virtual currency to virtual currency transactions, the Department believes that this is an important element of a sound anti-money laundering policy and therefore did not remove this provision. It is noted that entities must currently file a Currency Transaction Report with FinCEN when they are involved in cash transactions exceeding $10,000. This provision of the regulation is intended to capture instances where the transaction is not in fiat currency but in virtual currency. In addition, the regulation has been revised to clarify that licensees must only file such reports with the Department if they are not already required to do so under federal law. (Section 200.15)

A number of other comments concerned the misconception that the Department will require licensees to file duplicative Suspicious Activity Reports ("SAR") with both FinCEN and the Department. The Department has clarified the regulation to state that licensees must only make a separate filing with the Department concerning suspicious activity when they

are not already subject to SAR requirements under federal law. (Section 200.15)

The Department has also received comments stating that the proposed regulation infringes on privacy rights of consumers and presents First Amendment concerns. The Department disagrees with this comment and notes that the regulation as promulgated is not aimed at regulating the expressive aspects of virtual currency, but rather is seeking to regulate virtual currency financial services or products that pose a risk to consumers and the marketplace. The Department has a strong interest in ensuring that any licensees engaged in virtual currency business activity have robust anti-money laundering, cyber security, and consumer protection policies and procedures in place.

The Department also received several comments similar to those received during the previous comment period stating that virtual currency should be regulated under existing money transmission law or not at all. The Department has extensively considered the need to regulate virtual currency business activity and the appropriate way to do so, and it has concluded that a new regulation under the Financial Services Law is necessary to protect New York consumers and users of virtual currency-related services.

The Department has also received comments requesting a safe harbor for smaller entities whereby smaller companies that do not meet certain thresholds would not be required to meet some or all of the requirements set forth in the regulation. Many of these comments are similar to those received during the previous comment period. The Department has considered these comments and has determined that the provision for a conditional license acts as an appropriate on ramp for smaller entities while being able to ensure that licensees have appropriate safeguards in place. (200.4)

Department of Health

EMERGENCY RULE MAKING

Personal Care Services Program (PCSP) and Consumer Directed Personal Assistance Program (CDPAP)

I.D. No. HLT-25-15-00003-E

Filing No. 459

Filing Date: 2015-06-04

Effective Date: 2015-06-04

PURSUANT TO THE PROVISIONS OF THE State Administrative Procedure Act, NOTICE is hereby given of the following action:

Action taken: Amendment of sections 505.14 and 505.28 of Title 18 NYCRR.

Statutory authority: Public Health Law, section 201(1)(v); Social Services Law, sections 363-a(2), 365-a(2)(e) and 365-f

Finding of necessity for emergency rule: Preservation of public health.

Specific reasons underlying the finding of necessity: Pursuant to the authority vested in the Commissioner of Health by Social Services Law § 365-a(2)(e), the Commissioner is authorized to adopt standards, pursuant to emergency regulation, for the provision and management of services for individuals whose need for such services exceeds a specified level to be determined by the Commissioner.

Subject: Personal Care Services Program (PCSP) and Consumer Directed Personal Assistance Program (CDPAP).

Purpose: To establish definitions, criteria and requirements associated with the provision of continuous PC and continuous CDPA services.

Text of emergency rule: Paragraph (3) of subdivision (a) of section 505.14 is repealed and a new paragraph (3) is added to read as follows:

(3) Continuous personal care services means the provision of uninterrupted care, by more than one person, for more than 16 hours per day for a patient who, because of the patient's medical condition and disabilities, requires total assistance with toileting, walking, transferring or feeding at times that cannot be predicted.

Paragraph (4) of subdivision (a) of section 505.14 is amended by adding new subparagraph (iii) to read as follows:

(iii) Personal care services shall not be authorized if the patient's need for assistance can be met by either or both of the following:

(a) voluntary assistance available from informal caregivers including, but not limited to, the patient's family, friends or other responsible adult; or formal services provided by an entity or agency; or

(b) adaptive or specialized equipment or supplies including, but not limited to, bedside commodes, urinals, walkers and wheelchairs, when such equipment or supplies can be provided safely and cost-effectively.

Paragraph (5) of subdivision (a) of section 505.14 is repealed and a new paragraph (5) is added to read as follows:

(5) Live-in 24-hour personal care services means the provision of care by one person for a patient who, because of the patient's medical condition and disabilities, requires some or total assistance with one or more personal care functions during the day and night and whose need for assistance during the night is infrequent or can be predicted.

Clause (b) of subparagraph (i) of paragraph (6) of subdivision (a) of section 505.14 is amended to read as follows:

(b) The [initial] authorization for Level I services shall not exceed eight hours per week. [An exception to this requirement may be made under the following conditions:

(1) The patient requires some or total assistance with meal preparation, including simple modified diets, as a result of the following conditions:

(i) informal caregivers such as family and friends are unavailable, unable or unwilling to provide such assistance or are unacceptable to the patient; and

(ii) community resources to provide meals are unavailable or inaccessible, or inappropriate because of the patient's dietary needs.

(2) In such a situation, the local social services department may authorize up to four additional hours of service per week.]

Clause (b) of subparagraph (ii) of paragraph (6) of subdivision (a) of section 505.14 is amended to read as follows:

(b) When continuous [24-hour care] *personal care services* is indicated, additional requirements for the provision of services, as specified in clause (b)(4)(i)(c) of this section, must be met.

Clause (c) of subparagraph (ii) of paragraph (3) of subdivision (b) of section 505.14 is relettered as clause (d) and a new clause (c) is added to read as follows:

(c) When live-in 24-hour personal care services is indicated, the social assessment shall evaluate whether the patient's home has adequate sleeping accommodations for a personal care aide.

Subclauses (5) and (6) of clause (b) of subparagraph (iii) of paragraph (3) of subdivision (b) of section 505.14 are renumbered as subclauses (6) and (7), and new subclause (5) is added to read as follows:

(5) an evaluation whether adaptive or specialized equipment or supplies including, but not limited to, bedside commodes, urinals, walkers and wheelchairs, can meet the patient's need for assistance with personal care functions, and whether such equipment or supplies can be provided safely and cost-effectively;

Subclause (7) of clause (a) of subparagraph (iv) of paragraph (3) of subdivision (b) of section 505.14 is amended to read as follows:

(7) whether the patient can be served appropriately and more cost-effectively by using *adaptive or* specialized medical equipment *or supplies* covered by the MA program including, but not limited to, *bedside commodes, urinals, walkers, wheelchairs and* insulin pens; and

Clause (c) of subparagraph (iv) of paragraph (3) of subdivision (b) of section 505.14 is amended to read as follows:

(c) A social services district may determine that the assessments required by subclauses (a)(1) through *(6) and* (8) of this subparagraph may be included in the social assessment or the nursing assessment.

Clause (c) of subparagraph (i) of paragraph (4) of subdivision (b) of section 505.14 is amended to read as follows:

(c) the case involves the provision of continuous [24-hour] personal care services as defined in paragraph (a)(3) of this section. Documentation for such cases shall be subject to the following requirements:

Subclause (2) of clause (c) of subparagraph (i) of paragraph (4) of subdivision (b) of section 505.14 is amended to read as follows:

(2) The nursing assessment shall document that*:* the functions required by the patient[,] *;* the degree of assistance required for each function*, including that the patient requires total assistance with toileting, walking, transferring or feeding;* and the time of this assistance require the provision of continuous [24-hour care] *personal care services*.

Subparagraph (ii) of paragraph (4) of subdivision (b) of section 505.14 is amended to read as follows:

(ii) The local professional director, or designee, must review the physician's order and the social, nursing and other required assessments in accordance with the standards for levels of services set forth in subdivision (a) of this section, and is responsible for the final determination of the level and amount of care to be provided. *The local professional director or designee may consult with the patient's treating physician and may conduct an additional assessment of the patient in the home.* The final determination must be made [within five working days of the request] *with reasonable promptness, generally not to exceed seven business days after receipt of the physician's order and the completed social and nursing as-*

Exhibit U

Speech

June 3, 2015

Contact: Matt Anderson, 212-709-1691

NYDFS ANNOUNCES FINAL BITLICENSE FRAMEWORK FOR REGULATING DIGITAL CURRENCY FIRMS

Benjamin M. Lawsky, Superintendent of Financial Services, today announced the release of the New York State Department of Financial Services' (NYDFS) final BitLicense – the first comprehensive framework for regulating digital currency firms.

The BitLicense – which is the product of a nearly two-year-long NYDFS inquiry – contains key consumer protection, anti-money laundering compliance, and cyber security rules tailored for digital currency companies. A copy of the final BitLicense regulation is **available here**.

Superintendent Lawsky also delivered remarks today at the BITS Emerging Payments Forum in Washington, DC regarding the final BitLicense and payments regulation – the text of which can be found below.

***

Superintendent Lawsky 's Remarks at the BITS Emerging Payments Forum
Washington, DC
June 3, 2015

As Prepared for Delivery

Thank you for inviting me to speak with you here today.

I'd like to start these remarks with some broader thoughts on digital currencies, the payments system, and regulation.

Then I'd like to conclude with an update on the New York State Department of Financial Services' BitLicense framework for regulating virtual currency firms.

***

As some of you may know, I will be departing the New York State Department of Financial Services (DFS) later this month – after four years serving as the agency's first superintendent.

It has been a pretty eventful four years.

Now, if you asked me back when I took this job in 2011 what I thought we would be working on during my tenure – digital currency would not exactly have been at the top of the list.

Anti-money laundering enforcement? Yes

Electronic trading issues? Absolutely.

Mortgage servicing? For sure.

But crytocurrency?

Looking back, that was a bit of a surprise.

However, on the plus side, now I know what a Dogecoin is – not that it comes up much at dinner parties.

***

In many ways, the fact that we found ourselves working on an issue as unexpected as digital currency speaks to the extraordinarily dynamic nature of the financial markets and financial technology right now.

The pace of change is only going to accelerate in the years to come. And regulators need to be ready to meet that challenge.

The emergence of digital currency and other new forms of payments technology represent an important test for financial regulators such as NYDFS.

We have a responsibility to regulate new financial products in order to help protect consumers and root out illicit activity. That is the bread and butter job of a financial regulator.

However, by the same token, we should not react so harshly that we doom promising new technologies before they get out of the cradle.

Getting that balance right is hard, but it is key. At NYDFS, we've faced similar issues in the past as we've licensed new payment firms like Square or new insurers like Oscar. We want to promote and support companies that use new, emerging technologies to build better financial companies. We just need to make sure that we put appropriate regulatory guardrails in place.

Indeed, it was interesting to see that some responded to the emergence of digital currencies with calls to "ban Bitcoin."

That is a curious concept – banning Bitcoin.

How exactly does someone go about banning computer code?

The answer, of course, is that you cannot

Financial regulators and policymakers need to recognize that when it comes to digital currencies and other new payments technology – the genie is already out of the bottle.

And those that try to turn back the clock risk facing the same fate as the Luddites.

The question, then, is how exactly, in practice, regulators should balance their responsibility to protect consumers and root out fraud – while still permitting beneficial innovation to proceed.

We can tell you, from experience, setting the exact contours of the new rules of the road in these areas is extraordinarily difficult.

Regulators are not always going to get the balance precisely right.

Much like some startups – there are going to be some false starts.

Over the next 5, 10, 15 years, and beyond – you are going to see, I think, a fine-tuning and shaking out of digital currency regulation across the country and across the globe.

But we need to begin somewhere.

And we need to approach these exceedingly complex questions with an appropriate sense of humility as regulators.

The jury is still out on how we have met our regulatory test. And I don't think we will know how we did for some time.

But, we hope, the work NYDFS and other regulators have done will be a good start.

***

With that in mind, I'd like to share (with the benefit of hindsight) a few, brief lessons we have learned at NYDFS from our experience working on digital currency regulation.

I hope that these lessons will be helpful and informative to future policymakers. Not only in the area of digital currency – but also for a broad range of new financial technologies.

To start, as I previously noted, we had no inkling whatsoever back when we formed DFS that digital currency regulation would become a major issue facing our Department.

Frankly, we also had little to no expertise among our examiners in this area.

But we did have a specific legal responsibility to act because we believed that several firms could be engaging in money transmission – which is an activity that is regulated by our Department, as well as other states.

The first instinct among some at NYDFS was to shoehorn these new digital currency firms into our old money transmission rules.

However, state money transmission rules date back to the civil war – when there was barely mass communication, let alone an Internet.

And it became increasingly clear to us that such an approach simply would not work.

Digital currency was unlike anything we had ever seen before. It wasn't exactly Western Union.

Indeed, we began to ask ourselves questions like: How exactly do you set capital requirements for a "money transmitter" that holds digital currency, which many do not even consider "money?"

After a lot of discussion, we decided that we would instead launch a broad-based fact-finding inquiry into digital currency before making any final decisions.

To that point, when facing new financial technologies, it is very important for regulators to look before they leap.

Attempting to force novel technologies and business models into existing regulatory boxes – simply because "that is the way it has always been done" – may not be a sensible approach. We need, at times, to be more creative than that as regulators – even if it takes us outside our comfort zone.

***

Similarly, regulators also need to realize their own limitations; recognize what they do not know; and keep an open mind when approaching new technologies.

As you can probably imagine, people do not generally go into a career in financial regulation because they want to work on the cutting edge of technology.

So, it is important for regulators to work quickly, but carefully, to learn everything they can about these new technologies as they emerge.

I had a similar experience personally.

I'll be honest; I hadn't even heard the word Bitcoin until early 2013 in the context of the banking crisis that occurred in Cyprus.

And, at first, the whole concept struck me as a little bizarre.

However, the more we dug into it, the more interesting and promising it seemed.

We hadn't originally appreciated how the Bitcoin blockchain represented a major advance in cryptography, which could have significant applications in a multitude of areas.

That the technology underlying Bitcoin could be used not just as a currency, but potentially as a means to transfer all manner of personal property (such as deeds) securely over the Internet.

That – when it comes to Bitcoin – platforms could be built upon platforms could be built upon platforms by future innovators.

Frankly, we do not know what digital currency is going to look like in five or ten years – and there are a lot of interesting possibilities.

There might be – at the very least – a kernel of something here that has a profound impact on the future of payments technology and the financial system. Regulators are not always the experts on such matters, but my gut now is that it's likely.

So, as a regulator, even if a concept strikes us as a bit bizarre based on our past experience or work, it is important that we keep an open mind.

***

I'd like to next turn to the question of the relationship between regulators and technologists – and the need for greater dialogue and understanding between the two.

In many ways – I think it is fair to say – right now it often feels like regulators are from Mars and technologists are from Venus.

What we are currently seeing is the collision of a very tightly regulated financial sector and a much more lightly regulated technology sector.

That is manifesting itself in the financial technology business, as well as a range of other areas, such as ride and home sharing companies.

That collision isn't always going to be pretty at first.

But we – both regulators and technologists – have a responsibility to find common ground and work together in good faith.

There are two sides to that coin, of course.

Regulators should not simply ban or dismiss technology that they find unfamiliar. Or work to protect entrenched incumbent companies – which is the very definition of regulatory capture.

That said, technologists also have a responsibility of their own to meet. They cannot simply ignore the rules they do not like and try to create "facts on the ground."

Generally speaking, consumer protection rules exist for good reason.

And to the extent that they need to be updated, regulators should move quickly, but carefully, to do so.

Regulators can certainly be slow in responding to new technologies – no doubt. And technologists are right to call them out on it and put public pressure on them when they are dragging their feet. In particular, if those delays are intended to help protect entrenched incumbents.

But that is not an excuse for ignoring or violating the law.

We are still in the early innings of this collision of regulation and financial technology.

And I think things will improve with time as we foster greater dialogue and understanding.

But I think both sides – regulators and technologists – could benefit from taking a moment and trying to put themselves in the shoes of their counterpart across the table.

And then work together, in good faith to better serve consumers.

***

I'd like to turn now to the BitLicense.

Today, we are issuing the final BitLicense framework for regulating virtual currency firms.

This framework is the product of a nearly two-year-long regulatory inquiry that the New York State Department of Financial Services (NYDFS) began in 2013. In fact, this is the third and final version of the regulation we have put forward.

Over the course of our inquiry, we have received an immense amount of public feedback, which we believe significantly improved the final product.

Indeed, the second version of the regulation we put forward incorporated a number of substantial changes from our initial draft in response to those comments. In particular, we sought to help provide **an on-ramp for start-ups** – while still ensuring robust standards for consumer protection, cyber security, and anti-money-laundering compliance.

The third and final version does not include the type of major changes we saw in the last round. However, we did want to make several points clear today in order to allay various concerns we have heard during the public comment period.

To that end, we wanted to make crystal clear that:

- First, companies will not need prior approval for standard software or app updates – only for material changes to their products or business models. (A good example of a material change would be if a firm that was licensed as a wallet service decided to begin offering exchange services. We have no interest in micro-managing minor app updates. We're not Apple.)
- Second, we have no intention of being a regulator of software developers – only financial intermediaries. For example, students or other innovators who are simply developing software and are not holding onto customer funds are not required to apply for a BitLicense. There is an important reason for making this distinction when a company becomes a financial intermediary: There is a basic bargain that when a financial company is entrusted with safeguarding customer funds and receives a license from the state to do so – it accepts the need for heightened regulatory scrutiny to help ensure that a consumer's money does not just disappear into a black hole.
- Third, we are not going to require a duplicative set of application submissions for firms that want both a BitLicense and a money transmitter license. Firms will be able to cross-satisfy many of those license requirements. Companies will be able to work with us to have a "one-stop" application submission that covers all the bases they need.
- Fourth, companies that already file suspicious activity reports (also called "SARs") with federal regulators such as FinCEN do not have to file a duplicate set of those same SARs with our agency. Our goal is to avoid duplication where possible. And we generally already have access to that information when we need it through information sharing arrangements with federal regulators.
- Fifth, companies also would not need prior approval from NYDFS for every new round of venture capital funding. Generally, a company would only need prior approval if the investor wants to direct the management and policies of the firm (which is known as a "control person" in regulatory jargon). In other words, that provision is not targeted at truly "passive investors." The notion of approving a "control person" is pretty standard in the regulation of financial companies and is generally intended to help stop known fraudsters from having direct access to customer funds. Large new investors (i.e. those with a 10 percent or more stake) would simply need to document and demonstrate that they are not going to have such a role. Additionally, under the regulation, simply because someone sits on a company's board does not necessarily mean they are considered a control person.

We understand, of course, that we are not going to satisfy everyone with these new regulations.

Some have even suggested removing all anti-money laundering requirements for certain financial companies involved in digital currency, which we do not believe is warranted.

Again, we recognize that we are not going to please everyone. That is the nature of regulatory oversight.

For example, when we write new regulations for Wall Street, if the banks are completely happy with something we've drafted, it probably means we haven't done our jobs right.

Our goal, as always, is to be sensible and fair.

We are excited about the potential digital currency holds for helping drive long-overdue changes in our ossified payments system. We simply want to make sure that we put in place guardrails that protect consumers and root out illicit activity – without stifling beneficial innovation.

Ultimately, we think regulation is important to the long-term health of the virtual currency industry. Building trust and confidence among consumers is crucial for wider adoption. It also helps attract additional investment.

Digital currency companies have already sought to work with us to put in place consumer and anti-money laundering protections. In fact, one firm recently received a New York State charter to operate under the banking law. And we expect additional companies will follow in the weeks and months to come – whether under the banking law or through the BitLicense.

This is a critical and exciting time in the broader evolution of the payments system. Virtual currency is a novel field for regulators and everyone – including our office – must be willing to take a hard look at how these new rules are working when they are put into practice.

We have never claimed to have a monopoly on the truth. And regulators must always be willing to course correct when necessary.

However, it is our hope that digital currency and other innovations in payments technology – together with prudent regulation – will help deliver better service and lower costs to customers over the long term.

As we have noted in previous contexts, I think it would shock most consumers to learn that – at its core, despite modest improvements – our bank payments has changed little since it was created four decades ago in the 1970s.

And it generally takes you longer to transfer money electronically than it would to physically transport that cash to another state or country.

In a world where information travels around the globe in a matter of milliseconds, it can often take several days to transfer money to a friend's bank account.

In an age of smart phones and on-demand technology, we still have a disco-era payments system.

That needs to change and we are starting to see real efforts at improvements.

We need to recognize that our children and their children will not hesitate to bank and live their entire financial lives online.

And in the online world, people expect near-instantaneous execution.

Just think about how mad we all get when our Netflix connection buffers even for a few minutes.

The same standard will apply to how we make our car payments or send money to a friend. Of course, we still need to ensure that those transactions are safe and properly filtered from a compliance perspective.

While it is by no means assured, perhaps the emerging financial technologies we are seeing today will help drive innovation and bring our country's payments system into a bright new era.

That is certainly our hope at DFS.

Thank you again for inviting me to speak with you today – and I look forward to answering your questions.

###

Exhibit V

NEW YORK STATE

DEPARTMENT OF FINANCIAL SERVICES

PROPOSED

NEW YORK CODES, RULES AND REGULATIONS

TITLE 23. DEPARTMENT OF FINANCIAL SERVICES

CHAPTER I. REGULATIONS OF THE SUPERINTENDENT OF FINANCIAL SERVICES

PART 200. VIRTUAL CURRENCIES

NEW YORK STATE

DEPARTMENT OF FINANCIAL SERVICES

PROPOSED

NEW YORK CODES, RULES AND REGULATIONS

TITLE 23. DEPARTMENT OF FINANCIAL SERVICES

CHAPTER I. REGULATIONS OF THE SUPERINTENDENT OF FINANCIAL SERVICES

PART 200. VIRTUAL CURRENCIES

Statutory Authority: Financial Services Law, sections 102,104, 201, 206, 301, 302, 309, and 408

Section 200.1 Introduction

This Part contains regulations relating to the conduct of business involving Virtual Currency, as defined herein, in accordance with the superintendent's powers pursuant to the above-stated authority.

Section 200.2 Definitions

For purposes of this Part only, the following definitions shall apply:

(a) *Affiliate* means any Person that directly or indirectly controls, is controlled by, or is under common control with, another Person;

(b) *Cyber Security Event* means any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt, or misuse a Licensee's electronic systems or information stored on such systems;

(c) *Department* means the New York State Department of Financial Services;

(d) *Fiat Currency* means government-issued currency that is designated as legal tender in its country of issuance through government decree, regulation, or law;

(e) *Licensee* means any Person duly licensed by the superintendent pursuant to this Part;

(f) *New York* means the State of New York;

(g) *New York Resident* means any Person that resides, is located, has a place of business, or is conducting business in New York;

(h) *Person* means an individual, partnership, corporation, association, joint stock association, trust, or other business combination or entity, however organized;

(i) *Principal Officer* means an executive officer of an entity, including, but not limited to, the chief executive, financial, operating, and compliance officers, president, general counsel, managing partner, general partner, controlling partner, and trustee, as applicable;

(j) *Principal Stockholder* means any Person that directly or indirectly owns, controls, or holds with power to vote ten percent or more of any class of outstanding capital stock of a corporate entity or possesses the power to direct or cause the direction of the management or policies of the entity;

(k) *Principal Beneficiary* means any Person entitled to ten percent or more of the benefits of a trust;

(l) *Transmission* means the transfer, by or through a third party, of Virtual Currency from one Person to another Person, including the transfer from the account or storage repository of one Person to the account or storage repository of another Person;

(m) *Virtual Currency* means any type of digital unit that is used as a medium of exchange or a form of digitally stored value or that is incorporated into payment system technology. Virtual Currency shall be broadly construed to include digital units of exchange that (i) have a centralized repository or administrator; (ii) are decentralized and have no centralized repository or administrator; or (iii) may be created or obtained by computing or manufacturing effort. Virtual Currency shall not be construed to include digital units that are used solely within online gaming platforms with no market or application outside of those gaming platforms, nor shall Virtual Currency be construed to include digital units that are used exclusively as part of a customer affinity or rewards program, and can be applied solely as payment for purchases with the issuer and/or other designated merchants, but cannot be converted into, or redeemed for, Fiat Currency;

(n) *Virtual Currency Business Activity* means the conduct of any one of the following types of activities involving New York or a New York Resident:

(1) receiving Virtual Currency for transmission or transmitting the same;

(2) securing, storing, holding, or maintaining custody or control of Virtual Currency on behalf of others;

(3) buying and selling Virtual Currency as a customer business;

(4) performing retail conversion services, including the conversion or exchange of Fiat Currency or other value into Virtual Currency, the conversion or exchange of Virtual Currency into Fiat Currency or other value, or the conversion or exchange of one form of Virtual Currency into another form of Virtual Currency; or

(5) controlling, administering, or issuing a Virtual Currency.

Statutory Authority: Financial Services Law, sections 102, 201, 301, and 302

Section 200.3 License

(a) License required. No Person shall, without a license obtained from the superintendent as provided in this Part, engage in any Virtual Currency Business Activity.

(b) Unlicensed agents prohibited. Each Licensee is prohibited from conducting any Virtual Currency Business Activity through an agent or agency arrangement when the agent is not a Licensee.

(c) Exemption from licensing requirements. The following Persons are exempt from the licensing requirements otherwise applicable under this Part:

(1) Persons that are chartered under the New York Banking Law to conduct exchange services and are approved by the superintendent to engage in Virtual Currency Business Activity; and

(2) merchants and consumers that utilize Virtual Currency solely for the purchase or sale of goods or services.

Statutory Authority: Financial Services Law, sections 102, 201, 301, and 302

Section 200.4 Application

(a) Application for a license required under this Part shall be in writing, under oath, and in a form prescribed by the superintendent, and shall contain the following:

(1) the exact name of the applicant, including any doing business as (DBA) name, the form of organization, the date of organization, and the jurisdiction where organized or incorporated;

(2) a list of all of the applicant's Affiliates and an organization chart illustrating the relationship among the applicant and such Affiliates;

(3) a list of, and detailed biographical information for, each individual applicant and each director, Principal Officer, Principal Stockholder, and Principal Beneficiary of the applicant, as applicable, including such individual's name, physical and mailing addresses, and information and documentation regarding their personal history, experience, and qualification, which shall be accompanied by a form of authority, executed by such individual, to release information to the Department;

(4) a background report prepared by an independent investigatory agency acceptable to the superintendent for each individual applicant, and each Principal Officer, Principal Stockholder, and Principal Beneficiary of the applicant, as applicable;

(5) for each individual applicant, and each Principal Officer, Principal Stockholder, and Principal Beneficiary of the applicant, as applicable, and for all individuals to be employed by the applicant: (i) a set of completed fingerprints, or a receipt indicating the vendor (which vendor must be acceptable to the superintendent) at which, and the date when, the fingerprints were taken, for submission to the State Division of Criminal Justice Services and the Federal Bureau of Investigation; (ii) if applicable, such processing fees as prescribed by the superintendent; and (iii) two portrait-style photographs of the individuals measuring not more than two inches by two inches;

(6) an organization chart of the applicant and its management structure, including its Principal Officers or senior management, indicating lines of authority and the allocation of duties among its Principal Officers or senior management;

(7) a current financial statement for the applicant and each Principal Officer, Principal Stockholder, and Principal Beneficiary of the applicant, as applicable, and a projected pro forma balance sheet and income and expense statement for the next year of the applicant's operation;

(8) a description of the proposed, current, and historical business of the applicant, including detail on the products and services provided and to be provided, all associated website addresses, the jurisdictions in which the applicant is engaged in business, the principal place of business, the primary market of operation, the projected customer base, any specific marketing targets, and the physical address of any operation in New York;

(9) details of all banking arrangements;

(10) all written policies and procedures, including those required by this Part;

(11) an affidavit describing any administrative, civil, or criminal action, litigation, or proceeding before any governmental agency, court, or arbitration tribunal and any existing, pending, or threatened action, litigation, or proceeding against the applicant or any of its directors, Principal Officers, Principal Stockholders, and Principal Beneficiaries, as applicable, including the names of the parties, the nature of the proceeding, and the current status of the proceeding;

(12) if applicable, a copy of any insurance policies maintained for the benefit of the applicant, its directors or officers, or its customers;

(13) an explanation of the methodologies used to calculate the value of Virtual Currency in Fiat Currency; and

(14) such other additional information as the superintendent may require.

(b) As part of such application, the applicant shall demonstrate that it will be compliant with all of the requirements of this Part upon licensing.

(c) The superintendent may permit that any application for a license under this Part, or any other submission required by this Part, be made or executed by electronic means.

Statutory authority: Financial Services Law, sections 102, 201, 202, 301, and 302

Section 200.5 Application fees

As part of an application for licensing under this Part, each applicant must submit an initial application fee, in an amount prescribed by the superintendent, to cover the cost of processing the application, reviewing application materials, and investigating the financial condition and responsibility, financial and business experience, and character and general fitness of the applicant. If the application is denied or withdrawn, such fee shall not be refunded. Each Licensee may be required to pay fees to the Department to process additional applications related to the license.

Statutory authority: Financial Services Law, sections 202, 206, 301, 302, and 304-a; State Administrative Procedures Act, section 102

Section 200.6 Action by superintendent

(a) Generally. Upon the filing of an application for licensing under this Part, payment of the required fee, and demonstration by the applicant of its ability to comply with the provisions of this Part, the superintendent shall investigate the financial condition and responsibility, financial and business experience, and character and general fitness of the applicant. If the superintendent finds these qualities are such as to warrant the belief that the applicant's business will be conducted honestly, fairly, equitably, carefully, and efficiently within the purposes and intent of this Part, and in a manner commanding the confidence and trust of the community, the superintendent shall advise the applicant in writing of his or her approval of the application, and shall issue to the applicant a license to conduct Virtual Currency Business Activity, subject to the provisions of this Part and such other conditions as the superintendent shall deem appropriate; or the superintendent may deny the application.

(b) Approval or denial of application. The superintendent shall approve or deny every application for a license hereunder within 90 days from the filing of an application deemed by the superintendent to be complete. Such period of 90 days may be extended at the discretion of the superintendent for such additional reasonable period of time as may be required to enable compliance with this Part. A license issued pursuant to this Part shall remain in full force and effect until it is surrendered by the Licensee or revoked or suspended as provided in this Part.

(c) Suspension or revocation of license. The superintendent may suspend or revoke a license issued under this Part on any ground on which the superintendent might refuse to issue an original license, for a violation of any provision of this Part, for good cause shown, or for failure of the Licensee to pay a judgment, recovered in any court, within or without this State, by a claimant or creditor in an action arising out of, or relating to, the Licensee's Virtual Currency Business Activity, within thirty days after the judgment becomes final or within thirty days after expiration or termination of a stay of execution thereon; provided, however, that if execution on

the judgment is stayed, by court order or operation of law or otherwise, then proceedings to suspend or revoke the license (for failure of the Licensee to pay such judgment) may not be commenced by the superintendent during the time of such stay, and for thirty days thereafter. "Good cause" shall exist when a Licensee has defaulted or is likely to default in performing its obligations or financial engagements or engages in unlawful, dishonest, wrongful, or inequitable conduct or practices that may cause harm to the public.

(d) Hearing. No license issued under this Part shall be revoked or suspended except after a hearing thereon. The superintendent shall give a Licensee no less than ten days' written notice of the time and place of such hearing by registered or certified mail addressed to the principal place of business of such Licensee. Any order of the superintendent suspending or revoking such license shall state the grounds upon which it is based and be sent by registered or certified mail to the Licensee at its principal place of business as shown in the records of the Department.

(e) Preliminary injunction. The superintendent may, when deemed by the superintendent to be in the public interest, seek a preliminary injunction to restrain a Licensee from continuing to perform acts that violate any provision of this Part, the Financial Services Law, Banking Law, or Insurance Law.

(f) Preservation of powers. Nothing in this Part shall be construed as limiting any power granted to the superintendent under any other provision of the Banking Law, Insurance Law, or Financial Services Law, including any power to investigate possible violations of law, rule, or regulation or to impose penalties or take any other action against any Person for violation of such laws, rules, or regulations.

Statutory Authority: Financial Services Law, sections 102, 301, 302, 305, and 309

Section 200.7 Compliance

(a) Generally. Each Licensee is required to comply with all applicable federal and state laws, rules, and regulations.

(b) Compliance officer. Each Licensee shall designate a qualified individual or individuals responsible for coordinating and monitoring compliance with this Part and all other applicable federal and state laws, rules, and regulations.

(c) Compliance policy. Each Licensee shall maintain and enforce written compliance policies, including policies with respect to anti-fraud, anti-money laundering, cyber security, privacy and information security, and any other policy required under this Part, which must be reviewed and approved by the Licensee's board of directors or an equivalent governing body.

Statutory Authority: Financial Services Law, sections 102, 301, and 302

Section 200.8 Capital requirements

(a) Each Licensee shall maintain at all times such capital as the superintendent determines is sufficient to ensure the financial integrity of the Licensee and its ongoing operations. In determining the minimum amount of capital that must be maintained by a Licensee, the superintendent will consider a variety of factors, including but not limited to:

(1) the composition of the Licensee's total assets, including the position, size, liquidity, risk exposure, and price volatility of each type of asset;

(2) the composition of the Licensee's total liabilities, including the size and repayment timing of each type of liability;

(3) the actual and expected volume of the Licensee's Virtual Currency Business Activity;

(4) whether the Licensee is already licensed or regulated by the superintendent under the Financial Services Law, Banking Law, or Insurance Law, or otherwise subject to such laws as a provider of a financial product or service, and whether the Licensee is in good standing in such capacity;

(5) the amount of leverage employed by the Licensee;

(6) the liquidity position of the Licensee; and

(7) the financial protection that the Licensee provides for its customers through its trust account or bond.

(b) Each Licensee shall be permitted to invest its retained earnings and profits in only the following high-quality, investment-grade permissible investments with maturities of up to one year and denominated in United States dollars:

(1) certificates of deposit issued by financial institutions that are regulated by a United States federal or state regulatory agency;

(2) money market funds;

(3) state or municipal bonds;

(4) United States government securities; or

(5) United States government agency securities.

Statutory Authority: Financial Services Law, sections 102, 202, 301, and 302

Section 200.9 Custody and protection of customer assets

(a) Each Licensee shall maintain a bond or trust account in United States dollars for the benefit of its customers in such form and amount as is acceptable to the superintendent for the protection of the Licensee's customers.

(b) To the extent a Licensee secures, stores, holds, or maintains custody or control of Virtual Currency on behalf of another Person, such Licensee shall hold Virtual Currency of the same type and amount as that which is owed or obligated to such other Person.

(c) Each Licensee is prohibited from selling, transferring, assigning, lending, hypothecating, pledging, or otherwise using or encumbering assets, including Virtual Currency, held, stored, or maintained by, or under the custody or control of, such Licensee on behalf of another Person.

Statutory Authority: Financial Services Law, sections 102, 202, 301, and 302

Section 200.10 Material change to business

(a) Each Licensee must obtain the superintendent's prior written approval for any plan or proposal to introduce or offer a new product, service, or activity, or to make a material change to an existing product, service, or activity, involving New York or New York Residents.

(b) A "material change" may occur where:

(1) a change is proposed to an existing product, service, or activity that may cause such product, service, or activity to be materially different from that previously listed on the application for licensing by the superintendent;

(2) the proposed change may raise a legal or regulatory issue about the permissibility of the product, service, or activity; or

(3) the proposed change may raise safety and soundness or operational concerns.

(c) The Licensee shall submit a written plan describing the proposed material change, including a detailed description of the business operations, compliance policies, and the impact on the overall business of the Licensee, as well as such other information as requested by the superintendent.

Statutory Authority: Financial Services Law, sections 102, 202, 301, and 302

Section 200.11 Change of control; mergers and acquisitions

(a) Change of Control. No action shall be taken, except with the prior written approval of the superintendent, that may result in a change of control of a Licensee.

(1) Prior to any change of control, the Person seeking to acquire control of a Licensee shall submit a written application to the superintendent in a form and substance acceptable to the superintendent, including detailed information about the applicant and all directors, Principal Officers, Principal Stockholders, and Principal Beneficiaries of the applicant, as applicable.

(2) For purposes of this Section, the term "control" means the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of a Licensee whether through the ownership of stock of such Licensee or the stock of any Person that possesses such power. Control shall be presumed to exist if a Person, directly or indirectly, owns, controls, or holds with power to vote ten percent or more of the voting stock of a Licensee or of any Person that owns, controls, or holds with power to vote ten percent or more of the voting stock of such Licensee.

(3) The superintendent shall approve or deny every application for a change of control of a Licensee hereunder within 120 days from the filing of an application deemed by the superintendent to be complete. Such period of 120 days may be extended by the superintendent, for good cause shown, for such additional reasonable period of time as may be required to enable compliance with the requirements and conditions of this Part.

(4) In determining whether to approve a proposed change of control, the superintendent shall, among other factors, take into consideration the public interest and the needs and convenience of the public.

(b) Mergers and Acquisitions. No action shall be taken, except with the prior written approval of the superintendent, that may result in a merger or acquisition of all or a substantial part of the assets of a Licensee.

(1) Prior to any such merger or acquisition, an application containing a written plan of merger or acquisition shall be submitted to the superintendent by the entities that are to merge or by the acquiring entity, as applicable. Such plan shall be in form and substance satisfactory to the superintendent, and shall specify each entity to be merged, the entity that is to receive into itself the merging entity, or the entity acquiring all or substantially all of the assets of the Licensee, as applicable, and shall describe the terms and conditions of the merger or acquisition and the mode of carrying it into effect.

(2) The superintendent shall approve or deny a proposed merger or a proposed acquisition of all or a substantial part of the assets of a Licensee within 120 days after the submission of the proposed plan to the Department. Such period of 120 days may be extended by the superintendent, for good cause shown, for such additional reasonable period of time as may be required to enable compliance with the requirements and conditions of this Part.

(3) In determining whether to so approve a proposed merger or acquisition, the superintendent shall, among other factors, take into consideration the public interest and the needs and convenience of the public.

Statutory authority: Financial Services Law, sections 102, 202, 301, and 302

Section 200.12 Books and records

(a) Each Licensee shall, in connection with its Virtual Currency Business Activity, make, keep, and preserve all of its books and records in their original form or native file format for a period of at least ten years from the date of their creation and in a condition that will allow the superintendent to determine whether the Licensee is complying with all applicable laws, rules, and regulations. The books and records maintained by each Licensee shall, without limitation, include:

(1) for each transaction, the amount, date, and precise time of the transaction, any payment instructions, the total amount of fees and charges received and paid to, by, or on behalf of the Licensee, and the names, account numbers, and physical addresses of the parties to the transaction;

(2) a general ledger containing all assets, liabilities, capital, income, expense accounts, and profit and loss accounts;

(3) bank statements and bank reconciliation records;

(4) any statements or valuations sent or provided to customers and counterparties;

(5) records or minutes of meetings of the board of directors or an equivalent governing body;

(6) records demonstrating compliance with applicable state and federal anti-money laundering laws, rules, and regulations, including customer identification and verification documents, records linking customers to their respective accounts and balances, and a record of all compliance breaches;

(7) communications and documentation related to investigations of customer complaints and transaction error resolution or concerning facts giving rise to possible violations of laws, rules, or regulations;

(8) all other records required to be maintained in accordance with this Part; and

(9) all other records as the superintendent may require.

(b) Each Licensee shall provide the Department, upon request, immediate access to all facilities, books, records, documents, or other information maintained by the Licensee or its Affiliates, wherever located.

(c) Records of non-completed, outstanding, or inactive Virtual Currency accounts or transactions shall be maintained for at least five years after the time when any such Virtual Currency has been deemed, under the Abandoned Property Law, to be abandoned property.

Statutory authority: Financial Services Law, sections 102, 202, 301, 302, and 306

Section 200.13 Examinations

(a) Each Licensee shall permit and assist the superintendent to examine the Licensee whenever in the superintendent's judgment such examination is necessary or advisable, but not less than once every two calendar years, including, without limitation, to determine:

(1) the financial condition of the Licensee;

(2) the safety and soundness of the conduct of its business;

(3) the policies of its management;

(4) whether the requirements of laws, rules, and regulations have been complied with in the administration of its affairs; and

(5) such other matters as the superintendent may determine, including, but not limited to, any activities of the Licensee outside the State of New York if in the opinion of the superintendent such activities may affect the Licensee's business involving New York or New York Residents.

(b) Each Licensee shall permit and assist the superintendent at any time to examine all of the Licensee's books, records, accounts, documents, and other information.

(c) Each Licensee shall permit and assist the superintendent to make such special investigations as the superintendent shall deem necessary to determine whether a Licensee has violated any provision of the applicable laws, rules, or regulations and to the extent necessary shall permit and assist the superintendent to examine all relevant facilities, books, records, accounts, documents, and other information.

(d) For the purpose of determining the financial condition of the Licensee or its safety and soundness practices, the Licensee shall permit and assist the superintendent, when in the superintendent's judgment it is necessary or advisable, to examine an Affiliate of the Licensee.

Statutory authority: Financial Services Law, sections 102, 202, 301, and 302

Section 200.14 Reports and financial disclosures

(a) Each Licensee shall submit to the superintendent quarterly financial statements within 45 days following the close of the Licensee's fiscal quarter in the form, and containing such information, as the superintendent shall prescribe, including without limitation, the following information:

(1) a statement of the financial condition of the Licensee, including a complete balance sheet, income statement, profit and loss statement, statement of retained earnings, statement of net liquid assets, statement of net worth, statement of cash flows, and statement of change in ownership equity;

(2) a statement demonstrating compliance with any financial requirements established under this Part;

(3) financial projections and strategic business plans;

(4) a list of all off-balance sheet items;

(5) a chart of accounts, including a description of each account; and

(6) a report of permissible investments by the Licensee as permitted under this Part.

(b) Each Licensee shall submit audited annual financial statements, prepared in accordance with generally accepted accounting principles, together with an opinion of an independent certified public accountant and an evaluation by such accountant of the accounting procedures and internal controls of the Licensee within one hundred and twenty days of its fiscal year end. All such annual financial statements shall include:

(1) a statement of management's responsibilities for preparing the Licensee's annual financial statements, establishing and maintaining adequate internal controls and procedures for financial reporting, and complying with all applicable laws, rules, and regulations;

(2) an assessment by management of the Licensee's compliance with such applicable laws, rules, and regulations during the fiscal year covered by the financial statements, including management's conclusion as to whether the Licensee has complied with those laws, rules, and regulations during such period; and

(3) certification of the financial statements by an officer or director of the Licensee attesting to the truth and correctness of those statements.

(c) Each Licensee shall notify the superintendent in writing of any criminal action or insolvency proceeding against the Licensee or any of its directors, Principal Stockholders, Principal Officers, and Principal Beneficiaries, as applicable, immediately after the commencement of any such action or proceeding.

(d) Each Licensee shall notify the superintendent in writing of any proposed change to the methodology used to calculate the value of Virtual Currency in Fiat Currency that was submitted to the Department in accordance with Section 200.4 or this Subsection.

(e) Each Licensee shall submit a report to the superintendent immediately upon the discovery of any violation or breach of law, rule, or regulation related to the conduct of activity licensed under this Part.

(f) Each Licensee shall make additional special reports to the superintendent, at such times and in such form, as the superintendent shall prescribe.

Statutory authority: Financial Services Law, sections 102, 202, 301, 302, and 306

Section 200.15 Anti-money laundering program

All values in United States dollars referenced herein must be calculated using the methodology to determine the value of Virtual Currency in Fiat Currency that was approved by the Department under this Part.

(a) Each Licensee shall conduct an initial risk assessment that will consider legal, compliance, financial, and reputational risks associated with the Licensee's activities, services, customers, counterparties, and geographic location and shall establish, maintain, and enforce an anti-money laundering program based thereon. The Licensee shall conduct additional assessments on an annual basis, or more frequently as risks change, and shall modify its anti-money laundering program as appropriate to reflect any such changes.

(b) The anti-money laundering program shall, at a minimum:

(1) provide for a system of internal controls, policies, and procedures designed to ensure ongoing compliance with all applicable anti-money laundering laws, rules, and regulations;

(2) provide for independent testing for compliance with, and the effectiveness of, the anti-money laundering program to be conducted by qualified personnel of the Licensee or by a qualified outside party, at least annually, the findings of which shall be summarized in a written report submitted to the superintendent;

(3) designate a qualified individual or individuals in compliance responsible for coordinating and monitoring day-to-day compliance with the anti-money laundering program; and

(4) provide ongoing training for appropriate personnel to ensure they have a fulsome understanding of anti-money laundering requirements and to enable them to identify transactions required to be reported and maintain records required to be kept in accordance with this Part.

(c) The anti-money laundering program shall include a written anti-money laundering policy reviewed and approved by the Licensee's board of directors or equivalent governing body.

(d) Each Licensee, as part of its anti-money laundering program, shall maintain records and make reports in the manner set forth below.

(1) Records of Virtual Currency transactions. Each Licensee shall maintain the following information for all transactions involving the payment, receipt, exchange or conversion, purchase, sale, transfer, or transmission of Virtual Currency: the identity and physical addresses of the parties involved, the amount or value of the transaction, including in what denomination purchased, sold, or transferred, the method of payment, the date(s) on which the transaction was initiated and completed, and a description of the transaction.

(2) Reports on transactions. When a Licensee is involved in a transaction or series of transactions for the receipt, exchange, conversion, purchase, sale, transfer, or transmission of Virtual Currency, in an aggregate amount exceeding the United States dollar value of $10,000 in one day, by one Person, the Licensee shall notify the Department, in a manner prescribed by the superintendent, within 24 hours.

(3) Reporting of Suspicious Activity. Each Licensee shall monitor for transactions that might signify money laundering, tax evasion, or other illegal or criminal activity and notify the Department, in a manner prescribed by the superintendent, immediately upon detection of such a transaction(s).

(i) Each Licensee shall file Suspicious Activity Reports ("SARs") in accordance with applicable federal laws, rules, and regulations.

(ii) Each Licensee that is not required to file SARs under federal law shall file with the superintendent, in a form prescribed by the superintendent, reports of transactions that indicate a possible violation of law or regulation within 30 days from the detection of the facts that constitute a need for filing. Continuing suspicious activity shall be reviewed on an ongoing basis and a suspicious activity report shall be filed within 120 days of the last filing describing continuing activity.

(e) No Licensee shall structure transactions, or assist in the structuring of transactions, to evade reporting requirements under this Part.

(f) No Licensee shall engage in, facilitate, or knowingly allow the transfer or transmission of Virtual Currency when such action will obfuscate the identity of an individual customer or counterparty. Nothing in

this Section, however, shall be construed to require a Licensee to make available to the general public the fact or nature of the movement of Virtual Currency by individual customers or counterparties.

(g) Each Licensee shall also maintain, as part of its anti-money laundering program, a customer identification program.

(1) Identification and verification of account holders. When opening an account for a customer, each Licensee must, at a minimum, verify the customer's identity, to the extent reasonable and practicable, maintain records of the information used to verify such identity, including name, physical address, and other identifying information, and check customers against the Specially Designated Nationals ("SDNs") list maintained by the Office of Foreign Asset Control ("OFAC"), a part of the U.S. Treasury Department. Enhanced due diligence may be required based on additional factors, such as for high risk customers, high-volume accounts, or accounts on which a suspicious activity report has been filed.

(2) Enhanced due diligence for accounts involving foreign entities. Licensees that maintain accounts for non-U.S. Persons and non-U.S. Licensees must establish enhanced due diligence policies, procedures, and controls to detect money laundering, including assessing the risk presented by such accounts based on the nature of the foreign business, the type and purpose of the activity, and the anti-money laundering and supervisory regime of the foreign jurisdiction.

(3) Prohibition on accounts with foreign shell entities. Licensees are prohibited from maintaining relationships of any type in connection with their Virtual Currency Business Activity with entities that do not have a physical presence in any country.

(4) Identification required for large transactions. Each Licensee must require verification of accountholders initiating transactions having a value greater than $3,000.

(h) Each Licensee shall demonstrate that it has risk-based policies, procedures, and practices to ensure, to the maximum extent practicable, compliance with applicable regulations issued by OFAC.

(i) Each Licensee shall have in place appropriate policies and procedures to block or reject specific or impermissible transactions that violate federal or state laws, rules, or regulations.

(j) The individual(s) designated by the Licensee, pursuant to Subsection 200.15(b)(3), shall be responsible for day-to-day operations of the anti-money laundering program and shall, at a minimum:

(1) Monitor changes in anti-money laundering laws, including updated OFAC and SDN lists, and update the program accordingly;

(2) Maintain all records required to be maintained under this Section;

(3) Review all filings required under this Section before submission;

(4) Escalate matters to the board of directors, senior management, or appropriate governing body and seek outside counsel, as appropriate;

(5) Provide periodic reporting, at least annually, to the board of directors, senior management, or appropriate governing body; and

(6) Ensure compliance with relevant training requirements.

Statutory authority: Financial Services Law, sections 201, 202, 302, and 404

Section 200.16 Cyber security program

(a) Generally. Each Licensee shall establish and maintain an effective cyber security program to ensure the availability and functionality of the Licensee's electronic systems and to protect those systems and any sensitive data stored on those systems from unauthorized access, use, or tampering. The cyber security program shall be designed to perform the following five core cyber security functions:

(1) identify internal and external cyber risks by, at a minimum, identifying the information stored on the Licensee's systems, the sensitivity of such information, and how and by whom such information may be accessed;

(2) protect the Licensee's electronic systems, and the information stored on those systems, from unauthorized access, use, or other malicious acts through the use of defensive infrastructure and the implementation of policies and procedures;

(3) detect systems intrusions, data breaches, unauthorized access to systems or information, malware, and other Cyber Security Events;

(4) respond to detected Cyber Security Events to mitigate any negative effects; and

(5) recover from Cyber Security Events and restore normal operations and services.

(b) Policy. Each Licensee shall implement a written cyber security policy setting forth the Licensee's policies and procedures for the protection of its electronic systems and customer and counterparty data stored on those systems, which shall be reviewed and approved by the Licensee's board of directors or equivalent governing body at least annually. The cyber security policy must address the following areas:

(1) information security;

(2) data governance and classification;

(3) access controls;

(4) business continuity and disaster recovery planning and resources;

(5) capacity and performance planning;

(6) systems operations and availability concerns;

(7) systems and network security;

(8) systems and application development and quality assurance;

(9) physical security and environmental controls;

(10) customer data privacy;

(11) vendor and third-party service provider management;

(12) monitoring and implementing changes to core protocols not directly controlled by the Licensee, as applicable; and

(13) incident response.

(c) Chief Information Security Officer. Each Licensee shall designate a qualified employee to serve as the Licensee's Chief Information Security Officer ("CISO") responsible for overseeing and implementing the Licensee's cyber security program and enforcing its cyber security policy.

(d) Reporting. Each Licensee shall submit to the Department a report, prepared by the CISO and presented to the Licensee's board of directors or equivalent governing body, at least annually, assessing the availability, functionality, and integrity of the Licensee's electronic systems, identifying relevant cyber risks to the Licensee, assessing the Licensee's cyber security program, and proposing steps for the redress of any inadequacies identified therein.

(e) Audit. Each Licensee's cyber security program shall, at a minimum, include audit functions as set forth below.

(1) Penetration testing. Each Licensee shall conduct penetration testing of its electronic systems, at least annually, and vulnerability assessment of those systems, at least quarterly.

(2) Audit trail. Each Licensee shall maintain audit trail systems that:

(i) track and maintain data that allows for the complete and accurate reconstruction of all financial transactions and accounting;

(ii) protect the integrity of data stored and maintained as part of the audit trail from alteration or tampering;

(iii) protect the integrity of hardware from alteration or tampering, including by limiting access permissions to hardware, enclosing hardware in locked cages, and maintaining logs of physical access to hardware that allows for event reconstruction;

(iv) log system events including, at minimum, access and alterations made to the audit trail systems by the systems or by an authorized user, and all system administrator functions performed on the systems; and

(v) maintain records produced as part of the audit trail for a period of ten years in accordance with the recordkeeping requirements set forth in this Part.

(3) Source code reviews. Each Licensee shall have an independent, qualified third party conduct a source code review of any internally developed proprietary software used in the Licensee's business operations, at least annually.

(f) Personnel and Intelligence. Each Licensee shall:

(1) employ cyber security personnel adequate to manage the Licensee's cyber security risks and to perform the core cyber security functions specified in Subsection 200.16(a)(1)-(5);

(2) provide and require cyber security personnel to attend regular cyber security update and training sessions; and

(3) require key cyber security personnel to take steps to stay abreast of changing cyber security threats and countermeasures.

Statutory Authority: Financial Services Law, sections 102, 202, 301, and 302

Section 200.17 Business continuity and disaster recovery

(a) Each Licensee shall establish and maintain a written business continuity and disaster recovery ("BCDR") plan reasonably designed to ensure the availability and functionality of the Licensee's services in the event of an emergency or other disruption to the Licensee's normal business activities. The BCDR plan, at minimum, shall:

(1) identify documents, data, facilities, infrastructure, personnel, and competencies essential to the continued operations of the Licensee's business;

(2) identify the supervisory personnel responsible for implementing each aspect of the BCDR plan;

(3) include a plan to communicate with essential Persons in the event of an emergency or other disruption to the operations of the Licensee, including employees, counterparties, regulatory authorities, data and communication providers, disaster recovery specialists, and any other Persons essential to the recovery of documentation and data and the resumption of operations;

(4) include procedures for the maintenance of back-up facilities, systems, and infrastructure as well as alternative staffing and other resources to enable the timely recovery of data and documentation and to resume operations as soon as reasonably possible following a disruption to normal business activities;

(5) include procedures for the back-up or copying, with sufficient frequency, of documents and data essential to the operations of the Licensee and storing of the information off site; and

(6) identify third parties that are necessary to the continued operations of the Licensee's business.

(b) Each Licensee shall distribute a copy of the BCDR plan, and any revisions thereto, to all relevant employees and shall maintain copies of the BCDR plan at one or more accessible off-site locations.

(c) Each Licensee shall provide relevant training to all employees responsible for implementing the BCDR plan regarding their roles and responsibilities.

(d) Each Licensee shall promptly notify the superintendent of any emergency or other disruption to its operations that may affect its ability to fulfill regulatory obligations or that may have a significant adverse effect on the Licensee, its counterparties, or the market.

(e) The BCDR plan shall be tested at least annually by qualified, independent internal personnel or a qualified third party, and revised accordingly.

Statutory Authority: Financial Services Law, sections 102, 202, 301, and 302

Section 200.18 Advertising and marketing

(a) Each Licensee engaged in Virtual Currency Business Activity shall not advertise its products, services, or activities in New York or to New York Residents without including the name of the Licensee and the legend that such Licensee is "Licensed to engage in Virtual Currency Business Activity by the New York State Department of Financial Services."

(b) Each Licensee shall maintain, for examination by the superintendent, all advertising and marketing materials, including but not limited to print media, internet media (including websites), radio and television advertising, road show materials, presentations, and brochures. Each Licensee shall maintain hard copy, website captures, and audio and video scripts of its advertising and marketing materials, as applicable.

(c) In all advertising and marketing materials, each Licensee shall comply with all disclosure requirements under federal and state laws, rules, and regulations.

(d) In all advertising and marketing materials, each Licensee and any person or entity acting on its behalf, shall not, directly or by implication, make any false, misleading, or deceptive representations or omissions.

Statutory authority: Financial Services Law, sections 102, 202, 301, and 302

Section 200.19 Consumer protection

(a) Disclosure of material risks. As part of establishing a relationship with a customer, and prior to entering into an initial transaction for, on behalf of, or with such customer, each Licensee shall disclose in clear, conspicuous, and legible writing in the English language and in any other predominant language spoken by the customers of the Licensee, all material risks associated with its products, services, and activities and Virtual Currency generally, including at a minimum, the following:

(1) virtual currency is not legal tender, is not backed by the government, and accounts and value balances are not subject to Federal Deposit Insurance Corporation or Securities Investor Protection Corporation protections;

(2) legislative and regulatory changes or actions at the state, federal, or international level may adversely affect the use, transfer, exchange, and value of Virtual Currency;

(3) transactions in Virtual Currency are generally irreversible, and, accordingly, losses due to fraudulent or accidental transactions may not be recoverable;

(4) some Virtual Currency transactions shall be deemed to be made when recorded on a "block chain" ledger, which is not necessarily the date or time that the customer initiates the transaction;

(5) the value of Virtual Currency is derived from the continued willingness of market participants to exchange Fiat Currency for Virtual Currency, which may result in the potential for permanent and total loss of value of a particular Virtual Currency should the market for that Virtual Currency disappear;

(6) there is no assurance that a Person who accepts a Virtual Currency as payment today will continue to do so in the future;

(7) the volatility and unpredictability of the price of Virtual Currency relative to Fiat Currency may result in significant loss or tax liability over a short period of time;

(8) the nature of Virtual Currency may lead to an increased risk of fraud or cyber attack;

(9) the nature of Virtual Currency means that any technological difficulties experienced by the Licensee may prevent the access or use of a customer's Virtual Currency; and

(10) any bond or trust account for the benefit of customers may not be sufficient to cover any and all losses incurred by customers.

(b) Disclosure of general terms and conditions. When opening an account for a new customer, and prior to entering into an initial transaction for, on behalf of, or with such customer, each Licensee shall disclose in clear, conspicuous, and legible writing in the English language and in any other predominant language spoken by the customers of the Licensee, all relevant terms and conditions associated with its products, services, and activities and Virtual Currency generally, including at a minimum, the following, as applicable:

(1) the customer's liability for unauthorized Virtual Currency transactions;

(2) the customer's right to stop payment of a preauthorized Virtual Currency transfer and the procedure to initiate such a stop-payment order;

(3) the Licensee's liability to the customer under any applicable federal or state laws, rules, or regulations;

(4) under what circumstances the Licensee will, absent a court or government order, disclose information concerning the customer's account to third parties;

(5) the customer's right to receive periodic account statements and valuations from the Licensee;

(6) the customer's right to receive a receipt, trade ticket, or other evidence of a transaction;

(7) the customer's right to prior notice of a change in the Licensee's rules or policies; and

(8) such other disclosures as are customarily given in connection with the opening of customer accounts.

(c) Disclosures of the terms of transactions. Prior to each transaction in Virtual Currency, for, on behalf of, or with a customer, each Licensee shall furnish to each such customer a written disclosure in clear, conspicuous, and legible writing in the English language and in any other predominant language spoken by the customers of

the Licensee, containing the terms and conditions of the transaction, which shall include, at a minimum, to the extent applicable:

(1) the amount of the transaction;

(2) any fees, expenses, and charges borne by the customer, including applicable exchange rates;

(3) the type and nature of the Virtual Currency transaction;

(4) a warning that once executed the transaction may not be undone, if applicable; and

(5) such other disclosures as are customarily given in connection with a transaction of this nature.

(d) Acknowledgement of disclosures. Each Licensee shall ensure that all disclosures required in this Section are acknowledged as received by customers.

(e) Receipts. Upon completion of any transaction, each Licensee shall provide to a customer a receipt containing the following information:

(1) the name and contact information of the Licensee, including a telephone number established by the Licensee to answer questions and register complaints;

(2) the type, value, date, and precise time of the transaction;

(3) the fee charged;

(4) the exchange rate, if applicable;

(5) a statement of the liability of the Licensee for non-delivery or delayed delivery;

(6) a statement of the refund policy of the Licensee; and

(7) any additional information the superintendent may require.

(f) Each Licensee shall make available to the Department, upon request, the form of the receipts it is required to provide to customers in accordance with Subsection 200.19(e).

(g) Prevention of fraud. Licensees are prohibited from engaging in fraudulent activity and customers of Licensees that are victims of fraud shall be entitled to claim compensation from any trust account, bond, or

insurance policy maintained by the Licensee. Additionally, each Licensee shall take reasonable steps to detect and prevent fraud, including by establishing and maintaining a written anti-fraud policy. The anti-fraud policy shall, at a minimum, include:

(1) the identification and assessment of fraud-related risk areas;

(2) procedures and controls to protect against identified risks;

(3) allocation of responsibility for monitoring risks; and

(4) procedures for the periodic evaluation and revision of the anti-fraud procedures, controls, and monitoring mechanisms.

Statutory Authority: Financial Services Law, sections 102, 201, 202, 301, 302, 306, and 404

Section 200.20 Complaints

(a) Each Licensee shall establish and maintain written policies and procedures to fairly and timely resolve complaints.

(b) Each Licensee must provide, in a clear and conspicuous manner, on its website(s), in any physical location(s), and in any other location as the superintendent may prescribe, the following disclosures:

(1) the Licensee's mailing address, email address, and telephone number for the receipt of complaints;

(2) a statement that the complainant may also bring his or her complaint to the attention of the Department;

(3) the Department's mailing address, website, and telephone number; and

(4) such other information as the superintendent may require.

(c) Each Licensee shall report to the superintendent any change in the Licensee's complaint policies or procedures within seven days.

Statutory authority: Financial Services Law, sections 102, 201, 202, 301, and 302

Section 200.21 Transitional Period

A Person already engaged in Virtual Currency Business Activity must apply for a license in accordance with this Part within 45 days of the effective date of this regulation. In doing so, such applicant shall be deemed in compliance with the licensure requirements of this Part until it has been notified by the superintendent that its application has been denied, in which case it shall immediately cease operation in this state. Any Person engaged in Virtual Currency Business Activity that fails to submit an application for a license within 45 days of the effective date of this regulation shall be deemed to be conducting unlicensed Virtual Currency Business Activity.

Statutory authority: Financial Services Law, sections 202, 206, 302, 303, 305, 306, 309, 404, and 408; Executive Law, section 63.

Exhibit W

amazon.com

October 20, 2014

Mr. Dana V. Syracuse
Office of General Counsel
New York State Department of Financial Services
One State Street
New York, NY 10004

Re: Notice of Proposed Rulemaking for the Regulation of the Conduct of Virtual Currency Businesses I.D. No. DFS-29-14-00015-P

Dear Mr. Syracuse:

Amazon.com, Inc. ("Amazon") respectfully submits the following comments to the Notice of Proposed Rulemaking, I.D. No. DFS-29-14-00015-P ("Notice") issued by the New York State Department of Financial Services ("DFS"). Amazon appreciates the opportunity to comment upon the issues raised in the Notice.

The Notice would establish a regulatory licensing framework for virtual currency businesses engaged in certain types of activities involving New York or a New York resident. The Notice broadly defines "virtual currency."[1] It also contains two narrow exceptions for virtual currency used solely within online gaming platforms and virtual currency used exclusively as part of a customer affinity or rewards program that can only be applied towards purchases from the issuer or designated merchants and cannot be converted into or redeemed for fiat currency.[2]

Amazon recognizes the challenges faced by the DFS in issuing rules to regulate virtual currency in order to protect New York consumers and users and to ensure the safety and soundness of New York-licensed providers of virtual currency products and services. We are specifically concerned, however, that the broad definition of "virtual currency" may inadvertently result in certain products being captured and that the exceptions to this definition are too narrow to carve out such products. For the reasons discussed below, Amazon respectfully requests that the DFS expressly clarify that the following products are excluded

[1] "Virtual currency" would be defined in 23 N.Y.C.R.R. § 200.2(m) as follows: "*Virtual Currency* means any type of digital unit that is used as a medium of exchange or a form of digitally stored value or that is incorporated into payment system technology. Virtual Currency shall be broadly construed to include digital units of exchange that (i) have a centralized repository or administrator; (ii) are decentralized and have no centralized repository or administrator; or (iii) may be created or obtained by computing or manufacturing effort."

[2] *See* proposed 23 N.Y.C.R.R. § 200.2(m).

from the definition of "virtual currency" in its final rulemaking: (1) "closed-loop"[3] digital payment methods; and (2) prepaid access, stored value cards, or prepaid cards denominated in fiat currency. Clarifying that these products are excluded from the virtual currency regulations will ensure that consumers continue to have access to these popular payment methods, which do not pose the same money laundering or financial stability issues that cryptocurrencies and anonymous, tradeable virtual currencies pose to consumers and the financial system.

A. Closed-Loop Digital Payment Methods

Although the proposed definition of "virtual currency" excludes digital units that can be applied solely as payment for purchases with the issuer and/or other designated merchants, this closed-loop exclusion appears to be limited to digital units that are "used exclusively as part of a customer affinity or rewards program."[4] Merchants and their affiliates may choose to issue digital units that can be applied solely as payment for purchases with the issuer and/or other designated merchants (including affiliates of the issuer) that are not necessarily issued exclusively as part of a customer affinity or rewards program. For example, Amazon Coins and Google Play credits are digital units that can be purchased by customers to be used exclusively within the Amazon Appstore or Google Play app store, respectively. Amazon Coins and Google Play credits are not "used exclusively as part of a customer affinity or rewards program," but otherwise meet the remaining attributes of the proposed exclusion (*i.e.*, "can be applied solely as payment for purchases with the issuer and/or other designated merchants, but cannot be converted into, or redeemed for, Fiat Currency").

Closed-loop digital payment methods like Amazon Coins or Google Play credits are not virtual currency that the Notice intends to regulate. Other, similar regulatory frameworks contain exclusions for closed-loop products, and the applicability of such exclusions do not require the closed-loop product to be used exclusively as part of a customer affinity or rewards program.[5] Similar regulatory frameworks may also contain a separate express exclusion to cover

---

[3] The term "closed-loop" is typically used to describe a product, such as a prepaid card or digital currency that is issued by a single merchant or an affiliate of the merchant that is only accepted or honored by the issuer or its affiliates as payment for goods or services.

[4] *See* proposed 23 N.Y.C.R.R. § 200.2(m).

[5] For example, New York's money transmission statute and many other state money transmission statutes exclude from the definition of "payment instrument" and/or "stored value" instruments that are redeemable by the issuer and/or its affiliates for the purchase of goods or services. *See, e.g.*, N.Y. Bank. Law § 640(5); Cal. Fin. Code §§ 2003(q), (v); Tex. Fin. Code § 151.301(b)(6); Rev. Code Wash. §§ 19.230.010(6), (18). The Financial Crimes Enforcement Network's regulations relating to prepaid access also contains an exclusion for closed-loop products that does not require the closed-loop products to be used exclusively as part of a customer affinity or rewards program. 31 C.F.R. §1010.100(kkk) (defining *"Closed loop prepaid access"* as "[p]repaid access to funds or the value of funds that can be used only for goods or services in transactions involving a defined merchant or location (or set of locations), such as a specific retailer or retail chain, a college campus, or a subway system.").

rewards, incentive, or loyalty programs.[6] Amazon urges the DFS to clarify in its final rulemaking that the definition of "virtual currency" does not include digital units that can be applied solely as payment for purchases with the issuer and/or other designated merchants, but cannot be converted into, or redeemed for, fiat currency. In the absence of this clarification, issuers of closed-system payment methods might choose to discontinue them since complying with the full licensing regime would likely make these programs too expensive to continue to offer and cumbersome for customers to use.

B. Prepaid Access, Stored Value Cards, or Prepaid Cards

The broad definition of "virtual currency" may also inadvertently capture prepaid access products, stored value cards, or prepaid cards that are denominated in fiat currency and addressed under New York's Transmitters of Money statute (N.Y. Bank. Law, Article XIII-B).[7] To avoid any confusion, we believe it would provide clarity if the DFS expressly specified in the final rules that the definition of virtual currency does not include prepaid access products, stored value cards, or prepaid cards denominated in fiat currency. This will ensure that prepaid access products remain subject to one regulatory regime and that providers of these products can continue to rely on the interpretations and guidance provided by DFS regarding the status of these products under New York law.

* * * * * *

Thank you for your consideration of these comments. We would also be pleased to meet with the DFS to discuss these issues. If you have any questions, please feel free to contact me at [redacted]

Sincerely,

Cameron Cohen

Cameron Cohen
Associate General Counsel, Payments, Amazon.com, Inc.

---

[6] *See, e.g.*, La. Rev. Stat. § 6:1032(20); Tex. Fin. Code § 151.301(8).

[7] These products are currently analyzed under the definition of "payment instrument" in New York's Transmitters of Money statute. *See* N.Y. Bank. Law § 640(5).

Exhibit X

NEW YORK STATE

DEPARTMENT OF FINANCIAL SERVICES

NEW YORK CODES, RULES AND REGULATIONS

TITLE 23. DEPARTMENT OF FINANCIAL SERVICES

CHAPTER I. REGULATIONS OF THE SUPERINTENDENT OF FINANCIAL SERVICES

PART 200. VIRTUAL CURRENCIES

(ALL MATERIAL IS NEW)

Section 200.1 Introduction

This Part contains regulations relating to the conduct of business involving Virtual Currency, as defined herein, in accordance with the superintendent's powers pursuant to the above-stated authority.

Section 200.2 Definitions

For purposes of this Part only, the following definitions shall apply:

(a) *Affiliate* means any Person that directly or indirectly controls, is controlled by, or is under common control with, another Person;

(b) *Cyber Security Event* means any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt, or misuse a Licensee's electronic systems or information stored on such systems;

(c) *Department* means the New York State Department of Financial Services;

(d) *Exchange Service* means the conversion or exchange of Fiat Currency or other value into Virtual Currency, the conversion or exchange of Virtual Currency into Fiat Currency or other value, or the conversion or exchange of one form of Virtual Currency into another form of Virtual Currency;

(e) *Fiat Currency* means government-issued currency that is designated as legal tender in its country of issuance through government decree, regulation, or law;

(f) *Licensee* means any Person duly licensed by the superintendent pursuant to this Part;

(g) *New York* means the State of New York;

(h) *New York Resident* means any Person that resides, is located, has a place of business, or is conducting business in New York;

(i) *Person* means an individual, partnership, corporation, association, joint stock association, trust, or other entity, however organized;

(j) *Prepaid Card* means an electronic payment device that: (i) is usable at a single merchant or an affiliated group of merchants that share the same name, mark, or logo, or is usable at multiple, unaffiliated merchants or service providers; (ii) is issued in and for a specified amount of Fiat Currency; (iii) can be reloaded in and for only Fiat Currency, if at all; (iv) is issued and/or reloaded on a prepaid basis for the future purchase or delivery

of goods or services; (v) is honored upon presentation; and (vi) can be redeemed in and for only Fiat Currency, if at all;

(k) *Principal Officer* means an executive officer of an entity, including, but not limited to, the chief executive, financial, operating, and compliance officers, president, general counsel, managing partner, general partner, controlling partner, and trustee, as applicable;

(l) *Principal Stockholder* means any Person that directly or indirectly owns, controls, or holds with power to vote ten percent or more of any class of outstanding capital stock or other equity interest of an entity or possesses the power to direct or cause the direction of the management or policies of the entity;

(m) *Principal Beneficiary* means any Person entitled to ten percent or more of the benefits of a trust;

(n) *Qualified Custodian* means a bank, trust company, national bank, savings bank, savings and loan association, federal savings association, credit union, or federal credit union in the State of New York, subject to the prior approval of the superintendent. To the extent applicable, terms used in this definition shall have the meaning ascribed by the Banking Law;

(o) *Transmission* means the transfer, by or through a third party, of Virtual Currency from a Person to a Person, including the transfer from the account or storage repository of a Person to the account or storage repository of a Person;

(p) *Virtual Currency* means any type of digital unit that is used as a medium of exchange or a form of digitally stored value. Virtual Currency shall be broadly construed to include digital units of exchange that (i) have a centralized repository or administrator; (ii) are decentralized and have no centralized repository or administrator; or (iii) may be created or obtained by computing or manufacturing effort. Virtual Currency shall not be construed to include any of the following:

(1) digital units that (i) are used solely within online gaming platforms, (ii) have no market or application outside of those gaming platforms, (iii) cannot be converted into, or redeemed for, Fiat Currency or

Virtual Currency, and (iv) may or may not be redeemable for real-world goods, services, discounts, or purchases.

(2) digital units that can be redeemed for goods, services, discounts, or purchases as part of a customer affinity or rewards program with the issuer and/or other designated merchants or can be redeemed for digital units in another customer affinity or rewards program, but cannot be converted into, or redeemed for, Fiat Currency or Virtual Currency; or

(3) digital units used as part of Prepaid Cards;

(q) *Virtual Currency Business Activity* means the conduct of any one of the following types of activities involving New York or a New York Resident:

(1) receiving Virtual Currency for Transmission or Transmitting Virtual Currency, except where the transaction is undertaken for non-financial purposes and does not involve the transfer of more than a nominal amount of Virtual Currency;

(2) storing, holding, or maintaining custody or control of Virtual Currency on behalf of others;

(3) buying and selling Virtual Currency as a customer business;

(4) performing Exchange Services as a customer business; or

(5) controlling, administering, or issuing a Virtual Currency.

The development and dissemination of software in and of itself does not constitute Virtual Currency Business Activity.

Section 200.3 License

(a) License required. No Person shall, without a license obtained from the superintendent as provided in this Part, engage in any Virtual Currency Business Activity. Licensees are not authorized to exercise fiduciary powers, as defined under Section 100 of the Banking Law.

(b) Unlicensed agents prohibited. Each Licensee is prohibited from conducting any Virtual Currency Business Activity through an agent or agency arrangement when the agent is not a Licensee.

(c) Exemption from licensing requirements. The following Persons are exempt from the licensing requirements otherwise applicable under this Part:

(1) Persons that are chartered under the New York Banking Law and are approved by the superintendent to engage in Virtual Currency Business Activity; and

(2) merchants and consumers that utilize Virtual Currency solely for the purchase or sale of goods or services or for investment purposes.

Section 200.4 Application

(a) Application for a license required under this Part shall be in writing, under oath, and in a form prescribed by the superintendent, and shall contain the following:

(1) the exact name of the applicant, including any doing business as name, the form of organization, the date of organization, and the jurisdiction where organized or incorporated;

(2) a list of all of the applicant's Affiliates and an organization chart illustrating the relationship among the applicant and such Affiliates;

(3) a list of, and detailed biographical information for, each individual applicant and each director, Principal Officer, Principal Stockholder, and Principal Beneficiary of the applicant, as applicable, including such individual's name, physical and mailing addresses, and information and documentation regarding such individual's personal history, experience, and qualification, which shall be accompanied by a form of authority, executed by such individual, to release information to the Department;

(4) a background report prepared by an independent investigatory agency acceptable to the superintendent for each individual applicant, and each Principal Officer, Principal Stockholder, and Principal Beneficiary of the applicant, as applicable;

(5) for each individual applicant; for each Principal Officer, Principal Stockholder, and Principal Beneficiary of the applicant, as applicable; and for all individuals to be employed by the applicant who have access to any customer funds, whether denominated in Fiat Currency or Virtual Currency: (i) a set of completed fingerprints, or a receipt indicating the vendor (which vendor must be acceptable to the superintendent) at which, and the date when, the fingerprints were taken, for submission to the State Division of Criminal Justice Services and the Federal Bureau of Investigation; (ii) if applicable, such processing fees as prescribed by the superintendent; and (iii) two portrait-style photographs of the individuals measuring not more than two inches by two inches;

(6) an organization chart of the applicant and its management structure, including its Principal Officers or senior management, indicating lines of authority and the allocation of duties among its Principal Officers or senior management;

(7) a current financial statement for the applicant and each Principal Officer, Principal Stockholder, and Principal Beneficiary of the applicant, as applicable, and a projected balance sheet and income statement for the following year of the applicant's operation;

(8) a description of the proposed, current, and historical business of the applicant, including detail on the products and services provided and to be provided, all associated website addresses, the jurisdictions in which the applicant is engaged in business, the principal place of business, the primary market of operation, the projected customer base, any specific marketing targets, and the physical address of any operation in New York;

(9) details of all banking arrangements;

(10) all written policies and procedures required by, or related to, the requirements of this Part;

(11) an affidavit describing any pending or threatened administrative, civil, or criminal action, litigation, or proceeding before any governmental agency, court, or arbitration tribunal against the applicant or any of its directors, Principal Officers, Principal Stockholders, and Principal Beneficiaries, as applicable, including the names of the parties, the nature of the proceeding, and the current status of the proceeding;

(12) verification from the New York State Department of Taxation and Finance that the applicant is compliant with all New York State tax obligations in a form acceptable to the superintendent;

(13) if applicable, a copy of any insurance policies maintained for the benefit of the applicant, its directors or officers, or its customers;

(14) an explanation of the methodology used to calculate the value of Virtual Currency in Fiat Currency; and

(15) such other additional information as the superintendent may require.

(b) As part of such application, the applicant shall demonstrate that it will be compliant with all of the requirements of this Part upon licensing.

(c) Notwithstanding Subsection (b) of this Section, the superintendent may in his or her sole discretion and consistent with the purposes and intent of the Financial Services Law and this Part approve an application by granting a conditional license.

(1) A conditional license may be issued to an applicant that does not satisfy all of the regulatory requirements upon licensing.

(2) A Licensee that holds a conditional license may be subject to heightened review, whether in regard to the scope and frequency of examination or otherwise.

(3) Unless the superintendent removes the conditional status of or renews a conditional license, said license shall expire two years after its date of issuance.

i) The superintendent may in his or her sole discretion and consistent with the purposes and intent of the Financial Services Law and this Part:

(A) renew a conditional license for an additional length of time; or

(B) remove the conditional status from a conditional license.

(4) A conditional license may be suspended or revoked pursuant to Section 200.6 of this Part.

(5) A conditional license may impose any reasonable condition or conditions, as determined by the superintendent in his or her sole discretion.

(6) The superintendent may remove any condition or conditions from a conditional license that has been issued.

(7) In determining whether to issue a conditional license, renew or remove the conditional status of a conditional license, or impose or remove any specific conditions on a conditional license, the superintendent may consider any relevant factor or factors. Relevant factors may include but are not limited to:

i) the nature and scope of the applicant's or Licensee's business;

ii) the anticipated volume of business to be transacted by the applicant or Licensee;

iii) the nature and scope of the risks that the applicant's or Licensee's business presents to consumers, Virtual Currency markets, financial markets, and the general public;

iv) the measures which the applicant or Licensee has taken to limit or mitigate the risks its business presents;

v) whether the applicant or Licensee is registered with FinCEN;

vi) whether the applicant or Licensee is licensed, registered, or otherwise authorized by any governmental or self-regulatory authority to engage in financial services or other business activities;

vii) the applicant's or Licensee's financial services or other business experience; and

viii) the Licensee's history as a holder of a conditional license issued by the superintendent.

(d) The superintendent may permit that any application for a license under this Part, or any other submission required by this Part, be made or executed by electronic means.

Section 200.5 Application fees

As part of an application for licensing under this Part, each applicant must submit an initial application fee, in the amount of five thousand dollars, to cover the cost of processing the application, reviewing application materials, and investigating the financial condition and responsibility, financial and business experience, and character and general fitness of the applicant. If the application is denied or withdrawn, such fee shall not be refunded. Each Licensee may be required to pay fees to the Department to process additional applications related to the license.

Section 200.6 Action by superintendent

(a) Generally. Upon the filing of an application for licensing under this Part, payment of the required fee, and demonstration by the applicant of its ability to comply with the provisions of this Part upon licensing, the superintendent shall investigate the financial condition and responsibility, financial and business experience, and character and general fitness of the applicant. If the superintendent finds these qualities are such as to warrant the belief that the applicant's business will be conducted honestly, fairly, equitably, carefully, and efficiently within the purposes and intent of this Part, and in a manner commanding the confidence and trust of the community, the superintendent shall advise the applicant in writing of his or her approval of the application, and shall issue to the applicant a license to conduct Virtual Currency Business Activity, subject to the provisions of this Part and such other conditions as the superintendent shall deem appropriate; or the superintendent may deny the application.

(b) Approval or denial of application. The superintendent shall approve or deny every application for a license hereunder within 90 days from the filing of an application deemed by the superintendent to be complete. Such period of 90 days may be extended at the discretion of the superintendent for such additional reasonable period of time as may be required to enable compliance with this Part. A license issued pursuant to this Part shall remain in full force and effect until it is surrendered by the Licensee, is revoked or suspended, or expires as provided in this Part.

(c) Suspension or revocation of license. The superintendent may suspend or revoke a license issued under this Part on any ground on which the superintendent might refuse to issue an original license, for a violation of any provision of this Part, for good cause shown, or for failure of the Licensee to pay a judgment, recovered in any court, within or without this State, by a claimant or creditor in an action arising out of, or relating to, the Licensee's Virtual Currency Business Activity, within thirty days after the judgment becomes final or within thirty days after expiration or termination of a stay of execution thereon; provided, however, that if execution on

the judgment is stayed, by court order or operation of law or otherwise, then proceedings to suspend or revoke the license (for failure of the Licensee to pay such judgment) may not be commenced by the superintendent during the time of such stay, and for thirty days thereafter. "Good cause" shall exist when a Licensee has defaulted or is likely to default in performing its obligations or financial engagements or engages in unlawful, dishonest, wrongful, or inequitable conduct or practices that may cause harm to the public.

(d) Hearing. No license issued under this Part shall be revoked or suspended except after a hearing thereon. The superintendent shall give a Licensee no less than ten days' written notice of the time and place of such hearing by registered or certified mail addressed to the principal place of business of such Licensee. Any order of the superintendent suspending or revoking such license shall state the grounds upon which it is based and be sent by registered or certified mail to the Licensee at its principal place of business as shown in the records of the Department.

(e) Preliminary injunction. The superintendent may, when deemed by the superintendent to be in the public interest, seek a preliminary injunction to restrain a Licensee from continuing to perform acts that violate any provision of this Part, the Financial Services Law, Banking Law, or Insurance Law.

(f) Preservation of powers. Nothing in this Part shall be construed as limiting any power granted to the superintendent under any other provision of the Financial Services Law, Banking Law, or Insurance Law, including any power to investigate possible violations of law, rule, or regulation or to impose penalties or take any other action against any Person for violation of such laws, rules, or regulations.

Section 200.7 Compliance

(a) Generally. Each Licensee is required to comply with all applicable federal and state laws, rules, and regulations.

(b) Compliance officer. Each Licensee shall designate a qualified individual or individuals responsible for coordinating and monitoring compliance with this Part and all other applicable federal and state laws, rules, and regulations.

(c) Compliance policy. Each Licensee shall maintain and enforce written compliance policies, including policies with respect to anti-fraud, anti-money laundering, cyber security, privacy and information security, and any other policy required under this Part, which must be reviewed and approved by the Licensee's board of directors or an equivalent governing body.

Section 200.8 Capital requirements

(a) Each Licensee shall maintain at all times such capital in an amount and form as the superintendent determines is sufficient to ensure the financial integrity of the Licensee and its ongoing operations based on an assessment of the specific risks applicable to each Licensee. In determining the minimum amount of capital that must be maintained by a Licensee, the superintendent may consider a variety of factors, including but not limited to:

(1) the composition of the Licensee's total assets, including the position, size, liquidity, risk exposure, and price volatility of each type of asset;

(2) the composition of the Licensee's total liabilities, including the size and repayment timing of each type of liability;

(3) the actual and expected volume of the Licensee's Virtual Currency Business Activity;

(4) whether the Licensee is already licensed or regulated by the superintendent under the Financial Services Law, Banking Law, or Insurance Law, or otherwise subject to such laws as a provider of a financial product or service, and whether the Licensee is in good standing in such capacity;

(5) the amount of leverage employed by the Licensee;

(6) the liquidity position of the Licensee;

(7) the financial protection that the Licensee provides for its customers through its trust account or bond;

(8) the types of entities to be serviced by the Licensee; and

(9) the types of products or services to be offered by the Licensee.

(b) Each Licensee shall hold capital required to be maintained in accordance with this Section in the form of cash, virtual currency, or high-quality, highly liquid, investment-grade assets, in such proportions as are acceptable to the superintendent.

Section 200.9 Custody and protection of customer assets

(a) Each Licensee shall maintain a surety bond or trust account in United States dollars for the benefit of its customers in such form and amount as is acceptable to the superintendent for the protection of the Licensee's customers. To the extent a Licensee maintains a trust account in accordance with this section, such trust account must be maintained with a Qualified Custodian.

(b) To the extent a Licensee stores, holds, or maintains custody or control of Virtual Currency on behalf of another Person, such Licensee shall hold Virtual Currency of the same type and amount as that which is owed or obligated to such other Person.

(c) Each Licensee is prohibited from selling, transferring, assigning, lending, hypothecating, pledging, or otherwise using or encumbering assets, including Virtual Currency, stored, held, or maintained by, or under the custody or control of, such Licensee on behalf of another Person except for the sale, transfer, or assignment of such assets at the direction of such other Person.

Section 200.10 Material change to business

(a) Each Licensee must obtain the superintendent's prior written approval for any plan or proposal to introduce or offer a materially new product, service, or activity, or to make a material change to an existing product, service, or activity, involving New York or New York Residents.

(b) A "materially new product, service, or activity" or a "material change" may occur where:

(1) the proposed new product, service, or activity, or the proposed change may raise a legal or regulatory issue about the permissibility of the product, service, or activity;

(2) the proposed new product, service, or activity, or the proposed change may raise safety and soundness or operational concerns; or

(3) a change is proposed to an existing product, service, or activity that may cause such product, service, or activity to be materially different from that previously listed on the application for licensing by the superintendent.

(c) The Licensee shall submit a written plan describing the proposed materially new product, service, or activity, or the proposed material change, including a detailed description of the business operations, compliance policies, and the impact on the overall business of the Licensee, as well as such other information as requested by the superintendent.

(d) If a Licensee has any questions about the materiality of any proposed new product, service, or activity, or of any proposed change, the Licensee may seek clarification from the Department prior to introducing or offering that new product, service, or activity or making that change.

Section 200.11 Change of control; mergers and acquisitions

(a) Change of Control. No action shall be taken, except with the prior written approval of the superintendent, that may result in a change of control of a Licensee.

(1) Prior to any change of control, the Person seeking to acquire control of a Licensee shall submit a written application to the superintendent in a form and substance acceptable to the superintendent, including but not limited to detailed information about the applicant and all directors, Principal Officers, Principal Stockholders, and Principal Beneficiaries of the applicant, as applicable.

(2) For purposes of this Section, the term “control” means the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of a Licensee whether through the ownership of stock of such Licensee, the stock of any Person that possesses such power, or otherwise. Control shall be presumed to exist if a Person, directly or indirectly, owns, controls, or holds with power to vote ten percent or more of the voting stock of a Licensee or of any Person that owns, controls, or holds with power to vote ten percent or more of the voting stock of such Licensee. No Person shall be deemed to control another Person solely by reason of his being an officer or director of such other Person.

(3) The superintendent may determine upon application that any Person does not or will not upon the taking of some proposed action control another Person. Such determination shall be made within 30 days or such further period as the superintendent may prescribe. The filing of an application pursuant to this Subsection in good faith by any Person shall relieve the applicant from any obligation or liability imposed by this Section with respect to the subject of the application until the superintendent has acted upon the application. The superintendent may revoke or modify his or her determination, after notice and opportunity to be heard, whenever in his or her judgment revocation or modification is consistent with this Part. The superintendent may consider the following factors in making such a determination:

i) whether such Person's purchase of common stock is made solely for investment purposes and not to acquire control over the Licensee;

ii) whether such Person could direct, or cause the direction of, the management or policies of the Licensee;

iii) whether such Person could propose directors in opposition to nominees proposed by the management or board of directors of the Licensee;

iv) whether such Person could seek or accept representation on the board of directors of the Licensee;

v) whether such Person could solicit or participate in soliciting proxy votes with respect to any matter presented to the shareholders of the Licensee; or

vi) any other factor that indicates such Person would or would not exercise control of the Licensee.

(4) The superintendent shall approve or deny every application for a change of control of a Licensee hereunder within 120 days from the filing of an application deemed by the superintendent to be complete. Such period of 120 days may be extended by the superintendent, for good cause shown, for such additional reasonable period of time as may be required to enable compliance with the requirements and conditions of this Part.

(5) In determining whether to approve a proposed change of control, the superintendent shall, among other factors, take into consideration the public interest and the needs and convenience of the public.

(b) Mergers and Acquisitions. No action shall be taken, except with the prior written approval of the superintendent, that may result in a merger or acquisition of all or a substantial part of the assets of a Licensee.

(1) Prior to any such merger or acquisition, an application containing a written plan of merger or acquisition shall be submitted to the superintendent by the entities that are to merge or by the acquiring entity, as applicable. Such plan shall be in form and substance satisfactory to the superintendent, and shall specify

each entity to be merged, the surviving entity, or the entity acquiring all or substantially all of the assets of the Licensee, as applicable, and shall describe the terms and conditions of the merger or acquisition and the mode of carrying it into effect.

(2) The superintendent shall approve or deny a proposed merger or a proposed acquisition of all or a substantial part of the assets of a Licensee within 120 days after the filing of an application that contains a written plan of merger or acquisition and is deemed by the superintendent to be complete. Such period of 120 days may be extended by the superintendent, for good cause shown, for such additional reasonable period of time as may be required to enable compliance with the requirements and conditions of this Part.

(3) In determining whether to so approve a proposed merger or acquisition, the superintendent shall, among other factors, take into consideration the public interest and the needs and convenience of the public.

Section 200.12 Books and records

(a) Each Licensee shall, in connection with its Virtual Currency Business Activity, make, keep, and preserve all of its books and records in their original form or native file format for a period of at least seven years from the date of their creation and in a condition that will allow the superintendent to determine whether the Licensee is complying with all applicable laws, rules, and regulations. The books and records maintained by each Licensee shall, without limitation, include:

(1) for each transaction, the amount, date, and precise time of the transaction, any payment instructions, the total amount of fees and charges received and paid to, by, or on behalf of the Licensee, and the names, account numbers, and physical addresses of (i) the party or parties to the transaction that are customers or accountholders of the Licensee; and (ii) to the extent practicable, any other parties to the transaction;

(2) a general ledger containing all asset, liability, ownership equity, income, and expense accounts;

(3) bank statements and bank reconciliation records;

(4) any statements or valuations sent or provided to customers and counterparties;

(5) records or minutes of meetings of the board of directors or an equivalent governing body;

(6) records demonstrating compliance with applicable state and federal anti-money laundering laws, rules, and regulations, including customer identification and verification documents, records linking customers to their respective accounts and balances, and a record of all compliance breaches;

(7) communications and documentation related to investigations of customer complaints and transaction error resolution or concerning facts giving rise to possible violations of laws, rules, or regulations;

(8) all other records required to be maintained in accordance with this Part; and

(9) all other records as the superintendent may require.

(b) Each Licensee shall provide the Department, upon request, immediate access to all facilities, books, records, documents, or other information maintained by the Licensee or its Affiliates, wherever located.

(c) Records of non-completed, outstanding, or inactive Virtual Currency accounts or transactions shall be maintained for at least five years after the time when any such Virtual Currency has been deemed, under the Abandoned Property Law, to be abandoned property.

Section 200.13 Examinations

(a) Each Licensee shall permit and assist the superintendent to examine the Licensee whenever in the superintendent's judgment such examination is necessary or advisable, but not less than once every two calendar years, including, without limitation, to determine:

(1) the financial condition of the Licensee;

(2) the safety and soundness of the conduct of its business;

(3) the policies of its management;

(4) whether the Licensee has complied with the requirements of laws, rules, and regulations; and

(5) such other matters as the superintendent may determine, including, but not limited to, any activities of the Licensee outside the State of New York if in the opinion of the superintendent such activities may affect the Licensee's Virtual Currency Business Activity.

(b) Each Licensee shall permit and assist the superintendent at any time to examine all of the Licensee's books, records, accounts, documents, and other information.

(c) Each Licensee shall permit and assist the superintendent to make such special investigations as the superintendent shall deem necessary to determine whether a Licensee has violated any provision of the applicable laws, rules, or regulations and to the extent necessary shall permit and assist the superintendent to examine all relevant facilities, books, records, accounts, documents, and other information.

(d) For the purpose of determining the financial condition of the Licensee, its safety and soundness practices, or whether it has complied with the requirements of laws, rules, and regulations, the Licensee shall permit and assist the superintendent, when in the superintendent's judgment it is necessary or advisable, to examine an Affiliate of the Licensee.

Section 200.14 Reports and financial disclosures

(a) Each Licensee shall submit to the superintendent quarterly financial statements within 45 days following the close of the Licensee's fiscal quarter in the form, and containing such information, as the superintendent shall prescribe, including without limitation, the following information:

(1) a statement of the financial condition of the Licensee, including a balance sheet, income statement, statement of comprehensive income, statement of change in ownership equity, cash flow statement, and statement of net liquid assets;

(2) a statement demonstrating compliance with any financial requirements established under this Part;

(3) financial projections and strategic business plans;

(4) a list of all off-balance sheet items;

(5) a chart of accounts, including a description of each account; and

(6) a report of permissible investments by the Licensee as permitted under this Part.

(b) Each Licensee shall submit audited annual financial statements, together with an opinion and an attestation by an independent certified public accountant regarding the effectiveness of the Licensee's internal control structure. All such annual financial statements shall include:

(1) a statement of management's responsibilities for preparing the Licensee's annual financial statements, establishing and maintaining adequate internal controls and procedures for financial reporting, and complying with all applicable laws, rules, and regulations;

(2) an assessment by management of the Licensee's compliance with such applicable laws, rules, and regulations during the fiscal year covered by the financial statements; and

(3) certification of the financial statements by an officer or director of the Licensee attesting to the truth and correctness of those statements.

(c) Each Licensee shall notify the superintendent in writing of any criminal action or insolvency proceeding against the Licensee or any of its directors, Principal Stockholders, Principal Officers, and Principal Beneficiaries, as applicable, immediately after the commencement of any such action or proceeding.

(d) Each Licensee shall notify the superintendent in writing of any proposed change to the methodology used to calculate the value of Virtual Currency in Fiat Currency that was submitted to the Department in accordance with Section 200.4 or this Subsection.

(e) Each Licensee shall submit a report to the superintendent immediately upon the discovery of any violation or breach of law, rule, or regulation related to the conduct of activity licensed under this Part.

(f) Each Licensee shall make additional special reports to the superintendent, at such times and in such form, as the superintendent may request.

Section 200.15 Anti-money laundering program

(a) All values in United States dollars referenced in this Section must be calculated using the methodology to determine the value of Virtual Currency in Fiat Currency that was provided to the Department under this Part.

(b) Each Licensee shall conduct an initial risk assessment that will consider legal, compliance, financial, and reputational risks associated with the Licensee's activities, services, customers, counterparties, and geographic location and shall establish, maintain, and enforce an anti-money laundering program based thereon. The Licensee shall conduct additional assessments on an annual basis, or more frequently as risks change, and shall modify its anti-money laundering program as appropriate to reflect any such changes.

(c) The anti-money laundering program shall, at a minimum:

(1) provide for a system of internal controls, policies, and procedures designed to ensure ongoing compliance with all applicable anti-money laundering laws, rules, and regulations;

(2) provide for independent testing for compliance with, and the effectiveness of, the anti-money laundering program to be conducted by qualified internal personnel of the Licensee, who are not responsible for the design, installation, maintenance, or operation of the anti-money laundering program, or the policies and procedures that guide its operation, or a qualified external party, at least annually, the findings of which shall be summarized in a written report submitted to the superintendent;

(3) designate a qualified individual or individuals in compliance responsible for coordinating and monitoring day-to-day compliance with the anti-money laundering program; and

(4) provide ongoing training for appropriate personnel to ensure they have a fulsome understanding of anti-money laundering requirements and to enable them to identify transactions required to be reported and maintain records required to be kept in accordance with this Part.

(d) The anti-money laundering program shall include a written anti-money laundering policy reviewed and approved by the Licensee's board of directors or equivalent governing body.

(e) Each Licensee, as part of its anti-money laundering program, shall maintain records and make reports in the manner set forth below.

(1) Records of Virtual Currency transactions. Each Licensee shall maintain the following information for all Virtual Currency transactions involving the payment, receipt, exchange, conversion, purchase, sale, transfer, or transmission of Virtual Currency:

i) the identity and physical addresses of the party or parties to the transaction that are customers or accountholders of the Licensee and, to the extent practicable, any other parties to the transaction;

ii) the amount or value of the transaction, including in what denomination purchased, sold, or transferred;

iii) the method of payment;

iv) the date or dates on which the transaction was initiated and completed; and

v) a description of the transaction.

(2) Reports on transactions. When a Licensee is involved in a Virtual Currency to Virtual Currency transaction or series of Virtual Currency to Virtual Currency transactions that are not subject to currency transaction reporting requirements under federal law, including transactions for the payment, receipt, exchange, conversion, purchase, sale, transfer, or transmission of Virtual Currency, in an aggregate amount exceeding the United States dollar value of $10,000 in one day, by one Person, the Licensee shall notify the Department, in a manner prescribed by the superintendent, within 24 hours.

(3) Monitoring for suspicious activity. Each Licensee shall monitor for transactions that might signify money laundering, tax evasion, or other illegal or criminal activity.

(i) Each Licensee shall file Suspicious Activity Reports ("SARs") in accordance with applicable federal laws, rules, and regulations.

(ii) Each Licensee that is not subject to suspicious activity reporting requirements under federal law shall file with the superintendent, in a form prescribed by the superintendent, reports of transactions that indicate a possible violation of law or regulation within 30 days from the detection of the facts that constitute a need for filing. Continuing suspicious activity shall be reviewed on an ongoing basis and a suspicious activity report shall be filed within 120 days of the last filing describing continuing activity.

(f) No Licensee shall structure transactions, or assist in the structuring of transactions, to evade reporting requirements under this Part.

(g) No Licensee shall engage in, facilitate, or knowingly allow the transfer or transmission of Virtual Currency when such action will obfuscate or conceal the identity of an individual customer or counterparty. Nothing in this Section, however, shall be construed to require a Licensee to make available to the general public the fact or nature of the movement of Virtual Currency by individual customers or counterparties.

(h) Each Licensee shall also maintain, as part of its anti-money laundering program, a customer identification program.

(1) Identification and verification of account holders. When opening an account for, or establishing a service relationship with, a customer, each Licensee must, at a minimum, verify the customer's identity, to the extent reasonable and practicable, maintain records of the information used to verify such identity, including name, physical address, and other identifying information, and check customers against the Specially Designated Nationals ("SDNs") list maintained by the Office of Foreign Asset Control ("OFAC"), a part of the U.S. Treasury Department. Enhanced due diligence may be required based on additional factors, such as for high risk customers, high-volume accounts, or accounts on which a suspicious activity report has been filed.

(2) Enhanced due diligence for accounts involving foreign entities. Licensees that maintain accounts for non-U.S. Persons and non-U.S. Licensees must establish enhanced due diligence policies, procedures, and controls to detect money laundering, including assessing the risk presented by such accounts based on the nature of the foreign business, the type and purpose of the activity, and the anti-money laundering and supervisory regime of the foreign jurisdiction.

(3) Prohibition on accounts with foreign shell entities. Licensees are prohibited from maintaining relationships of any type in connection with their Virtual Currency Business Activity with entities that do not have a physical presence in any country.

(4) Identification required for large transactions. Each Licensee must require verification of the identity of any accountholder initiating a transaction with a value greater than $3,000.

(i) Each Licensee shall demonstrate that it has risk-based policies, procedures, and practices to ensure, to the maximum extent practicable, compliance with applicable regulations issued by OFAC.

(j) Each Licensee shall have in place appropriate policies and procedures to block or reject specific or impermissible transactions that violate federal or state laws, rules, or regulations.

(k) The individual or individuals designated by the Licensee, pursuant to Paragraph 200.15(c)(3), shall be responsible for day-to-day operations of the anti-money laundering program and shall, at a minimum:

(1) Monitor changes in anti-money laundering laws, including updated OFAC and SDN lists, and update the program accordingly;

(2) Maintain all records required to be maintained under this Section;

(3) Review all filings required under this Section before submission;

(4) Escalate matters to the board of directors, senior management, or appropriate governing body and seek outside counsel, as appropriate;

(5) Provide periodic reporting, at least annually, to the board of directors, senior management, or appropriate governing body; and

(6) Ensure compliance with relevant training requirements.

Section 200.16 Cyber security program

(a) Generally. Each Licensee shall establish and maintain an effective cyber security program to ensure the availability and functionality of the Licensee's electronic systems and to protect those systems and any sensitive data stored on those systems from unauthorized access, use, or tampering. The cyber security program shall be designed to perform the following five core cyber security functions:

(1) identify internal and external cyber risks by, at a minimum, identifying the information stored on the Licensee's systems, the sensitivity of such information, and how and by whom such information may be accessed;

(2) protect the Licensee's electronic systems, and the information stored on those systems, from unauthorized access, use, or other malicious acts through the use of defensive infrastructure and the implementation of policies and procedures;

(3) detect systems intrusions, data breaches, unauthorized access to systems or information, malware, and other Cyber Security Events;

(4) respond to detected Cyber Security Events to mitigate any negative effects; and

(5) recover from Cyber Security Events and restore normal operations and services.

(b) Policy. Each Licensee shall implement a written cyber security policy setting forth the Licensee's policies and procedures for the protection of its electronic systems and customer and counterparty data stored on those systems, which shall be reviewed and approved by the Licensee's board of directors or equivalent governing body at least annually. The cyber security policy must address the following areas:

(1) information security;

(2) data governance and classification;

(3) access controls;

(4) business continuity and disaster recovery planning and resources;

(5) capacity and performance planning;

(6) systems operations and availability concerns;

(7) systems and network security;

(8) systems and application development and quality assurance;

(9) physical security and environmental controls;

(10) customer data privacy;

(11) vendor and third-party service provider management;

(12) monitoring and implementing changes to core protocols not directly controlled by the Licensee, as applicable; and

(13) incident response.

(c) Chief Information Security Officer. Each Licensee shall designate a qualified employee to serve as the Licensee's Chief Information Security Officer ("CISO") responsible for overseeing and implementing the Licensee's cyber security program and enforcing its cyber security policy.

(d) Reporting. Each Licensee shall submit to the Department a report, prepared by the CISO and presented to the Licensee's board of directors or equivalent governing body, at least annually, assessing the availability, functionality, and integrity of the Licensee's electronic systems, identifying relevant cyber risks to the Licensee, assessing the Licensee's cyber security program, and proposing steps for the redress of any inadequacies identified therein.

(e) Audit. Each Licensee's cyber security program shall, at a minimum, include audit functions as set forth below.

(1) Penetration testing. Each Licensee shall conduct penetration testing of its electronic systems, at least annually, and vulnerability assessment of those systems, at least quarterly.

(2) Audit trail. Each Licensee shall maintain audit trail systems that:

(i) track and maintain data that allows for the complete and accurate reconstruction of all financial transactions and accounting;

(ii) protect the integrity of data stored and maintained as part of the audit trail from alteration or tampering;

(iii) protect the integrity of hardware from alteration or tampering, including by limiting electronic and physical access permissions to hardware and maintaining logs of physical access to hardware that allows for event reconstruction;

(iv) log system events including, at minimum, access and alterations made to the audit trail systems by the systems or by an authorized user, and all system administrator functions performed on the systems; and

(v) maintain records produced as part of the audit trail in accordance with the recordkeeping requirements set forth in this Part.

(f) Application Security. Each Licensee's cyber security program shall, at minimum, include written procedures, guidelines, and standards reasonably designed to ensure the security of all applications utilized by the Licensee. All such procedures, guidelines, and standards shall be reviewed, assessed, and updated by the Licensee's CISO at least annually.

(g) Personnel and Intelligence. Each Licensee shall:

(1) employ cyber security personnel adequate to manage the Licensee's cyber security risks and to perform the core cyber security functions specified in Paragraph 200.16(a)(1)-(5);

(2) provide and require cyber security personnel to attend regular cyber security update and training sessions; and

(3) require key cyber security personnel to take steps to stay abreast of changing cyber security threats and countermeasures.

Section 200.17 Business continuity and disaster recovery

(a) Each Licensee shall establish and maintain a written business continuity and disaster recovery ("BCDR") plan reasonably designed to ensure the availability and functionality of the Licensee's services in the event of an emergency or other disruption to the Licensee's normal business activities. The BCDR plan, at minimum, shall:

(1) identify documents, data, facilities, infrastructure, personnel, and competencies essential to the continued operations of the Licensee's business;

(2) identify the supervisory personnel responsible for implementing each aspect of the BCDR plan;

(3) include a plan to communicate with essential Persons in the event of an emergency or other disruption to the operations of the Licensee, including employees, counterparties, regulatory authorities, data and communication providers, disaster recovery specialists, and any other Persons essential to the recovery of documentation and data and the resumption of operations;

(4) include procedures for the maintenance of back-up facilities, systems, and infrastructure as well as alternative staffing and other resources to enable the timely recovery of data and documentation and to resume operations as soon as reasonably possible following a disruption to normal business activities;

(5) include procedures for the back-up or copying, with sufficient frequency, of documents and data essential to the operations of the Licensee and storing of the information off site; and

(6) identify third parties that are necessary to the continued operations of the Licensee's business.

(b) Each Licensee shall distribute a copy of the BCDR plan, and any revisions thereto, to all relevant employees and shall maintain copies of the BCDR plan at one or more accessible off-site locations.

(c) Each Licensee shall provide relevant training to all employees responsible for implementing the BCDR plan regarding their roles and responsibilities.

(d) Each Licensee shall promptly notify the superintendent of any emergency or other disruption to its operations that may affect its ability to fulfill regulatory obligations or that may have a significant adverse effect on the Licensee, its counterparties, or the market.

(e) The BCDR plan shall be tested at least annually by qualified, independent internal personnel or a qualified third party, and revised accordingly.

Section 200.18 Advertising and marketing

(a) Each Licensee engaged in Virtual Currency Business Activity shall not advertise its products, services, or activities in New York or to New York Residents without including the name of the Licensee and the legend that such Licensee is "Licensed to engage in Virtual Currency Business Activity by the New York State Department of Financial Services."

(b) Each Licensee shall maintain, for examination by the superintendent, all advertising and marketing materials for a period of at least seven years from the date of their creation, including but not limited to print media, internet media (including websites), radio and television advertising, road show materials, presentations, and brochures. Each Licensee shall maintain hard copy, website captures of material changes to internet advertising and marketing, and audio and video scripts of its advertising and marketing materials, as applicable.

(c) In all advertising and marketing materials, each Licensee shall comply with all disclosure requirements under federal and state laws, rules, and regulations.

(d) In all advertising and marketing materials, each Licensee and any person or entity acting on its behalf, shall not, directly or by implication, make any false, misleading, or deceptive representations or omissions.

Section 200.19 Consumer protection

(a) Disclosure of material risks. As part of establishing a relationship with a customer, and prior to entering into an initial transaction for, on behalf of, or with such customer, each Licensee shall disclose in clear, conspicuous, and legible writing in the English language and in any other predominant language spoken by the customers of the Licensee, all material risks associated with its products, services, and activities and Virtual Currency generally, including at a minimum, the following:

(1) Virtual Currency is not legal tender, is not backed by the government, and accounts and value balances are not subject to Federal Deposit Insurance Corporation or Securities Investor Protection Corporation protections;

(2) legislative and regulatory changes or actions at the state, federal, or international level may adversely affect the use, transfer, exchange, and value of Virtual Currency;

(3) transactions in Virtual Currency may be irreversible, and, accordingly, losses due to fraudulent or accidental transactions may not be recoverable;

(4) some Virtual Currency transactions shall be deemed to be made when recorded on a public ledger, which is not necessarily the date or time that the customer initiates the transaction;

(5) the value of Virtual Currency may be derived from the continued willingness of market participants to exchange Fiat Currency for Virtual Currency, which may result in the potential for permanent and total loss of value of a particular Virtual Currency should the market for that Virtual Currency disappear;

(6) there is no assurance that a Person who accepts a Virtual Currency as payment today will continue to do so in the future;

(7) the volatility and unpredictability of the price of Virtual Currency relative to Fiat Currency may result in significant loss over a short period of time;

(8) the nature of Virtual Currency may lead to an increased risk of fraud or cyber attack;

(9) the nature of Virtual Currency means that any technological difficulties experienced by the Licensee may prevent the access or use of a customer's Virtual Currency; and

(10) any bond or trust account maintained by the Licensee for the benefit of its customers may not be sufficient to cover all losses incurred by customers.

(b) Disclosure of general terms and conditions. When opening an account for a new customer, and prior to entering into an initial transaction for, on behalf of, or with such customer, each Licensee shall disclose in clear, conspicuous, and legible writing in the English language and in any other predominant language spoken by the customers of the Licensee, all relevant terms and conditions associated with its products, services, and activities and Virtual Currency generally, including at a minimum, the following, as applicable:

(1) the customer's liability for unauthorized Virtual Currency transactions;

(2) the customer's right to stop payment of a preauthorized Virtual Currency transfer and the procedure to initiate such a stop-payment order;

(3) under what circumstances the Licensee will, absent a court or government order, disclose information concerning the customer's account to third parties;

(4) the customer's right to receive periodic account statements and valuations from the Licensee;

(5) the customer's right to receive a receipt, trade ticket, or other evidence of a transaction;

(6) the customer's right to prior notice of a change in the Licensee's rules or policies; and

(7) such other disclosures as are customarily given in connection with the opening of customer accounts.

(c) Disclosures of the terms of transactions. Prior to each transaction in Virtual Currency, for, on behalf of, or with a customer, each Licensee shall furnish to each such customer a written disclosure in clear, conspicuous, and legible writing in the English language and in any other predominant language spoken by the customers of the Licensee, containing the terms and conditions of the transaction, which shall include, at a minimum, to the extent applicable:

(1) the amount of the transaction;

(2) any fees, expenses, and charges borne by the customer, including applicable exchange rates;

(3) the type and nature of the Virtual Currency transaction;

(4) a warning that once executed the transaction may not be undone, if applicable; and

(5) such other disclosures as are customarily given in connection with a transaction of this nature.

(d) Acknowledgement of disclosures. Each Licensee shall ensure that all disclosures required in this Section are acknowledged as received by customers.

(e) Receipts. Upon completion of any transaction, each Licensee shall provide to a customer a receipt containing the following information:

(1) the name and contact information of the Licensee, including a telephone number established by the Licensee to answer questions and register complaints;

(2) the type, value, date, and precise time of the transaction;

(3) the fee charged;

(4) the exchange rate, if applicable;

(5) a statement of the liability of the Licensee for non-delivery or delayed delivery;

(6) a statement of the refund policy of the Licensee; and

(7) any additional information the superintendent may require.

(f) Each Licensee shall make available to the Department, upon request, the form of the receipts it is required to provide to customers in accordance with Subsection 200.19(e).

(g) Prevention of fraud. Licensees are prohibited from engaging in fraudulent activity. Additionally, each Licensee shall take reasonable steps to detect and prevent fraud, including by establishing and maintaining a written anti-fraud policy. The anti-fraud policy shall, at a minimum, include:

(1) the identification and assessment of fraud-related risk areas;

(2) procedures and controls to protect against identified risks;

(3) allocation of responsibility for monitoring risks; and

(4) procedures for the periodic evaluation and revision of the anti-fraud procedures, controls, and monitoring mechanisms.

Section 200.20 Complaints

(a) Each Licensee shall establish and maintain written policies and procedures to fairly and timely resolve complaints.

(b) Each Licensee must provide, in a clear and conspicuous manner, on its website or websites, in all physical locations, and in any other location as the superintendent may prescribe, the following disclosures:

(1) the Licensee's mailing address, email address, and telephone number for the receipt of complaints;

(2) a statement that the complainant may also bring his or her complaint to the attention of the Department;

(3) the Department's mailing address, website, and telephone number; and

(4) such other information as the superintendent may require.

(c) Each Licensee shall report to the superintendent any change in the Licensee's complaint policies or procedures within seven days.

Section 200.21 Transitional Period

A Person already engaged in Virtual Currency Business Activity must apply for a license in accordance with this Part within 45 days of the effective date of this regulation. In doing so, such applicant shall be deemed in compliance with the licensure requirements of this Part until it has been notified by the superintendent that its application has been denied, in which case it shall immediately cease operating in this state and doing business with New York State Residents. Any Person engaged in Virtual Currency Business Activity that fails to submit an application for a license within 45 days of the effective date of this regulation shall be deemed to be conducting unlicensed Virtual Currency Business Activity.

Section 200.22 Severability

If any provision of this Part or the application thereof to any Person or circumstance is adjudged invalid by a court of competent jurisdiction, such judgment shall not affect or impair the validity of the other provisions of this Part or the application thereof to other Persons or circumstances.

Exhibit Y

Comments to the New York State Department of Financial Services on

BitLicense

The Proposed Virtual Currency Regulatory Framework

on behalf of

Electronic Frontier Foundation
Internet Archive
reddit

by Marcia Hofmann, EFF Special Counsel and Attorney at Law

With assistance from:
Rainey Reitman, Joseph Bonneau, David Greene,
Jennifer Lynch, Parker Higgins and Cindy Cohn

October 21, 2014

October 21, 2014

VIA EMAIL—dana.syracuse@dfs.ny.gov

Benjamin M. Lawsky
Superintendent
Dana V. Syracuse
Office of General Counsel
New York Department of Financial Services
One State Street
New York, NY 10004

RE: Comment on DFS-29-14-00015-P: New York State Department of Financial Services BitLicense Proposal

Dear Superintendent Lawsky and General Counsel Syracuse:

The Electronic Frontier Foundation, Internet Archive, and reddit submit this comment in response to DFS-29-14-00015-P, the New York State Department of Financial Services inquiry and proposed regulation of virtual currency businesses.[1] We believe that, as currently drafted, the "BitLicense" regulatory framework raises profound civil liberties concerns and stifles innovation.

The proposal would infringe the privacy rights of casual users and digital currency innovators, as well as fundamentally burden freedom of speech and association.

The framework would also create expensive new obligations for businesses developing new products and services in the digital currency ecosystem, likely foreclosing many of them from doing business involving New York and its residents.

Commenters

The Electronic Frontier Foundation (EFF) is a non-profit civil liberties law and technology organization. Founded in 1990, EFF champions individual privacy, free expression and innovation. With over 20,000 members around the globe, EFF uses public education campaigns, impact litigation, open source technology projects, policy analysis, and grassroots activism to ensure that civil liberties are protected even as society's use of technology increases.

EFF has documented and criticized different forms of financial censorship for many years and has used its popular blog and mailing list to analyze the ramifications of

[1] 2014-29 N.Y. St. Reg. 14 (July 23, 2014) (to be codified at Part 200 to Title 23 NYCRR), http://docs.dos.ny.gov/info/register/2014/july23/pdf/rulemaking.pdf.

decreased financial privacy. EFF also allows supporters to make donations through Bitcoin.

The Internet Archive is a public non-profit organization that was founded in 1996 to build an "Internet library," with the purpose of offering permanent access for researchers, historians, scholars, artists, and the general public to collections in digital format. Collaborating with many libraries, state agencies, and other archives, the Archive collects and receives electronic and physical data and media, including texts, audio, videos/film, software, television news, and archived web pages. The Internet Archive provides free access to these resources via its websites, including archive.org and openlibrary.org.

The Archive helped set up and provides administrative support to Internet Archive Federal Credit Union, which has had to close accounts for individuals and business associated with Bitcoin due to regulatory pressure. The Internet Archive accepts donations almost daily via Bitcoin, has paid employees modest portions of their salaries in Bitcoin (on a voluntary basis), pays for some of its catered meals in Bitcoin, and has archived a great deal of Bitcoin-related media in the normal course of its archival activities. The Archive's employees also regularly pay for lunch with Bitcoin at a nearby restaurant.

reddit was founded by Steve Huffman and Alexis Ohanian in 2005, and is an online community where users submit, vote, and comment on content, stories, and discussions. The hottest stories as determined by the community through discussions and voting rise to the top of the site, while cooler stories sink. Anyone can create a community (called a "subreddit"); each subreddit is independent and moderated by a team of volunteers. reddit is open source, and community members are constantly tinkering and contributing features and translations back to the site. In September 2014, reddit received more than 6.175 billion page views and more than 174 million unique visitors. reddit also hosts the world's largest gift exchange as listed in the Guinness Book of World Records through redditgifts.com, and features video and original programming through reddit.tv.

reddit believes block chain technology has many potential applications that may improve the experience for its users. The BitLicense framework may limit reddit's ability to leverage this technology to enhance its community and impact the privacy of reddit's users.

Introduction: Digital Currencies and Bitcoin-like Protocols

There are more than 500 digital currencies currently in existence.[2] Most of them have an underlying global peer-to-peer architecture similar to Bitcoin, an Internet protocol that makes it possible for people to transact directly with each other

[2] See Crypto-Currency Market Capitalizations, http://coinmarketcap.com (last updated Oct. 21, 2014).

without an intermediary. Every transaction is verified and recorded in a public ledger known as a block chain.

Bitcoin was originally envisioned by the pseudonymous developer Satoshi Nakamoto as a decentralized electronic payment system that would operate independently of financial institutions.[3] This payment system continues to be Bitcoin's most widely known application, and when people hear "Bitcoin," they often think of the units of value exchanged through the protocol (also known as "bitcoins").

Many different kinds of transactions can be recorded in block chain-like public ledgers, though, which means there are potential uses of block chains that are separate and independent of money transfers.

Indeed, developers are finding ways to use block chain technology to record a wide range of transactions that rely on authentication and validation, such as keeping track of property ownership; buying and selling equity in digital media; sharing storage space or processing power; recording and transferring domain names; managing public records; and casting and verifying votes.[4]

While developers are building these new applications upon systems often associated with payments, they are not financial institutions and should not be treated that way for purposes of regulation.

Whether used to transfer currency or in a wholly different capacity, Bitcoin-like systems have great potential as a civil liberties-enhancing technology. One of the benefits of Bitcoin and similar currencies is that they offer the potential for pseudonymous transactions because the block chain does not directly link a transaction to the parties' names. Furthermore, the decentralized nature of the protocol makes it naturally resistant to censorship.

As a payment system, Bitcoin-like currencies share these attributes with cash. We should consider this a feature, not a bug; it is an innovative way to import some of the civil liberties protections we already enjoy offline into the digital world.

---

[3] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* (2008), https://bitcoin.org/bitcoin.pdf.

[4] *See, e.g.*, Olga Kharif, *Bitcoin 2.0 Shows Technology Evolving Beyond Use as Money*, Bloomberg (Mar. 27, 2014), http://www.bloomberg.com/news/2014-03-28/bitcoin-2-0-shows-technology-evolving-beyond-use-as-money; Ledra Capital, *Bitcoin Series 24: The Mega-Master Blockchain Master List*, http://ledracapital.com/blog/2014/3/11/bitcoin-series-24-the-mega-master-blockchain-list (last visited Oct. 20, 2014); Anil Dash, *A Bitcoin for Digital Art* (May 9, 2014), https://medium.com/message/a-bitcoin-for-digital-art-8c7db719e495; Ethereum, https://www.ethereum.org (last visited Oct. 21, 2014); Namecoin, http://namecoin.info (last visited Oct. 21, 2014).

NY DFS has proposed this regulatory framework "to protect consumers and root out illegal activity," which are important, laudable goals.[5] But as currently written, the BitLicense proposal would also undermine the unique civil liberties benefits digital currencies offer by design.

Argument

I. Key Definitions in the BitLicense Framework are Vague, Confusing, and Overly Broad, Which Makes the Scope of the Proposed Regulation Unclear.

The BitLicense proposal would require anyone who engages in any "Virtual Currency Business Activity" involving New York or a New York resident to first obtain a license from NY DFS.[6] Unfortunately, certain definitions leave a great deal of uncertainty about what would actually be subject to regulation.

A. "Virtual Currency"

The BitLicense framework uses the term "virtual currency" to describe the type of unit it aims to regulate.[7]

As an initial matter, we believe NY DFS's use of the word "virtual" may cause confusion. Some commentators use the term "virtual currency" to refer to a narrow subset of currencies associated with online games, while "digital currency" is used more broadly to refer to any currency that is electronically transferred and stored.[8] Because the BitLicense proposal would affect a far wider range of currencies than those associated with online games, we use the term "digital currency" throughout this comment, and encourage NY DFS to consider adopting this terminology for further proceedings.

Turning to the BitLicense framework, NY DFS has defined "Virtual Currency" as "any type of digital unit that is used as a medium of exchange *or* a form of digitally stored value *or* that is incorporated into payment system technology" (emphasis added).[9] The terms "digital unit," "medium of exchange," and "digitally stored value"

---

[5] Press Release, New York Department of Financial Services, NY DFS Releases Proposed BitLicense Regulatory Framework for Virtual Currency Firms (July 17, 2014), http://www.dfs.ny.gov/about/press2014/pr1407171.html (hereafter "NY DFS Press Release").

[6] Section 200.3(a).

[7] Section 200.2(m).

[8] *See, i.e.*, Andrew Wagner, *Digital vs. Virtual Currencies*, Bitcoin Magazine (Aug. 22, 2014), http://bitcoinmagazine.com/15862/digital-vs-virtual-currencies; Danny Bradbury, *Is Bitcoin a Digital Currency or a Virtual One?*, Coindesk (Mar. 19, 2014), http://www.coindesk.com/bitcoin-digital-currency-virtual-one. *See also* Bitcoin Foundation Comment on NYDFS "BitLicense" Proposal at 1-2 (Oct. 8, 2014), https://bitcoinfoundation.org/resources/bitcoin-foundation-comment-on-nydfs-bitlicense-proposal.

[9] Section 200.2(m).

are vague, and NY DFS presumably believes they describe digital units independent of any payment system—otherwise, it would be unnecessary to specifically incorporate them in "Virtual Currency."

As a result of this broad definition, the framework seems to extend not just to financial institutions or money transmission services, but also more broadly to applications of the block chain that use "digital units" as a "medium of exchange" or "a form of digitally stored value."

The definition currently includes specific carve-outs for certain "digital units" used solely within online gaming platforms and customer affinity or rewards programs. NY DFS should add another exception for non-financial uses of digital currency systems, such as self-executing contracts and tracking digital assets.

B. "Virtual Currency Business Activity"

The BitLicense proposal would require a license for any "Virtual Currency Business Activity" involving the State of New York or residents of New York.[10]

First, as a practical matter, this regulation will reach many businesses that have only a tenuous connection to the state. Digital currencies rely on global internet infrastructure, and so the vast majority of businesses in the digital currency ecosystem will be likely to engage in commerce involving New York or New York residents at some point in time. Even companies based wholly outside the United States will be responsible for complying with this regulation if they only conduct occasional business with New York residents.

Second, the basic definition of "Virtual Currency Business Activity" is extremely broad. This term includes:

- receiving Virtual Currency for transmission or transmitting the same;
- securing, storing, or maintaining custody or control of Virtual Currency on behalf of customers;
- buying and selling Virtual Currency as a customer business;
- performing retail conversion services, including the conversion or exchange of Fiat Currency or other value into Virtual Currency, the conversion or exchange of Virtual Currency into Fiat Currency or other value, or the conversion or exchange of one form of Virtual Currency into another form of Virtual Currency; or
- controlling, administering, or issuing a Virtual Currency.[11]

---

[10] Section 200.2(n).

[11] Section 200.2(n)(1)-(5).

This definition would certainly cover any business that hosts digital currency wallets, operates an exchange, or provides digital currency storage. It would also include people inventing new types of digital currency—even currencies not intended for use as financial instruments, given the breadth of the "Virtual Currency" definition.

Unfortunately, it is not clear what the outer limits of "Virtual Currency Business Activity" are.

For example, the definition covers anyone who "controls," "administers," or "issues" a currency. This might be read to include operators of peer-to-peer nodes, who play a key role in keeping digital currency systems up and running, and so might be considered to "administer" those currencies.

The definition could also include software developers who create programs enabling people to store and transact with digital currencies, such as makers of wallets that bitcoin holders use to keep the currency on their computers or smartphones. Because these developers create programs to "secur[e], stor[e], or maintain[] custody or control of Virtual Currency on behalf of customers," as well as to help "administer" currency, they might also fall under this regulation.

The BitLicense proposal could also cover digital currency miners, since their computing efforts are the source of digital currency. Miners could easily be said to "control[], administer[], or issu[e] a Virtual Currency." According to NY DFS's public statements, the agency does not intend to sweep up miners in this regulation[12]—and yet there is no explicit exception for miners in the text of the proposal.

Even the Bitcoin Foundation and core members of the Bitcoin development team might be subject to this regulation, since they play a fundamental role in the growth of Bitcoin and determining the rules around it. Their activities might be considered "controlling" and "administering" the currency.

C. "Transmission"

The framework's definition of "transmission" makes the picture even murkier. "Virtual Currency Business Activity" specifically includes "receiving Virtual Currency for transmission or transmitting the same." The term "transmission" is defined as "the transfer, by or through a third party, of Virtual Currency from one Person to another Person, *including the transfer from the account or storage repository of one Person to the account or storage repository of another Person*" (emphasis added).[13]

---

[12] NY DFS Press Release; Nermin Hajdarbegovic, *Lawsky: Bitcoin Developers and Miners Exempt From BitLicense*, CoinDesk (Oct. 15, 2014), http://www.coindesk.com/lawsky-bitcoin-developers-miners-exempt-bitlicense.

[13] Section 200.2(l).

At first blush, NY DFS appears to intend to limit "transmission" to third-party intermediaries that conduct financial transactions between people. But then the definition goes on to explicitly include peer-to-peer transactions involving the accounts or storage repositories of the parties. It is unclear whether an individual would need a license under this proposal to merely operate a peer-to-peer node in a digital currency system, or to send digital currency directly from a wallet on her phone to another person.

We were heartened to see Superintendent Lawsky recently explain in public remarks that the BitLicense proposal is meant to cover "financial intermediaries," not people developing software or platforms.[14] He said:

> To clarify, we do not intend to regulate software or software development. For example, a software developer who creates and provides wallet software to customers for their own use will not need a license. Those who are innovating and developing the latest platforms for digital currencies will not need a license.

Unfortunately, this is not what the text of the BitLicense framework actually says. NY DFS must hone the definitions discussed above to clarify the scope of the regulation.

II. The BitLicense Proposal Intrudes Upon the Personal Privacy of Consumers Who Transact With Digital Currencies and Business People Innovating in the Digital Currency Ecosystem.

One of the most promising features of digital currency is its potential as a privacy-enhancing technology, since all transactions are linked to pseudonymous public keys rather than real-world identities. Unfortunately, the BitLicense framework would eviscerate this feature by compromising the privacy of average consumers, developers, and entrepreneurs.

First, the proposal provides that "No Licensee shall engage in, facilitate, or knowingly allow the transfer or transmission of Virtual Currency when such action will obfuscate the identity of an individual customer or counterparty."[15] This requirement has profound implications for Bitcoin-like systems that have pseudonymity built into them by design. NY DFS is effectively proposing to nullify this hallmark of digital currency protocols, along with the privacy protection it provides, by forbidding licensees to allow any non-personally identifiable transactions.

Second, the BitLicense framework would require licensees to keep detailed records of all transactions they perform for 10 years "in a condition that will allow [NY DFS]

---

[14] Hajdarbegovic, *Lawsky: Bitcoin Developers and Miners Exempt From BitLicense.*

[15] Section 200.15(f).

to determine whether the Licensee is complying with all laws and regulations," including:

- the amount, date, and precise time of the transaction, and any payment instructions;
- the total amount of fees and charges received and paid to, by, or on behalf of the licensee;
- names of the parties to the transaction;
- account numbers of the parties to the transaction; and
- physical addresses of the parties to the transaction.[16]

While the framework purports to exempt "merchants or consumers that utilize Virtual Currency solely for the purchase or sale of goods or services,"[17] the proposal *would* require licensees to maintain specific details about transactions—including information about merchants who accept digital currencies and their customers.[18]

This represents an enormous expansion of the recordkeeping requirements even for financial services covered by state and federal anti-money laundering regulations[19]—although, as explained above, the wording of the current proposal appears to extend to many businesses and individuals who are not required to comply with those rules.

Forcing companies to maintain detailed records about every transaction, no matter how mundane or insignificant, is burdensome and unnecessary. But we are even more concerned that every transaction would have to be linked to the names and physical addresses of all parties, and then kept for 10 years in case NY DFS should wish to inspect that information.

This is particularly invasive for individuals who may wish to make digital currency payments for sensitive purposes. The Electronic Frontier Foundation and Internet Archive are concerned about this possibility because they are non-profit organizations that accept Bitcoin donations, and they believe there are many

---

[16] Section 200.12(a)(1).

[17] Section 200.3(c)(2).

[18] Section 200.12.

[19] According to FinCEN's regulations implementing the Bank Secrecy Act, "All records that are required to be retained by this chapter shall be retained for a period of five years." 31 C.F.R. § 1010.430(d) (formerly at 31 C.F.R. § 103.38(d)). New York anti-money laundering regulations require licensees to comply with federal requirements. NY DFS Superintendent's Regulation 416.1(b)(2)(i); *see also* NY DFS General Regulations of the Banking Board § 116.2.

legitimate reasons why someone would prefer privacy in her financial transactions.[20]

Consider a Federal Bureau of Investigation or National Security Agency employee who would like to donate money to support EFF, which is in ongoing litigation against the government over warrantless surveillance activities. Or consider a teenager who wants to buy contraceptives without anyone knowing, or a grassroots political organization raising money for the legal defense of a political prisoner.

In each case, there are reasons why a person may want to spend money without having that fact linked to his or her identity for a decade.[21] This is possible with cash transactions. Given the privacy-protective nature of digital currency protocols, it should be possible for digital currency transactions, too.

Furthermore, requiring companies to maintain these records creates a massive consumer privacy risk if those records should ever be stolen by malicious actors.

The public nature of the block chain makes the privacy risk of long-term record storage far greater for digital currency-related businesses than keeping equivalent records would be for more traditional businesses. If a retail company such as Target, for example, maintains a consumer database linking individual consumers to their credit card numbers, a hacker who compromises that database cannot recreate a wide-scale financial history for each consumer unless the hacker is able to match that data with purchase records from elsewhere.

But if a business maintains a database linking pseudonymous Bitcoin public keys with personally identifying information about consumers (as would be required under the proposed regulation), a hacker who compromises the database could identify a broad swath of consumer financial transactions by cross-referencing the stolen information with the block chain. This comparison could personally identify and publicly expose an extensive amount of information about consumers' financial activities over time—not just with the hacked business, but with other parties, too.

It is also worth noting that if a business maintained customer purchase records limited to transactional information and pseudonymous Bitcoin addresses, the privacy risk to consumers would be very low, since a malicious attacker could learn nothing more than what is already publicly recorded in the block chain.

We believe it is important to allow the privacy-enhancing design of digital currency to work in favor of consumers, not against them. We encourage NY DFS not to

---

[20] For a longer list of non-profit, political, activist, cultural, and other organizations that accept Bitcoin, see https://en.bitcoin.it/wiki/Donation-accepting_organizations_and_projects (last visited Oct. 21, 2014).

[21] For more observations on the privacy implications of the BitLicense proposal, see Harley Geiger, *NY's Proposed BitRegs a Threat to Privacy and Innovation*, Center for Democracy and Technology (Sept. 5, 2014), https://cdt.org/blog/nys-bitregs-a-threat-to-privacy-and-innovation.

impose record-keeping requirements beyond those already established by state and federal anti-money laundering regulations.

Finally, the BitLicense proposal would compromise the privacy of individuals who want to work in the digital currency space. The framework would require BitLicense applicants to submit an extensive amount of personal information about key officers, directors, stockholders, and beneficiaries to NY DFS, including:

- information about their personal history, experience, and qualifications;
- a background report from an independent investigative agency;
- fingerprints for submission to state and federal law enforcement;
- portrait-style photos;
- financial statements;
- "details of all banking arrangements"; and
- an affidavit detailing all actual or potential legal proceedings (apparently even those that are unrelated to business activities, such as divorce actions).[22]

The proposed regulations also provide that NY DFS will affirmatively investigate the "financial condition and responsibility, financial and business experience, and character and general fitness" of any applicant who applies for a license.[23]

The framework would force individuals building digital currency businesses to forfeit their personal privacy more than what makes sense or is necessary. As a result, people who care about their privacy might avoid working in the digital currency space altogether.

III. The BitLicense Proposal Licenses Speech, and Must Respect the Well Established Legal Limitations on Prior Restraints

Bitcoin is not just a unit of value or a way to transact payments; the protocol is a platform for other uses with expressive and associational value. The protocol can also be used to organize and express views as a group, and people already use Bitcoin to publish political commentary, make religious statements, and create art. The BitLicense proposal could chill these expressive activities because it would require prior approval from NY DFS before people can engage in a wide variety of activities using digital currency protocols—including activities that have nothing to do with payments. As drafted, the BitLicense proposal appears to impose a prior

[22] Section 200.4(a)(3)-(5), (7), (9), (11).

[23] Section 200.6(a).

restraint on protected expression without adequate procedural safeguards, which makes it vulnerable to legal attack.

A. Digital Currency Protocols Implicate First Amendment Interests

1. Digital Currency Protocols are Code, Which is Speech For Purposes of the First Amendment

While digital currencies are most commonly thought of as means of payment, at their very essence, digital currency protocols are code. And as courts have long recognized, code is speech protected by the First Amendment. *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 445-46 (2d Cir. 2001); *Junger v. Daley*, 209 F.3d 481, 485 (6th Cir. 2000); *see also Bernstein v. Dep't of Justice*, 176 F.3d 1132, 1140-41 (9th Cir. 1999), *reh'g granted, opinion withdrawn*, 192 F.3d 1308 (9th Cir. 1999); *Karn v. Dep't of State*, 925 F. Supp. 1, 9-10 (D.D.C. 1996) (assuming, without deciding, that source code with English comments interspersed throughout is "speech").

The Second Circuit in *Corley* explained why this is so:

> Instructions such as computer code, which are intended to be executable by a computer, will often convey information capable of comprehension and assessment by a human being. A programmer reading a program learns information about instructing a computer, and might use this information to improve personal programming skills and perhaps the craft of programming. Moreover, programmers communicating ideas to one another almost inevitably communicate in code, much as musicians use notes. Limiting First Amendment protection of programmers to descriptions of computer code (but not the code itself) would impede discourse among computer scholars, just as limiting protection for musicians to descriptions of musical scores (but not sequences of notes) would impede their exchange of ideas and expression. Instructions that communicate information comprehensible to a human qualify as speech whether the instructions are designed for execution by a computer or a human (or both).

The Bitcoin software is fully open source, which means anyone can read it, understand how it works, and suggest contributions to the code.[24] Further, the protocol and its functionality is the topic of a great deal of academic research.[25]

Thus, government action triggers First Amendment protections when it regulates computer programs such as digital currency protocols—a fact that is especially true

---

[24] *See, i.e.*, Bitcoin Core, https://github.com/bitcoin/bitcoin/ (last visited Oct. 21, 2014).

[25] For a list of academic research on Bitcoin, see Bitcoin Wiki, Ressearch, https://en.bitcoin.it/wiki/Research (last visited Oct. 21, 2014).

given the open source nature of these programs, which allows users to view, share, and develop ideas based upon the code itself.[26]

2. Digital Currency Systems Foster Freedom of Association

Digital currency protocols aren't just themselves speech. They also raise constitutional concerns about freedom of association, which is important because the First Amendment protects the freedom to organize and express political views as a group. *NAACP v. State of Alabama ex rel. Patterson*, 357 U.S. 449, 460-62 (1958).

Bitcoin-like systems are used for organizing and engaging with groups or communities. Both EFF and the Internet Archive accept Bitcoin donations to support their work, and appreciate the privacy-enhancing features of the system.

Others are using digital currency systems to organize in creative ways. For example:

- MyPowers is a crowdfunding service that makes it possible to create digital coins associated with a certain person, organization, or event. People can buy these custom coins to join a movement of like-minded people and support issues or individuals they care about, using the coins as keys to access goods or services provided by the coin's creator.[27]

- SolarCoin is a digital currency that aims to incentivize the production of solar energy by providing monetary rewards to solar energy generators over time.[28] An environmentally minded community of volunteers and supporters continues to grow around the project.[29]

- The online community reddit recently announced that it is exploring the possibility of issuing a digital asset backed by shares to community members using a block chain.[30] This would make it possible for reddit members to have an ownership interest in their community.

---

[26] This difference is how the Second Circuit distinguished the code in *Corley* from that in *Vartuli*, where the Commodities Future Trading Commission was allowed to regulate code that was marketed as an automatically functioning trading system and was not used as a vehicle for expressive communication. *CFTC v. Vartuli*, 228 F.3d 94, 110-11 (2d Cir. 2000).

[27] MyPowers, http://mypowers.com (last visited Oct. 21, 2014).

[28] SolarCoin, http://solarcoin.org (last visited Oct. 21, 2014).

[29] SolarCoin Forum, http://solarcoin.org/forum/index.php?sid=24b41c3381c996592815948afddcfe53 (last visited Oct. 21, 2014).

[30] Liz Gaines, *Reddit Raises $50 Million, Plans to Share Stock With Community Members*, Re/code (Sept. 30, 2014), http://recode.net/2014/09/30/reddit-raises-50m-plans-to-share-stock-with-community-members.

Among other things, this technology could enable members of reddit to vote on community issues in proportion to their ownership of the digital asset in a decentralized, cryptographically auditable way. This would be an exciting development for the community. However, if reddit were required to collect members' personal information in order for them to hold and transfer this asset, it would destroy the pseudonymous nature of the reddit community. And particularly due to the expense of complying with the BitLicense proposal, reddit's best option may be to exclude citizens of New York from participating in the digital asset project.

These alternative uses of digital currency protocols have great potential to harness support for social and political causes in new, innovative ways. However, these efforts would be directly subject to BitLicensing because they involve "creating" "Virtual Currencies" as defined by the framework.

3. Block Chains Are Publishing Platforms for Protected Expression

While the Bitcoin block chain is most closely associated with publication of financial transactions, it can be used to publish other material, as well. As a publishing platform, a block chain is inherently resistant to censorship: once information is published there, it is nearly impossible to remove. Some Bitcoin users have taken advantage of this feature by encoding data into Bitcoin transactions, which are then permanently added to the block chain.

Since its very inception, the Bitcoin block chain has had a tradition of political, artistic, and even religious expression, all of which are speech protected by the First Amendment.[31] A few examples:

- *Political speech.* The very first block of data in the Bitcoin block chain contains a timestamp and message: "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks." This statement, presumably from Satoshi Nakamoto, refers to a newspaper article published in the British newspaper *The Times* with the headline "Chancellor Alistair Darling on Brink of Second Bailout for Banks." The statement is political, as Bitcoin was conceived as a response to the weaknesses of centralized financial institutions.[32]

  The block chain also hosts this memorial tribute to Nelson Mandela, containing a photo and quotes from the activist and world leader. *(See next page.)*

---

[31] For a colorful, varied list of examples of expressive speech published in the public ledger, see Ken Shirriff, *Hidden Surprises in the Bitcoin Blockchain and How They Are Stored, Nelson Mandela, Wikileaks, Photos, and Python Software*, Ken Shirriff's Blog (Feb. 16, 2014), http://www.righto.com/2014/02/ascii-bernanke-wikileaks-photographs.html. The images in this comment come from Mr. Shirriff's post.

[32] Bitcoin Wiki, Genesis Block, https://en.bitcoin.it/wiki/Genesis_block (last visited Oct. 21, 2014).

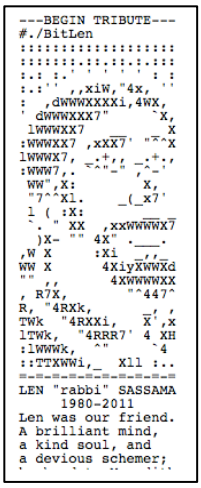
Nelson Mandela (1918-2013)
"I am fundamentally an optimist. Whether that comes from nature or nurture, I cannot say. Part of being optimistic is keeping one's head pointed toward the sun, one's feet moving forward. There were many dark moments when my faith in humanity was sorely tested, but I would not and could not give myself up to despair. That way lays defeat and death."
"I learned that courage was not the absence of fear, but the triumph over it. The brave man is not he who does not feel afraid, but he who conquers that fear."

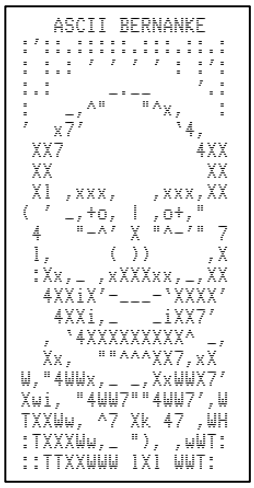
- *Religious expression.* The Bitcoin mining pool Eligius has published religious prayer in the block chain.

```
Benedictus Sanguis eius pretiosissimus.
Benedictus Iesus in sanctissimo altaris Sacramento.
Ave Maria, gratia plena, Dominus tecum. Benedicta tu in mulieribus, ...
...and life everlasting, through the merits of Jesus Christ, my Lord and Red
eemer.
O Heart of Jesus, burning with love for us, inflame our hearts with love for
 Thee.
Jesus, meek and humble of heart, make my heart like unto thine!
```

- *ASCII art.* Security researcher Dan Kaminsky added an ASCII (or plain text) memorial for cryptographer and privacy advocate Len Sassaman to the block chain after Sassaman's death.

  The block chain also contains an ASCII tribute with overtly political dimensions: a portrait of former Federal Reserve chairman Ben Bernanke. *(See next page.)*





- *Creative imagery*. The blockchain is also home to a number of logos, photographs, and other graphical works.

B. As Currently Written, the BitLicense Proposal Creates the Specter of an Unconstitutional System of Prior Restraints on Protected Speech

Because the BitLicense framework implicates expressive and associational interests, it must take into account well-established First Amendment limitations on licensing schemes and other restrictions on speech. It does not appear that NY DFS considered this issue while drafting the BitLicense framework. If implemented as currently written, the proposal would impose a system of prior restraints upon protected expression without providing adequate procedural safeguards, impermissibly undermining First Amendment values.

Any scheme that seeks to license speech raises the specter of a prior restraint. The BitLicense proposal is no different. The regulation has "a close enough nexus to expression, or to conduct commonly associated with expression, to pose a real and substantial threat of . . . censorship risks." *City of Lakewood v. Plain Dealer Pub. Co.*, 486 U.S. 750, 759 (1988).

As currently written, the proposal would forbid anyone from engaging in "Virtual Currency Business Activity" involving New York or New York residents without first obtaining a license from NY DFS.[33] The proposal explains that NY DFS will grant a license if it "belie[ves] that the applicant's business will be conducted honestly, fairly, equitably, carefully, and efficiently . . . and in a manner commanding the confidence and trust of the community[.]"[34]

The BitLicense proposal would operate as a content-based restriction: that is, the licensing requirement is squarely aimed at regulating digital currency protocols, which are themselves speech protected by the First Amendment.

NY DFS may take the position that the licensing requirement is a content-neutral restriction that could have the incidental effect of impinging on protected speech and association. If so, it is still a prior restraint: "even if the government may constitutionally impose content-neutral prohibitions on a particular manner of speech, it may not *condition* that speech on obtaining a license or permit from a government official in that official's boundless discretion." *Lakewood*, 486 U.S. at 764 (emphasis in original); *FW/PBS, Inc. v. Dallas*, 493 U.S. 215, 223 (1990) (plurality opinion).

And indeed, NY DFS's discretion is boundless under the regulation as currently written. The agency would have complete freedom to decide whether an applicant should be given a license to engage in Virtual Currency Business Activity. NY DFS can deny a license if it harbors any doubt or concern whatsoever about the applicant or its business—or constitutionally protected expression that NY DFS simply finds objectionable.

A system of prior restraints "bear[s] a heavy presumption against its constitutional validity." *Bantam Books, Inc. v. Sullivan*, 372 U.S. 58, 70 (1963). The Fourteenth Amendment requires that when a state adopts regulations for unprotected speech, it must include procedures to ensure that lawful, constitutionally protected speech is not curtailed, as well. *Id*., 372 U.S. at 66.

As the Supreme Court has explained, "[A] noncriminal process which requires the prior submission of [expression] to a censor avoids constitutional infirmity only if it takes place under procedural safeguards designed to obviate the dangers of a censorship system." *Freedman v. Maryland*, 380 U.S. 51, 58 (1965).

According to *Freedman,* the government must satisfy three requirements to ensure the validity of a licensing scheme that imposes a prior restraint on speech:

- any prior restraint of protected expression must be for a brief, specified period of time;

---

[33] Section 200.3(a).

[34] Section 200.6(a).

- there must be expeditious judicial review of the censor's decision; and
- the censor must bear the burden of going to court to suppress the speech in question, as well as bear the burden of proof.

380 U.S. 58-60.

The BitLicense proposal does not satisfy any of these standards.

The framework does not include provisions to ensure that any prior restraint of protected expression will be for a short, definite amount of time, and it does not require NY DFS to seek judicial review of its decision to deny a license, much less expeditious judicial review.[35] The proposal does not even set out a process for an applicant to appeal the denial of a license. Regardless, even if there were such a procedure, *Freedman* puts the burden on the censor to seek judicial review of its decision, not the applicant.

The proposal does say that NY DFS "*may, when deemed by the superintendent to be in the public interest*, seek a preliminary injunction to restrain a Licensee from continuing to perform acts that violate any provision of" the proposed regulation or other laws (emphasis added.)[36] But *Freedman* explicitly *requires* the State of New York to go to court if it seeks to suppress expressive activity, and to do so within a specified, brief period of time. The proposal lacks these safeguards.

NY DFS should remedy these defects. Otherwise, the BitLicense proposal may not pass muster under the First Amendment.

IV. The BitLicense Proposal Includes Overly Burdensome Financial Recordkeeping, Compliance, and Reporting Requirements That Will Stifle Innovation in the Digital Currency Space.

Finally, the BitLicense framework includes myriad financial, recordkeeping, compliance, and reporting requirements that will heavily discourage digital currency innovators from doing business that might be subject to these regulations.

Financial institutions and money transmitting services are already subject to a complex system of state and federal regulation, including extensive anti-money laundering laws, regulations, and orders. Companies transmitting digital currencies as intermediaries must already comply with these rules, just as anyone else would.

But NY DFS's proposal would impose additional technology-specific demands that would make it nearly impossible for entrepreneurs and developers to be part of the digital currency ecosystem until they are established and have adequate resources to comply with New York's demands. Many will simply avoid doing business in New

[35] Section 200.6(d).

[36] Section 200.6.

York or with New York's residents because complying with the state's regulations will be such a daunting endeavor.

A few examples:

- *Financial obligations*. Each licensee must "maintain at all times such capital as the superintendent determines is sufficient to ensure the financial integrity of the Licensee and its ongoing operations." This financial obligation may keep underfunded startups from entering the digital currency market. The proposal also imposes serious restrictions on investments, which must be denominated in U.S. dollars, regardless of where in the world the licensee is based.[37]

  Furthermore, the proposal requires each licensee to maintain a bond or trust account deemed acceptable by NY DFS.[38] It is unclear how much money a licensee will have to keep in the account to satisfy NY DFS's expectations, but again, this cost may be prohibitive for small businesses.

- *Permissions for business activities.* Every licensee must get NY DFS's written permission before offering any new product, service, or activity, or making a change to any existing product service, or activity involving New York or New York residents.[39] The proposal also requires a licensee to get NY DFS's express approval before undergoing any sort of business restructuring.[40] Thus, it appears licensees will have to get New York's permission before changing any aspect of their business activities, whether those changes involve Virtual Currency Business Activity or not.

- *Recordkeeping requirements.* The proposal imposes extensive recordkeeping requirements for 10 years.[41] Licensees also have to maintain copies of "all advertising and marketing materials, including, but not limited to print media, internet media (including websites), radio and television advertising, road show materials, presentations, and brochures."[42] This requirement does not appear to be limited to advertising involving Virtual Currency Business Activity.

- *Submission to examinations.* Licensees must submit to extensive examinations of their own or their affiliates' "books, records, accounts, documents, and other information" "whenever" NY DFS deems it "necessary

---

[37] Section 200.8.

[38] Section 200.9.

[39] Section 200.10.

[40] Section 200.11.

[41] Section 200.12.

[42] Section 200.18.

or advisable." They must also allow NY DFS to inspect their facilities.[43] These are new and demanding requirements for any business not already covered by existing anti-money laundering regulations.

- *Reporting requirements.* Licensees have to send NY DFS extensive financial statements every quarter.[44] In addition, they have to submit audited annual financial statements, along with supporting documentation and assessments. Again, these demands are onerous for businesses that are not already required to comply with existing anti-money laundering programs.

- *Extensive security, business continuity, and disaster recovery mandates.* The proposal would impose a variety of security, business continuity, and disaster recovery requirements.[45] These are important objectives, but the mandates are exhaustively specific, going so far as to demand that licensees keep all their hardware "in locked cages."[46] These exacting requirements contribute to the burdensome nature of these regulations.

  We believe security of financial systems is a crucial issue, but it is unclear why digital currency businesses should be held to different standards than more traditional financial institutions. If it has not done so already, we encourage NY DFS to consider soliciting input from the information security community about how financial intermediaries can best secure their systems and data, whether they transmit digital currencies or not.

- *Heightened anti-money laundering regulations*. The framework would impose an anti-money laundering program on licensees that is more formidable than the existing requirements under state and federal law.[47] There is no reason why digital currency businesses should be treated differently than other financial businesses on a technology-specific basis. The BitLicense proposal should impose no greater burden than state or federal anti-money laundering laws regulating traditional financial institutions.

- *Disclosures*. Digital currency businesses must make heavily detailed disclosures to consumers about "[a]ll material risks associated with [the company's] products, services and activities and Virtual Currency generally"—regardless of whether the transaction with the consumer

---

[43] Sections 200.12 & 200.13.

[44] Sections 200.14, 200.15, 200.16.

[45] Sections 200.16 and 200.17.

[46] Section 200.16(e)(2)(iii).

[47] Section 200.15. For a detailed comparison of NY DFS's proposed anti-money laundering program for digital currency businesses and anti-money laundering requirements under current state and federal law, see John Bliss, Strevus Comment on theBitLicense Proposal (Sept. 16, 2014), http://www.strevus.com/blognews/strevus-comment-ny-bitlicense-proposal.

actually involves digital currency.[48] No comparable disclosures are required when businesses transmit any other form of payment, including cash or credit. And if these disclosures are in the form of detailed fine-print, they risk suffering the same fate as end-user license agreements and website terms of service: nobody will read them. NY DFS should consider how to ensure any required disclosures are accessible, comprehensive, and most informative to consumers.

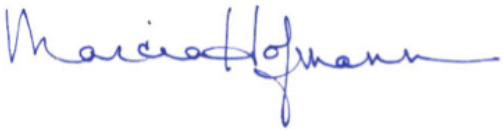
Finally, anyone engaged in Virtual Currency Business Activity would need to apply for a license within 45 days of when the regulation goes into effect.[49] Given the proposal's exhaustive requirements, very few companies will be in a position to actually comply with these regulations in such a short amount of time.

The BitLicense proposal would have the unintended consequence of pushing innovators out of the New York market. NY DFS should consider how to make these regulations less byzantine, and also less targeted at a single technology.

Conclusion

Companies and their users should be encouraged to adopt and build upon new technologies—not penalized with a crushing regulatory burden. We encourage NY DFS to go back to the drawing board and consider this proposal again in light of the impact it would have on privacy, free expression, and innovation.

Sincerely,



Marcia Hofmann
Law Office of Marcia Hofmann
25 Taylor Street
San Francisco, CA 94102
(415) 830-6664
marcia@marciahofmann.com

On behalf of the Electronic Frontier Foundation, Internet Archive, and reddit

[48] Section 200.19.

[49] Section 200.21.

Exhibit Z

ELECTRONIC FRONTIER FOUNDATION
Protecting Rights and Promoting Freedom on the Electronic Frontier

March 27, 2015

VIA EMAIL—VCRegComments@dfs.ny.gov
dana.syracuse@dfs.ny.gov

Benjamin M. Lawsky
Superintendent
Dana Syracuse
Office of the General Counsel
New York State Department of Financial Services
One State St.
New York, NY 10004

RE: Comments of the Electronic Frontier Foundation to the New York State Department of Financial Services on the Revised BitLicense Regulatory Framework

Dear Superintendent Lawsky and General Counsel Syracuse:

The Electronic Frontier Foundation ("EFF") submits these comments in response to the New York State Department of Financial Services' ("NYDFS") revised BitLicense regulatory framework, DFS-29-14-00015-RP,[1] as a supplement to the comments submitted by EFF pursuant to the initial BitLicense proposal.[2]

As a preliminary matter, implementing digital currency regulations now will only serve to stifle innovation. Digital currency is an industry in its infancy. And although NYDFS's goals in proposing a regulatory framework for digital currencies—protecting consumers and rooting out illegal activity—are laudable, it is simply too soon to begin regulating virtual currencies. We do not know, as a practical matter, what the use of virtual currencies will look like ten years from now. We therefore do not know what regulation is actually needed—and what regulation will be effective—to achieve NYDFS's stated goals. We also do not know what other services unique to virtual currencies might arise, such as free and independent third-party guarantors for contracts or deals, and whether such services will as a practical matter have the resources to meet the proposed recordkeeping obligations. Because of the concern over stifling innovation, any regulations adopted now should include a mandate that any recordkeeping burdens and restrictions imposed be reconsidered every two years to assess whether they can be cut back.

---

[1] 2015-08 N.Y. St. Reg. 17 (Feb. 25, 2015), http://www.dfs.ny.gov/legal/regulations/revised_vc_regulation.pdf.

[2] *See* Comments of Electronic Frontier Foundation, Internet Archive, and reddit to the New York State Department of Financial Services on BitLicense: The Proposed Virtual Currency Regulatory Framework (Oct. 21, 2014) https://www.eff.org/files/2014/10/21/bitlicense-comments-eff-ia-reddit-hofmann-cover.pdf.

815 Eddy Street • San Francisco, CA 94109 USA
voice +1 415 436 9333 fax +1 415 436 9993 web www.eff.org email information@eff.org

We do, however, recognize and applaud NYDFS's efforts to improve the original BitLicense proposal. Most significantly, through explicitly providing that "[t]he development and dissemination of software in and of itself does not constitute Virtual Currency Business," NYDFS has taken a great step toward ensuring that its BitLicense regulations will not stifle innovation in the digital currency space.

But NYDFS must make additional changes to the revised regulatory framework to more fully protect privacy, free expression, and innovation, and to ensure that the proposed regulations do not undermine the unique civil liberties benefits digital currencies can offer. Indeed, as we noted in our earlier comments, one of the most promising features of digital currency is its potential as a privacy-enhancing technology, since all transactions are linked to pseudonymous public keys rather than real-world identities. The revised BitLicense proposal—like the initial proposal—would eviscerate this feature by compromising the privacy of average consumers as well as small business owners and entrepreneurs.

(1) The revised BitLicense proposal's recordkeeping requirements are unduly burdensome and create a massive consumer privacy risk.

The revised BitLicense proposal would require licensees to keep detailed records of all transactions they perform for seven years "in a condition that will allow [NYDPS] to determine whether the Licensee is complying with all applicable laws, rules and regulations."[3] The proposal mandates that such records include, for each transaction: (a) the amount, date, and precise time of the transaction, and any payment instructions; (b) the total amount of fees and charges received and paid to, by, or on behalf of the Licensee; and (c) the names, account numbers, and physical addresses of (i) the party or parties to the transaction that are customers or accountholders of the Licensee, and (ii) to the extent practicable, any other parties to the transaction.[4]

While we appreciate NYDFS's attempt to decrease the burden imposed by its initial regulations through requiring that licensees maintain records on counterparties only "to the extent practicable," the revised BitLicense proposal would still dramatically expand the recordkeeping requirements of state and federal anti-money laundering regulations, such as FinCEN (which, for example, requires collection of data regarding counterparties only if the data is received during the course of the transaction). As we stated in our initial comments, forcing companies to maintain detailed records about every transaction, no matter how mundane or insignificant, is burdensome and unnecessary and will stifle innovation. Furthermore, the phrase "to the extent practicable" is vague—leaving licensees unsure of the efforts they must undertake to collect data about counterparties.

Of even more concern are the privacy issues raised by requiring that every transaction be linked to names and physical addresses of the parties (and then maintained for seven years). Not

---

[3] Section 200.12(a).

[4] Section 200.12(a)(1).

only does this undermine pseudonymity, but it also creates a massive consumer privacy risk should malicious actors ever get access to those records. The public nature of the blockchain makes the privacy risk of long-term record storage far greater for digital currency-related businesses than equivalent recordkeeping for more traditional businesses.

EFF believes it is important that NYDFS ensure that the privacy-enhancing potential of digital currency works in favor of consumers—not against them. We recommend that NYDFS impose recordkeeping requirements no greater than those already imposed by state and federal anti-money laundering regulations.

(2) The revised BitLicense proposal's ban on identity obfuscation threatens user privacy.

The revised BitLicense proposal—like the initial proposal—provides that "No Licensee shall engage in, facilitate, or knowingly allow the transfer or transmission of Virtual Currency when such action will obfuscate or conceal the identity of an individual customer or counterparty."[5] This ban on identity obfuscation has profound implications for Bitcoin-like systems that have pseudonymity built into them by design. As mentioned, one of the benefits of Bitcoin and similar currencies is that they offer the potential for pseudonymous transactions because the blockchain does not directly link a transaction to the parties' name. But the revised regulations would nullify this hallmark of digital currency protocols—along with the privacy protection pseudonymity provides—by forbidding licensees to allow any non-personally identifiable transactions. Indeed, although the BitLicense proposal states that "[n]othing in this Section . . . shall be construed to require a Licensee to make available to the general public the fact or nature of the movement of Virtual Currency by individual customers or counterparties,"[6] this is not enough to ensure privacy of transaction details. Because transactions on the blockchain are transparent by nature—and because there are various techniques to link personal identities to Bitcoin pseudonyms—users of digital currency may choose to use identity obfuscation to safeguard the privacy of their online transactions. Any regulations the NYDFS adopts should give users breathing room to take extra steps to protect the privacy of their transaction details, not take it away.

Furthermore, identity obfuscation is not clearly defined. Many commonplace Bitcoin practices, such as generating new change addresses with every transaction, could be interpreted as identity obfuscation. A ban on obfuscation generally is thus not only unwarranted, but it will also cause great confusion and uncertainty.

EFF recommends that NYDFS remove the ban on identify obfuscation and thereby allow users to keep personal and sensitive transaction details private.

---

[5] Section 200.15(g).

[6] *Id.*

(3) NYDFS is moving far too quickly to enact a BitLicense proposal.

Lastly, NYDFS is moving far too quickly to enact a BitLicense proposal. NYDFS provided for a mere 30-day period for public comment on its revised BitLicense regulatory framework, as compared to the 90-day period provided on the initial proposal.[7] This is simply not enough time for the public to comment on the unprecedented issue of digital currency regulation. To ensure that any regulatory framework is adopted with prudence, rather than haste, NYDFS must slowdown its process and allow more time for public comment on its revised BitLicense proposal—either by extending the deadline for public comment or by providing for a second public comment period on the revised BitLicense proposal.

Sincerely,

Rainey Reitman
Director of Activism
Electronic Frontier Foundation

Jamie Williams
Frank Stanton Legal Fellow
Electronic Frontier Foundation

[7] *See* Announcement of Revised BitLicense Regulatory Framework, http://www.dfs.ny.gov/legal/regulations/rev_bitlicense_reg_framework.htm.

Exhibit AA

California LEGISLATIVE INFORMATION

AB-129 Lawful money. (2013-2014)

Bill Analysis
06/19/14- Assembly Floor Analysis
06/06/14- Senate Floor Analyses
06/02/14- Senate Banking And Financial Institutions
01/28/14- Assembly Floor Analysis
01/17/14- Assembly Banking And Finance

Assembly Bill No. 129

CHAPTER 74

An act to repeal Section 107 of the Corporations Code, relating to business associations.

[Approved by Governor June 28, 2014. Filed with Secretary of State June 28, 2014.]

LEGISLATIVE COUNSEL'S DIGEST

AB 129, Dickinson. Lawful money.

Existing law prohibits a corporation, flexible purpose corporation, association, or individual from issuing or putting in circulation, as money, anything but the lawful money of the United States.

This bill would repeal that provision.

The people of the State of California do enact as follows:

SECTION 1. Section 107 of the Corporations Code is repealed.

O

Date of Hearing: January 21, 2014

ASSEMBLY COMMITTEE ON BANKING AND FINANCE
Roger Dickinson, Chair
AB 129 (Dickinson) – As Amended: January 7, 2014

SUBJECT: Lawful money: Alternative currency.

SUMMARY: Specifies that current law which bans the issuance or circulation of anything but lawful money of the United States does not prohibit the issuance and use of alternative currency.

EXISTING STATE LAW provides under Corporations Code section 107 that no corporation, flexible purpose corporation, association, or individual shall not issue or put in circulation, as money, anything but the lawful money of the United States.

EXISTING FEDERAL LAW provides that manufacturing counterfeit United States currency or altering genuine currency to increase its value is a violation of Title 18, Section 471 of the United States Code (U.S.C.) and is punishable by a fine of up to $5,000, or 15 years imprisonment, or both.

Possession of counterfeit United States obligations with fraudulent intent is a violation of Title 18, Section 472 of the U.S.C. and is punishable by a fine of up to $15,000, or 15 years imprisonment, or both.

Anyone who manufactures a counterfeit U.S. coin in any denomination above five cents is subject to the same penalties as all other counterfeiters. Anyone who alters a genuine coin to increase its numismatic value is in violation of Title 18, Section 331 of the U.S.C., which is punishable by a fine of up to $2,000, or imprisonment for up to 5 years, or both.

Forging, altering, or trafficking United States Government checks, bonds, or other obligations is a violation of Title 18, Section 510 of the U.S.C. and is punishable by a fine of up to $10,000, or ten years imprisonment, or both.

Printed reproductions, including photographs of paper currency, checks, bonds, postage stamps, revenue stamps, and securities of the United States and foreign governments (except under the conditions previously listed) are violations of Title 18, Section 474 of the U.S.C. Violations are punishable by fines of up to $5,000, or 15 years imprisonment, or both.

Section 31 U.S.C. 5103. Declares that United States coins and currency (including Federal Reserve Notes and circulating notes of Federal Reserve banks and national banks) are legal tender for all debts, public charges, taxes, and dues.

FISCAL EFFECT: None

COMMENTS:

This bill makes clarifying changes to current law to ensure that various forms of alternative currency such as digital currency, points, coupons, or other objects of monetary value do not violate the law when those methods are used for the purchase of goods and services or the transmission of payments. Modern methods of payment have expanded beyond the typical cash or credit card transactions.

Bitcoin, a digital currency (Also called cryptocurrency), has gained massive media attention recently as the number of businesses has expanded to accept Bitcoins for payment. Long before the introduction of digital currencies, various businesses have created points models that reward consumers with points for completion of various tasks such as spending a certain dollar amount, or even by purchasing points with dollars. These point systems effectively operate as currency allowing the consumers to buy a retail item or pay for some type of service. Many communities across the United States and in California have created "community currencies" that are created by members of a community in conjunction with merchants who agree to accept the alternative currency. These "community currencies" are created for a variety of reasons, some of which include encouraging consumers to shop at small businesses within the community or increasing neighborhood cohesiveness. "Community currency" has also become a form of political protest as some communities that use such currency do so in protest of US monetary policies, or large financial institutions. The following is a list of "community currencies" in California:

- Barter Bucks- Concord, California
- Bay Bucks San Francisco, California
- Berkeley Barter Network Berkeley, California
- Berkeley Bread Berkeley, California
- Central Pound Clovis, California
- Davis Dollars Davis, California
- Escondido Dollars Escondido, California
- Fairbuck Fairfax, California
- Humboldt Hours Eureka, California and Arcata, California
- Mendocino SEED Fort Bragg, California
- North Fork Shares North Fork, California
- San Luis Obispo Hours San Luis Obispo, California
- Sand Dollars Bolinas, California
- Santa Barbara Hours Santa Barbara, California
- Santa Monica Hours Santa Monica, California
- Sequoia Hours Garberville, California
- Sonoma County Community Cash Santa Rosa, California
- TradeMarket Nevada City, California
- Ukiah Hours Ukiah, California

The following is a list of the largest digital currencies (cryptocurrencies) that are in use:

- Bitcoin
- Ripple
- Litecoin
- Peercoin
- Namecoin
- Dogecoin
- Primecoin

Recently, a new digital currency attempted to emerge, known as COINYE (Originally called COINYE West) which was modeled after Bitcoin and implied a connection to rapper Kanye West via

a cartoon picture of Kanye West as the currency's logo. A lawsuit filed in a Manhattan federal court sought to stop COINYE on the grounds that it used the rapper's image to cash in on his popularity without his consent, damaging his reputation and confusing consumers about the source of the cryptocurrency.

Facing legal action, creators of COINY have ended the project and COINYE is now *Lost in the World*, but may have been nothing more than a *Dark Fantasy*.

Bitcoin

Bitcoin has garnered the most attention of any other digital currency, but even for its increasing awareness in the marketplace, many people do not completely understand what it is or how it works. Bitcoin has been called the world's "first decentralized digital currency" and was created in 2009 by a programmer using the alias, Satoshi Nakomoto. The idea behind Bitcoin is that it doesn't have a central clearinghouse or any singular authority and it is not pegged to any real tangible currency. Its value arises from the value that people assign to it. It works via peer-to-peer network where tasks are shared amongst multiple interconnected peers who each make a portion of their resources (computing power) directly available to other network participants, without the need for centralized coordination by servers. The network depends on users who provide their computing power to reconcile transactions and keep the block chain. These users in the system are called "minors" because they can potentially be rewarded for their participation in the network with the creation of Bitcoins. Bitcoins are created (mined) as thousands of dispersed computers solve complex math problems. With the solving of the complete math problem Bitcoins are created. Bitcoin was designed to be a finite resources such as gold or silver, thus the total number that can ever be created is capped at 21 million Bitcoins. It has been estimated that the last .00000001 of a Bitcoin will be "mined" in 2140.

Transactions occur via public key encryption which generates two mathematically related keys. One key, the private key is retained by the individual and the other key is made public. The intended recipients public key is used to encode payments, which can only be retrieved by the associated private key. The payer in the transaction uses his or her own private key to approve the transfer to the recipient. Every Bitcoin transaction is registered in a public, distributed ledger called the block chain. New transactions are checked against the block chain to ensure that the same Bitcoins have not already been spent.

Is Bitcoin completely anonymous? No, it has been described as pseudonymous as it is somewhat like cash in that once Bitcoins have been received by one party no third party exists between the parties that knows their identities. However, the transaction information is recorded in the block chain as has every Bitcoin transaction that has occurred in history. Additionally, a person's identity, such as IP address, is recoded when the person makes a Bitcoin transaction at a website or uses one of the numerous services to exchange dollars from Bitcoins. One study, "Evaluating User Privacy in Bitcoin" by Elli Androulaki found that using behavior based analytical techniques could reveal the identities of 40% of Bitcoin users.

Emergence of New Payment Systems Under Old Statutory Regimes.

In 2013, this committee held several oversight hearings examining the growth of technological innovation in the payments industry and the lack of modernity in some of California's statutes that

address the movement of money. The most recent hearing, The Technology of Consumer Financial Transactions, occurred on November 21, 2013 and highlighted the growing trends and changes within the payments world (Background paper available at http://abnk.assembly.ca.gov/sites/abnk.assembly.ca.gov/files/The%20Technology%20of%20Consumer%20Financial%20Transactions%20background%20document.pdf). What emerged from that hearing is that California has a growing and innovative payments market, but a stagnant regulatory regime. The majority of all hearing participants agreed that for most payment transactions a law already exist, but technology has confused the manner in which that law may apply and ultimately who may have the various legal responsibilities in the event of loss.

AB 129 is a continuation of efforts began last year to update, California's codes concerning payment systems. AB 129 amends Corporations Code 107, a largely outdated prohibition on the issuance and use of "anything but the lawful money of the United States." According to the literal meaning of the statute anyone that issues or uses digital currency, community currency, or perhaps even reward points is in violation of the law. However, staff is unaware of any prosecutions, arrest or enforcement actions relating to this statute. Section 107 can actually be traced back to the first state constitution of California, established in 1849, which contained a provision prohibiting the creation and issuance of paper to be used as money by any bank. This was a common prohibition across the states during the 19th century as the risk of states, or even non-state entities creating their own money was a real concern. In 1972, during a series of revisions to the California Constitution the currency provision was removed from the Constitution and placed in the Corporations Code.

Section 107 may not be necessary at all, but until further research is conducted staff recommends simply amending Section 107 until it is clear that its elimination will not create unintended consequences. In the intervening time the following technical amendments are suggested:

1) Eliminate references to "corporation, flexible purpose corporation, association, or individual" and instead replace with "person." The Corporations code already defines "person" to mean "corporation" and "individual" is never defined as a term, but is typically included in the "person" definition.

2) Insert "of the United States" after "money" on page 3, line 5.

REGISTERED SUPPORT / OPPOSITION:

Support

None on file.

Opposition

None on file.

Analysis Prepared by: Mark Farouk / B. & F. / (916) 319-3081

ASSEMBLY THIRD READING
AB 129 (Dickinson)
As Amended January 23, 2014
Majority vote

BANKING & FINANCE 10-0

Ayes: Dickinson, Morrell, Achadjian, Bonta, Chau, Gatto, Linder, Perea, Rodriguez, Weber

SUMMARY: Specifies that current law which bans the issuance or circulation of anything but lawful money of the United States does not prohibit the issuance and use of alternative currency.

EXISTING FEDERAL LAW provides that manufacturing counterfeit United States currency or altering genuine currency to increase its value is a violation of Title 18, Section 471 of the United States Code (U.S.C.) and is punishable by a fine of up to $5,000, or 15 years imprisonment, or both.

Possession of counterfeit United States obligations with fraudulent intent is a violation of Title 18, Section 472 of the U.S.C. and is punishable by a fine of up to $15,000, or 15 years imprisonment, or both.

Anyone who manufactures a counterfeit United States coin in any denomination above five cents is subject to the same penalties as all other counterfeiters. Anyone who alters a genuine coin to increase its numismatic value is in violation of Title 18, Section 331 of the U.S.C., which is punishable by a fine of up to $2,000, or imprisonment for up to five years, or both.

Forging, altering, or trafficking United States Government checks, bonds, or other obligations is a violation of Title 18, Section 510 of the U.S.C. and is punishable by a fine of up to $10,000, or 10 years imprisonment, or both.

Printed reproductions, including photographs of paper currency, checks, bonds, postage stamps, revenue stamps, and securities of the United States and foreign governments (except under the conditions previously listed) are violations of Title 18, Section 474 of the U.S.C. Violations are punishable by fines of up to $5,000, or 15 years imprisonment, or both.

U.S.C. 5103 Section 31 declares that United States coins and currency (including Federal Reserve Notes and circulating notes of Federal Reserve banks and national banks) are legal tender for all debts, public charges, taxes, and dues.

EXISTING STATE LAW provides under Corporations Code Section 107 that no corporation, flexible purpose corporation, association, or individual shall not issue or put in circulation, as money, anything but the lawful money of the United States.

FISCAL EFFECT: None

COMMENTS: This bill makes clarifying changes to current law to ensure that various forms of alternative currency such as digital currency, points, coupons, or other objects of monetary value

do not violate the law when those methods are used for the purchase of goods and services or the transmission of payments. Modern methods of payment have expanded beyond the typical cash or credit card transactions. Bitcoin, a digital currency (Also called cryptocurrency), has gained massive media attention recently as the number of businesses has expanded to accept Bitcoins for payment. Long before the introduction of digital currencies, various businesses have created points models that reward consumers with points for completion of various tasks such as spending a certain dollar amount, or even by purchasing points with dollars. These point systems effectively operate as currency allowing the consumers to buy a retail item or pay for some type of service. Many communities across the United States and in California have created "community currencies" that are created by members of a community in conjunction with merchants who agree to accept the alternative currency. These "community currencies" are created for a variety of reasons, some of which include encouraging consumers to shop at small businesses within the community or increasing neighborhood cohesiveness. "Community currency" has also become a form of political protest as some communities that use such currency do so in protest of United States monetary policies, or large financial institutions. The following is a list of "community currencies" in California:

1) Barter Bucks Concord, California

2) Bay Bucks San Francisco, California

3) Berkeley Barter Network Berkeley, California

4) Berkeley Bread Berkeley, California

5) Central Pound Clovis, California

6) Davis Dollars Davis, California

7) Escondido Dollars Escondido, California

8) Fairbuck Fairfax, California

9) Humboldt Hours Eureka, California and Arcata, California

10) Mendocino SEED Fort Bragg, California

11) North Fork Shares North Fork, California

12) San Luis Obispo Hours San Luis Obispo, California

13) Sand Dollars Bolinas, California

14) Santa Barbara Hours Santa Barbara, California

15) Santa Monica Hours Santa Monica, California

16) Sequoia Hours Garberville, California

17) Sonoma County Community Cash Santa Rosa, California

18) TradeMarket Nevada City, California

19) Ukiah Hours Ukiah, California

The following is a list of the largest digital currencies (cryptocurrencies) that are in use:

1) Bitcoin

2) Ripple

3) Litecoin

4) Peercoin

5) Namecoin

6) Dogecoin

7) Primecoin

Recently, a new digital currency attempted to emerge, known as COINYE (Originally called COINYE West) which was modeled after Bitcoin and implied a connection to rapper Kanye West via a cartoon picture of Kanye West as the currency's logo. A lawsuit filed in a Manhattan federal court sought to stop COINYE on the grounds that it used the rapper's image to cash in on his popularity without his consent, damaging his reputation and confusing consumers about the source of the cryptocurrency.

Facing legal action, creators of COINY have ended the project and COINYE is now *Lost in the World*, but may have been nothing more than a *Dark Fantasy*.

Bitcoin

Bitcoin has garnered the most attention of any other digital currency, but even for its increasing awareness in the marketplace, many people do not completely understand what it is or how it works. Bitcoin has been called the world's "first decentralized digital currency" and was created in 2009 by a programmer using the alias, Satoshi Nakomoto. The idea behind Bitcoin is that it does not have a central clearinghouse or any singular authority and it is not pegged to any real tangible currency. Its value arises from the value that people assign to it. It works via peer-to-peer network where tasks are shared amongst multiple interconnected peers who each make a portion of their resources (computing power) directly available to other network participants, without the need for centralized coordination by servers. The network depends on users who provide their computing power to reconcile transactions and keep the block chain. These users in the system are called "minors" because they can potentially be rewarded for their participation in the network with the creation of Bitcoins. Bitcoins are created (mined) as thousands of dispersed computers solve complex math problems. With the solving of the complete math problem Bitcoins are created. Bitcoin was designed to be a finite resource such as gold or silver,

thus the total number that can ever be created is capped at 21 million Bitcoins. It has been estimated that the last .00000001 of a Bitcoin will be "mined" in 2140.

Transactions occur via public key encryption which generates two mathematically related keys. One key, the private key is retained by the individual and the other key is made public. The intended recipients public key is used to encode payments, which can only be retrieved by the associated private key. The payer in the transaction uses his or her own private key to approve the transfer to the recipient. Every Bitcoin transaction is registered in a public, distributed ledger called the block chain. New transactions are checked against the block chain to ensure that the same Bitcoins have not already been spent.

Is Bitcoin completely anonymous? No, it has been described as pseudonymous as it is somewhat like cash in that once Bitcoins have been received by one party no third party exists between the parties that knows their identities. However, the transaction information is recorded in the block chain as has every Bitcoin transaction that has occurred in history. Additionally, a person's identity, such as IP address, is recoded when the person makes a Bitcoin transaction at a Web site or uses one of the numerous services to exchange dollars from Bitcoins. One study, "Evaluating User Privacy in Bitcoin" by Elli Androulaki found that using behavior based analytical techniques could reveal the identities of 40% of Bitcoin users. AB 129 is a continuation of efforts that began last year to update, California's codes concerning payment systems. AB 129 amends Corporations Code Section 107, a largely outdated prohibition on the issuance and use of "anything but the lawful money of the United States." According to the literal meaning of the statute anyone that issues or uses digital currency, community currency, or perhaps even reward points is in violation of the law. However, the Assembly Banking and Finance Committee is unaware of any prosecutions, arrest or enforcement actions relating to this statute. Corporations Code Section 107 can actually be traced back to the first state constitution of California, established in 1849, which contained a provision prohibiting the creation and issuance of paper to be used as money by any bank. This was a common prohibition across the states during the 19th century as the risk of states, or even non-state entities creating their own money was a real concern. In 1972, during a series of revisions to the California Constitution the currency provision was removed from the Constitution and placed in the Corporations Code.

Analysis Prepared by: Mark Farouk / B. & F. / (916) 319-3081

FN: 0002981

CONCURRENCE IN SENATE AMENDMENTS
AB 129 (Dickinson)
As Amended May 22, 2014
Majority vote

ASSEMBLY: 75-0 (January 29, 2014) SENATE: 28-3 (June 19, 2014)

Original Committee Reference: B. & F.

SUMMARY: Repeals existing law which bans the issuance or circulation of anything but lawful money of the United States.

The Senate amendments repeal Financial Code (FC) Section 107 which bans the use of anything but lawful currency.

EXISTING FEDERAL LAW provides that manufacturing counterfeit United States currency or altering genuine currency to increase its value is a violation of United States Code (U.S.C.) Title 18 Section 471 and is punishable by a fine of up to $5,000, or 15 years imprisonment, or both.

Possession of counterfeit United States obligations with fraudulent intent is a violation of U.S.C. Title 18 Section 472 and is punishable by a fine of up to $15,000, or 15 years imprisonment, or both.

Anyone who manufactures a counterfeit United States coin in any denomination above $0.05 is subject to the same penalties as all other counterfeiters. Anyone who alters a genuine coin to increase its numismatic value is in violation of U.S.C. Title 18 Section 331, which is punishable by a fine of up to $2,000, or imprisonment for up to five years, or both.

Forging, altering, or trafficking United States Government checks, bonds, or other obligations is a violation of U.S.C. Title 18 Section 510 and is punishable by a fine of up to $10,000, or 10 years imprisonment, or both.

Printed reproductions, including photographs of paper currency, checks, bonds, postage stamps, revenue stamps, and securities of the United States and foreign governments (except under the conditions previously listed) are violations of U.S.C. Title 18 Section 474. Violations are punishable by fines of up to $5,000, or 15 years imprisonment, or both.

U.S.C. Title 31 Section 5103 declares that United States coins and currency (including Federal Reserve Notes and circulating notes of Federal Reserve banks and national banks) are legal tender for all debts, public charges, taxes, and dues.

EXISTING STATE LAW provides under Corporations Code Section 107 that no corporation, flexible purpose corporation, association, or individual shall not issue or put in circulation, as money, anything but the lawful money of the United States.

AS PASSED BY THE ASSEMBLY, this bill amended FC Section 107 to specify that alternative currency such as digital currency are legal to use. Subsequent research provided that FC Section 107 was not necessary, so the entire section is repealed via the Senate amendments.

FISCAL EFFECT: None

COMMENTS: This bill makes clarifying changes to current law to ensure that various forms of alternative currency such as digital currency, points, coupons, or other objects of monetary value do not violate the law when those methods are used for the purchase of goods and services or the transmission of payments. Modern methods of payment have expanded beyond the typical cash or credit card transactions. Bitcoin, a digital currency (also called cryptocurrency), has gained massive media attention recently as the number of businesses has expanded to accept Bitcoins for payment. Long before the introduction of digital currencies, various businesses have created points models that reward consumers with points for completion of various tasks such as spending a certain dollar amount, or even by purchasing points with dollars. These point systems effectively operate as currency allowing the consumers to buy a retail item or pay for some type of service. Many communities across the United States and in California have created "community currencies" that are created by members of a community in conjunction with merchants who agree to accept the alternative currency. These "community currencies" are created for a variety of reasons, some of which include encouraging consumers to shop at small businesses within the community or increasing neighborhood cohesiveness. "Community currency" has also become a form of political protest as some communities that use such currency do so in protest of United States monetary policies, or large financial institutions. The following is a list of alternative currencies:

1) BerkShares. While Bitcoin and Litecoins are worldwide currencies, BerkShares are hyper-local: they are only accepted in the Berkshires, a region in western Massachusetts. According to the BerkShares Web site, more than 400 Berkshires businesses accept the currency, and 13 banks serve as exchange stations. "The currency distinguishes the local businesses that accept the currency from those that do not, building stronger relationships and greater affinity between the business community and the citizens," the site reads.

2) Equal Dollars. Philadelphia is also trying out a local currency with Equal Dollars. When you sign up to participate, you receive 50 Equal Dollars; to earn more, you can offer your own possessions in an online marketplace, volunteer or refer friends.

3) Starbucks Stars. Use of Starbucks Stars is limited not to a particular geographic locality, but to the corporate ecosystem that is Starbucks. Once you get a Starbucks Card, you can earn Starbucks Stars — which buy drinks and food — by paying with the card, using the Starbucks app, or entering Starbucks Star codes from various grocery store products. According to Kemp-Robertson, 30% of transactions at Starbucks are made using Starbucks Stars.

4) Amazon Coins. Another company-specific currency, Amazon Coins, can be exchanged for "Kindle Fire apps, games, or in-app items." You get 500 Amazon Coins, worth $5, by purchasing a Kindle Fire, or can buy more Amazon Coins at a slight savings.

5) Linden Dollars. Usable within the online community Second Life, can be bought with traditional currency or earned by selling goods or offering services to other Second Life residents. Many people earn actual Linden salaries — some to the tune of a million Linden Dollars.

6) Bitcoin. Bitcoin has garnered the most attention of any other digital currency, but even for its increasing awareness in the marketplace, many people do not completely understand what it is or how it works. Bitcoin has been called the world's "first decentralized digital currency" and was created in 2009 by a programmer using the alias, Satoshi Nakomoto. The idea behind Bitcoin is that it doesn't have a central clearinghouse or any singular authority and it is not pegged to any real tangible currency. Its value arises from the value that people assign to it. It works via peer-to-peer network where tasks are shared amongst multiple interconnected peers who each make a portion of their resources (computing power) directly available to other network participants, without the need for centralized coordination by servers. The network depends on users who provide their computing power to reconcile transactions and keep the block chain. These users in the system are called "minors" because they can potentially be rewarded for their participation in the network with the creation of Bitcoins. Bitcoins are created (mined) as thousands of dispersed computers solve complex math problems. With the solving of the complete math problem Bitcoins are created. Bitcoin was designed to be a finite resource such as gold or silver, thus the total number that can ever be created is capped at 21 million Bitcoins. It has been estimated that the last .00000001 of a Bitcoin will be "mined" in 2140.

Analysis Prepared by: Mark Farouk / B. & F. / (916) 319-3081

FN: 0003933

CONCURRENCE IN SENATE AMENDMENTS
AB 129 (Dickinson)
As Amended May 22, 2014
Majority vote

ASSEMBLY: 75-0 (January 29, 2014) SENATE: 28-3 (June 19, 2014)

Original Committee Reference: B. & F.

SUMMARY: Repeals existing law which bans the issuance or circulation of anything but lawful money of the United States.

The Senate amendments repeal Financial Code (FC) Section 107 which bans the use of anything but lawful currency.

EXISTING FEDERAL LAW provides that manufacturing counterfeit United States currency or altering genuine currency to increase its value is a violation of United States Code (U.S.C.) Title 18 Section 471 and is punishable by a fine of up to $5,000, or 15 years imprisonment, or both.

Possession of counterfeit United States obligations with fraudulent intent is a violation of U.S.C. Title 18 Section 472 and is punishable by a fine of up to $15,000, or 15 years imprisonment, or both.

Anyone who manufactures a counterfeit United States coin in any denomination above $0.05 is subject to the same penalties as all other counterfeiters. Anyone who alters a genuine coin to increase its numismatic value is in violation of U.S.C. Title 18 Section 331, which is punishable by a fine of up to $2,000, or imprisonment for up to five years, or both.

Forging, altering, or trafficking United States Government checks, bonds, or other obligations is a violation of U.S.C. Title 18 Section 510 and is punishable by a fine of up to $10,000, or 10 years imprisonment, or both.

Printed reproductions, including photographs of paper currency, checks, bonds, postage stamps, revenue stamps, and securities of the United States and foreign governments (except under the conditions previously listed) are violations of U.S.C. Title 18 Section 474. Violations are punishable by fines of up to $5,000, or 15 years imprisonment, or both.

U.S.C. Title 31 Section 5103 declares that United States coins and currency (including Federal Reserve Notes and circulating notes of Federal Reserve banks and national banks) are legal tender for all debts, public charges, taxes, and dues.

EXISTING STATE LAW provides under Corporations Code Section 107 that no corporation, flexible purpose corporation, association, or individual shall not issue or put in circulation, as money, anything but the lawful money of the United States.

AS PASSED BY THE ASSEMBLY, this bill amended FC Section 107 to specify that alternative currency such as digital currency are legal to use. Subsequent research provided that FC Section 107 was not necessary, so the entire section is repealed via the Senate amendments.

FISCAL EFFECT: None

COMMENTS: This bill makes clarifying changes to current law to ensure that various forms of alternative currency such as digital currency, points, coupons, or other objects of monetary value do not violate the law when those methods are used for the purchase of goods and services or the transmission of payments. Modern methods of payment have expanded beyond the typical cash or credit card transactions. Bitcoin, a digital currency (also called cryptocurrency), has gained massive media attention recently as the number of businesses has expanded to accept Bitcoins for payment. Long before the introduction of digital currencies, various businesses have created points models that reward consumers with points for completion of various tasks such as spending a certain dollar amount, or even by purchasing points with dollars. These point systems effectively operate as currency allowing the consumers to buy a retail item or pay for some type of service. Many communities across the United States and in California have created "community currencies" that are created by members of a community in conjunction with merchants who agree to accept the alternative currency. These "community currencies" are created for a variety of reasons, some of which include encouraging consumers to shop at small businesses within the community or increasing neighborhood cohesiveness. "Community currency" has also become a form of political protest as some communities that use such currency do so in protest of United States monetary policies, or large financial institutions. The following is a list of alternative currencies:

1) BerkShares. While Bitcoin and Litecoins are worldwide currencies, BerkShares are hyper-local: they are only accepted in the Berkshires, a region in western Massachusetts. According to the BerkShares Web site, more than 400 Berkshires businesses accept the currency, and 13 banks serve as exchange stations. "The currency distinguishes the local businesses that accept the currency from those that do not, building stronger relationships and greater affinity between the business community and the citizens," the site reads.

2) Equal Dollars. Philadelphia is also trying out a local currency with Equal Dollars. When you sign up to participate, you receive 50 Equal Dollars; to earn more, you can offer your own possessions in an online marketplace, volunteer or refer friends.

3) Starbucks Stars. Use of Starbucks Stars is limited not to a particular geographic locality, but to the corporate ecosystem that is Starbucks. Once you get a Starbucks Card, you can earn Starbucks Stars — which buy drinks and food — by paying with the card, using the Starbucks app, or entering Starbucks Star codes from various grocery store products. According to Kemp-Robertson, 30% of transactions at Starbucks are made using Starbucks Stars.

4) Amazon Coins. Another company-specific currency, Amazon Coins, can be exchanged for "Kindle Fire apps, games, or in-app items." You get 500 Amazon Coins, worth $5, by purchasing a Kindle Fire, or can buy more Amazon Coins at a slight savings.

5) Linden Dollars. Usable within the online community Second Life, can be bought with traditional currency or earned by selling goods or offering services to other Second Life residents. Many people earn actual Linden salaries — some to the tune of a million Linden Dollars.

6) Bitcoin. Bitcoin has garnered the most attention of any other digital currency, but even for its increasing awareness in the marketplace, many people do not completely understand what it is or how it works. Bitcoin has been called the world's "first decentralized digital currency" and was created in 2009 by a programmer using the alias, Satoshi Nakomoto. The idea behind Bitcoin is that it doesn't have a central clearinghouse or any singular authority and it is not pegged to any real tangible currency. Its value arises from the value that people assign to it. It works via peer-to-peer network where tasks are shared amongst multiple interconnected peers who each make a portion of their resources (computing power) directly available to other network participants, without the need for centralized coordination by servers. The network depends on users who provide their computing power to reconcile transactions and keep the block chain. These users in the system are called "minors" because they can potentially be rewarded for their participation in the network with the creation of Bitcoins. Bitcoins are created (mined) as thousands of dispersed computers solve complex math problems. With the solving of the complete math problem Bitcoins are created. Bitcoin was designed to be a finite resource such as gold or silver, thus the total number that can ever be created is capped at 21 million Bitcoins. It has been estimated that the last .00000001 of a Bitcoin will be "mined" in 2140.

Analysis Prepared by: Mark Farouk / B. & F. / (916) 319-3081

FN: 0003933

CONCURRENCE IN SENATE AMENDMENTS
AB 129 (Dickinson)
As Amended May 22, 2014
Majority vote

ASSEMBLY: 75-0 (January 29, 2014) SENATE: 28-3 (June 19, 2014)

Original Committee Reference: B. & F.

SUMMARY: Repeals existing law which bans the issuance or circulation of anything but lawful money of the United States.

The Senate amendments repeal Financial Code (FC) Section 107 which bans the use of anything but lawful currency.

EXISTING FEDERAL LAW provides that manufacturing counterfeit United States currency or altering genuine currency to increase its value is a violation of United States Code (U.S.C.) Title 18 Section 471 and is punishable by a fine of up to $5,000, or 15 years imprisonment, or both.

Possession of counterfeit United States obligations with fraudulent intent is a violation of U.S.C. Title 18 Section 472 and is punishable by a fine of up to $15,000, or 15 years imprisonment, or both.

Anyone who manufactures a counterfeit United States coin in any denomination above $0.05 is subject to the same penalties as all other counterfeiters. Anyone who alters a genuine coin to increase its numismatic value is in violation of U.S.C. Title 18 Section 331, which is punishable by a fine of up to $2,000, or imprisonment for up to five years, or both.

Forging, altering, or trafficking United States Government checks, bonds, or other obligations is a violation of U.S.C. Title 18 Section 510 and is punishable by a fine of up to $10,000, or 10 years imprisonment, or both.

Printed reproductions, including photographs of paper currency, checks, bonds, postage stamps, revenue stamps, and securities of the United States and foreign governments (except under the conditions previously listed) are violations of U.S.C. Title 18 Section 474. Violations are punishable by fines of up to $5,000, or 15 years imprisonment, or both.

U.S.C. Title 31 Section 5103 declares that United States coins and currency (including Federal Reserve Notes and circulating notes of Federal Reserve banks and national banks) are legal tender for all debts, public charges, taxes, and dues.

EXISTING STATE LAW provides under Corporations Code Section 107 that no corporation, flexible purpose corporation, association, or individual shall not issue or put in circulation, as money, anything but the lawful money of the United States.

AS PASSED BY THE ASSEMBLY, this bill amended FC Section 107 to specify that alternative currency such as digital currency are legal to use. Subsequent research provided that FC Section 107 was not necessary, so the entire section is repealed via the Senate amendments.

FISCAL EFFECT: None

COMMENTS: This bill makes clarifying changes to current law to ensure that various forms of alternative currency such as digital currency, points, coupons, or other objects of monetary value do not violate the law when those methods are used for the purchase of goods and services or the transmission of payments. Modern methods of payment have expanded beyond the typical cash or credit card transactions. Bitcoin, a digital currency (also called cryptocurrency), has gained massive media attention recently as the number of businesses has expanded to accept Bitcoins for payment. Long before the introduction of digital currencies, various businesses have created points models that reward consumers with points for completion of various tasks such as spending a certain dollar amount, or even by purchasing points with dollars. These point systems effectively operate as currency allowing the consumers to buy a retail item or pay for some type of service. Many communities across the United States and in California have created "community currencies" that are created by members of a community in conjunction with merchants who agree to accept the alternative currency. These "community currencies" are created for a variety of reasons, some of which include encouraging consumers to shop at small businesses within the community or increasing neighborhood cohesiveness. "Community currency" has also become a form of political protest as some communities that use such currency do so in protest of United States monetary policies, or large financial institutions. The following is a list of alternative currencies:

1) BerkShares. While Bitcoin and Litecoins are worldwide currencies, BerkShares are hyper-local: they are only accepted in the Berkshires, a region in western Massachusetts. According to the BerkShares Web site, more than 400 Berkshires businesses accept the currency, and 13 banks serve as exchange stations. "The currency distinguishes the local businesses that accept the currency from those that do not, building stronger relationships and greater affinity between the business community and the citizens," the site reads.

2) Equal Dollars. Philadelphia is also trying out a local currency with Equal Dollars. When you sign up to participate, you receive 50 Equal Dollars; to earn more, you can offer your own possessions in an online marketplace, volunteer or refer friends.

3) Starbucks Stars. Use of Starbucks Stars is limited not to a particular geographic locality, but to the corporate ecosystem that is Starbucks. Once you get a Starbucks Card, you can earn Starbucks Stars — which buy drinks and food — by paying with the card, using the Starbucks app, or entering Starbucks Star codes from various grocery store products. According to Kemp-Robertson, 30% of transactions at Starbucks are made using Starbucks Stars.

4) Amazon Coins. Another company-specific currency, Amazon Coins, can be exchanged for "Kindle Fire apps, games, or in-app items." You get 500 Amazon Coins, worth $5, by purchasing a Kindle Fire, or can buy more Amazon Coins at a slight savings.

5) Linden Dollars. Usable within the online community Second Life, can be bought with traditional currency or earned by selling goods or offering services to other Second Life residents. Many people earn actual Linden salaries — some to the tune of a million Linden Dollars.

6) Bitcoin. Bitcoin has garnered the most attention of any other digital currency, but even for its increasing awareness in the marketplace, many people do not completely understand what it is or how it works. Bitcoin has been called the world's "first decentralized digital currency" and was created in 2009 by a programmer using the alias, Satoshi Nakomoto. The idea behind Bitcoin is that it doesn't have a central clearinghouse or any singular authority and it is not pegged to any real tangible currency. Its value arises from the value that people assign to it. It works via peer-to-peer network where tasks are shared amongst multiple interconnected peers who each make a portion of their resources (computing power) directly available to other network participants, without the need for centralized coordination by servers. The network depends on users who provide their computing power to reconcile transactions and keep the block chain. These users in the system are called "minors" because they can potentially be rewarded for their participation in the network with the creation of Bitcoins. Bitcoins are created (mined) as thousands of dispersed computers solve complex math problems. With the solving of the complete math problem Bitcoins are created. Bitcoin was designed to be a finite resource such as gold or silver, thus the total number that can ever be created is capped at 21 million Bitcoins. It has been estimated that the last .00000001 of a Bitcoin will be "mined" in 2140.

Analysis Prepared by: Mark Farouk / B. & F. / (916) 319-3081

FN: 0003933

SENATE BANKING & FINANCIAL INSTITUTIONS COMMITTEE
Senator Noreen Evans, Chair
2013-2014 Regular Session

AB 129 (Dickinson) Hearing Date: June 4, 2014

As Amended: May 22, 2014
Fiscal: No
Urgency: No

SUMMARY Would delete the code section prohibiting the issuance or placement into circulation, as money, anything other than the lawful money of the United States.

EXISTING FEDERAL LAW

1. Prohibits the manufacture of counterfeit United States currency or the alteration of genuine currency to increase its value (18 USC Section 471).

EXISTING LAW

1. Prohibits a corporation, flexible purpose corporation, association, or individual from issuing or putting into circulation, as money, anything but the lawful money of the United States.

COMMENTS

1. Purpose: This bill is intended to delete a code section the author believes to be unnecessary.

2. Background: The concept contained in Corporations Code Section 107 originates with California's first Constitution, adopted in 1849. That constitution prohibited the creation and issuance of paper to be used as money by any bank – an attempt to ensure that only the federal government could issue lawful currency. During a series of revisions to California's Constitution in the early 1970s, the prohibition against placing currencies other than lawful money of the United States into circulation was placed in the Corporations Code. It has remained there ever since, essentially unchanged.

3. Discussion: Although it appears that no state department or agency has ever initiated an enforcement action for a violation of Corporations Code Section 107, this bill's author is concerned that Corporations Code Section 107 may restrict the development and use of alternate currencies. Alternative currencies include virtual currencies such as Bitcoin, Ripple, Peercoin, Primecoin, and others, and community currencies, such as Davis Dollars, Sonoma County Community Cash, Bay Bucks, and others.

   Virtual currencies are unique, typically encrypted computer files that can be converted to or from a government-backed currency to purchase goods and

services from merchants that accept virtual currencies. Virtual currency is accepted as currency by some businesses, exchanged for cash by others, and can also be purchased as an investment. Bitcoin is perhaps the most well-known of virtual currencies, and representative of some of the pitfalls of owning cyber cash. In February 2014, Mt. Gox, the largest and best-known Bitcoin exchange, announced that several hundred million dollars in Bitcoin had been hacked and stolen. Within a week of the announcement, Mt. Gox had declared bankruptcy. A similar fate befell a much smaller Bitcoin exchange called FlexCoin, which shut down after hackers stole $600,000 in Bitcoin from its servers. Although the currency survived the bankruptcies of these exchanges, some have pointed to Bitcoin users' vulnerability as support for predictions that Bitcoin is too fragile to survive long-term.

Community currencies are essentially vouchers or cash equivalents. They are purchased for cash, sometimes at a discount (i.e., $5 buys you $10 in community cash) and sometimes at face value ($5 in US currency buys you $5 in community currency). Typically, community currency is used as a way to encourage purchases at local merchants; because the currency is only accepted by merchants within the community currency network.

4. What Does California's Financial Regulator Think? California's Department of Business Oversight (DBO) is in the process of determining whether alternative currency exchanges fit into a traditional currency regulatory framework. DBO is, however, concerned about the risks that certain alternative currencies can pose.

   In April, 2014, DBO issued a consumer advisory, warning Californians of the risks of virtual currencies, also known as crypto-currencies, virtual money, or digital cash. In its consumer advisory, DBO characterized virtual currency transactions as high-risk, due to the vulnerability of cyber attacks, and observed that because virtual currency exchanges are unregulated, consumers have little recourse to recover lost funds. Unlike deposits at insured banks and credit unions, there is no virtual currency deposit insurance.

   DBO's consumer advisory also lists the following risks:

   a. There are few, if any, consumer protections without licensing. Virtual currencies are not regulated by any state in the United States, nor by the federal government.

   b. Virtual currency is difficult to recover, if stolen. If a virtual currency is stored on an electronic device that is stolen, lost, or destroyed, there may be no way for the owner to recover the currency stored on the lost, stolen, or destroyed device.

   c. Virtual currency represents an emerging technology, which is evolving rapidly. A currency accepted today may be obsolete tomorrow.

d. The value of virtual currency can fluctuate widely. Between March 2013 and March 2014, a single Bitcoin sold for as low as $100 and as high as $1,200.

e. Virtual currencies carry with them uncertain tax implications. Under a recent Internal Revenue Service ruling, all virtual currencies will be treated as property for tax purposes, and any value gains must be declared and will be taxed as a capital gain.

f. Virtual currencies have been associated with criminal enterprises, including illegal drug transactions, arms trading, money laundering, and other criminal activity. To the extent a virtual currency exchange is shut down by law enforcement, users of that virtual currency risk losing their investments.

5. Is This Bill Premature? Given the numerous risks associated with alternative currencies, it may be premature to delete the provision of California law which appears to prohibit them. However, since it appears that neither DBO nor the Attorney General have ever used Section 107 to sanction any issuers of either virtual or community currency, its deletion could be characterized as a simple codification of the state's policy toward the issuers and users of these currencies.

6. Summary of Arguments in Support: The author states, "The creation of a currency to undermine the U.S. dollar is not the same threat it was in the 18th century. Federal law is sufficient to prohibit and punish those actions, such as counterfeiting, that actually undermine U.S. currency."

7. Summary of Arguments in Opposition: None received.

LIST OF REGISTERED SUPPORT/OPPOSITION

Support

None received

Opposition

None received

Consultant: Eileen Newhall (916) 651-4102

SENATE RULES COMMITTEE AB 129
Office of Senate Floor Analyses
1020 N Street, Suite 524
(916) 651-1520 Fax: (916) 327-4478

THIRD READING

Bill No: AB 129
Author: Dickinson (D)
Amended: 5/22/14 in Senate
Vote: 21

SENATE BANKING & FINANCIAL INSTITUTIONS COMM.: 7-1, 6/4/14
AYES: Evans, Block, Correa, Hill, Roth, Torres, Vidak
NOES: Morrell
NO VOTE RECORDED: Hueso

ASSEMBLY FLOOR: 75-0, 1/29/14 - See last page for vote

SUBJECT: Lawful money

SOURCE: Author

DIGEST: This bill repeals the code section (Corporations Code [CORP] Section 107) prohibiting the issuance or placement into circulation, as money, anything other than the lawful money of the United States.

ANALYSIS: Existing federal law prohibits the manufacture of counterfeit United States currency or the alteration of genuine currency to increase its value.

Existing state law prohibits a corporation, flexible purpose corporation, association, or individual from issuing or putting into circulation, as money, anything but the lawful money of the United States.

This bill repeals the code section (CORP Section 107) prohibiting the issuance or placement into circulation, as money, anything other than the lawful money of the United States.

CONTINUED

Background

The concept contained in CORP Section 107 originates with California's first Constitution, adopted in 1849. That constitution prohibited the creation and issuance of paper to be used as money by any bank – an attempt to ensure that only the federal government could issue lawful currency. During a series of revisions to California's Constitution in the early 1970s, the prohibition against placing currencies other than lawful money of the United States into circulation was placed in the CORP. It has remained there ever since, essentially unchanged.

Alternative currencies. Although it appears that no state department or agency has ever initiated an enforcement action for a violation of CORP Section 107, this bill's author is concerned that CORP Section 107 may restrict the development and use of alternate currencies. Alternative currencies include virtual currencies (Bitcoin, Ripple, Peercoin, Primecoin, and others) and community currencies (Davis Dollars, Sonoma County Community Cash, Bay Bucks, and others).

Virtual currencies are unique, typically encrypted computer files that can be converted to or from a government-backed currency to purchase goods and services from merchants that accept virtual currencies. Virtual currency is accepted as currency by some businesses, exchanged for cash by others, and can also be purchased as an investment. Bitcoin is perhaps the most well-known of virtual currencies, and representative of some of the pitfalls of owning cyber cash. In February 2014, Mt. Gox, the largest and best-known Bitcoin exchange, announced that several hundred million dollars in Bitcoin had been hacked and stolen. Within a week of the announcement, Mt. Gox had declared bankruptcy. A similar fate befell a much smaller Bitcoin exchange called FlexCoin, which shut down after hackers stole $600,000 in Bitcoin from its servers. Although the currency survived the bankruptcies of these exchanges, some have pointed to Bitcoin users' vulnerability as support for predictions that Bitcoin is too fragile to survive long-term.

Community currencies are essentially vouchers or cash equivalents. They are purchased for cash, sometimes at a discount (i.e., $5 buys you $10 in community cash) and sometimes at face value ($5 in US currency buys you $5 in community currency). Typically, community currency is used as a way to encourage purchases at local merchants; because the currency is only accepted by merchants within the community currency network.

Department of Business Oversight (DBO): consumer advisory. DOB is in the process of determining whether alternative currency exchanges fit into a traditional

CONTINUED

currency regulatory framework. DBO is, however, concerned about the risks that certain alternative currencies can pose.

In April 2014, DBO issued a consumer advisory, warning Californians of the risks of virtual currencies, also known as crypto-currencies, virtual money, or digital cash. In its consumer advisory, DBO characterized virtual currency transactions as high-risk, due to the vulnerability of cyber attacks, and observed that because virtual currency exchanges are unregulated, consumers have little recourse to recover lost funds. Unlike deposits at insured banks and credit unions, there is no virtual currency deposit insurance.

DBO's consumer advisory also lists the following risks:

- There are few, if any, consumer protections without licensing. Virtual currencies are not regulated by any state in the United States, nor by the federal government.

- Virtual currency is difficult to recover, if stolen. If virtual currency is stored on an electronic device that is stolen, lost, or destroyed, there may be no way for the owner to recover the currency stored on the lost, stolen, or destroyed device.

- Virtual currency represents an emerging technology, which is evolving rapidly. A currency accepted today may be obsolete tomorrow.

- The value of virtual currency can fluctuate widely. Between March 2013 and March 2014, a single Bitcoin sold for as low as $100 and as high as $1,200.

- Virtual currencies carry with them uncertain tax implications. Under a recent Internal Revenue Service ruling, all virtual currencies will be treated as property for tax purposes, and any value gains must be declared and will be taxed as a capital gain.

- Virtual currencies have been associated with criminal enterprises, including illegal drug transactions, arms trading, money laundering, and other criminal activity. To the extent a virtual currency exchange is shut down by law enforcement, users of that virtual currency risk losing their investments.

Comments

According to the author, "AB 129 repeals Corporations Code Section 107 which is an outdated prohibition on the issuance and use of 'anything but the lawful money

CONTINUED

of the United States.' According to the literal meaning of the statute anyone that issues or uses digital currency, community currency, or perhaps even reward points is in violation of the law. However, no prosecutions, arrests or enforcement actions have occurred pursuant to this statute."

FISCAL EFFECT: Appropriation: No Fiscal Com.: No Local: No

ASSEMBLY FLOOR: 75-0, 1/29/14
AYES: Achadjian, Alejo, Allen, Ammiano, Atkins, Bigelow, Bloom, Bocanegra, Bonilla, Bonta, Bradford, Brown, Ian Calderon, Campos, Chau, Chávez, Chesbro, Conway, Cooley, Dababneh, Dahle, Daly, Dickinson, Donnelly, Eggman, Fong, Frazier, Beth Gaines, Garcia, Gatto, Gomez, Gonzalez, Gorell, Gray, Grove, Hagman, Hall, Harkey, Roger Hernández, Holden, Jones, Jones-Sawyer, Levine, Linder, Lowenthal, Maienschein, Mansoor, Medina, Melendez, Morrell, Mullin, Muratsuchi, Nazarian, Nestande, Olsen, Pan, Patterson, V. Manuel Pérez, Quirk, Quirk-Silva, Rendon, Ridley-Thomas, Rodriguez, Salas, Skinner, Stone, Ting, Wagner, Waldron, Weber, Wieckowski, Wilk, Williams, Yamada, John A. Pérez
NO VOTE RECORDED: Buchanan, Fox, Gordon, Logue, Perea

MW:nl 6/6/14 Senate Floor Analyses

SUPPORT/OPPOSITION: NONE RECEIVED

****** END ******

Exhibit AB

California LEGISLATIVE INFORMATION

AB-1326 Virtual currency. (2015-2016)

Date	Action
09/11/15	Ordered to inactive file at the request of Senator Mitchell.
08/31/15	Read second time. Ordered to third reading.
08/27/15	From committee: Do pass. (Ayes 6. Noes 1.) (August 27).
08/24/15	In committee: Referred to APPR. suspense file.
08/19/15	Re-referred to Com. on APPR.
08/19/15	Withdrawn from committee.
08/18/15	Read second time and amended. Re-referred to Com. on PUB. S.
08/17/15	From committee: Amend, and do pass as amended and re-refer to Com. on PUB. S. (Ayes 7. Noes 0.) (July 15).
07/06/15	From committee chair, with author's amendments: Amend, and re-refer to committee. Read second time, amended, and re-referred to Com. on B. & F.I.
06/18/15	Referred to Coms. on B. & F.I. and PUB. S.
06/03/15	In Senate. Read first time. To Com. on RLS. for assignment.
06/03/15	Read third time. Passed. Ordered to the Senate. (Ayes 55. Noes 22. Page 1879.)
06/02/15	Read second time. Ordered to third reading.
06/01/15	Read second time and amended. Ordered returned to second reading.
05/28/15	From committee: Amend, and do pass as amended. (Ayes 12. Noes 5.) (May 28).
05/13/15	In committee: Set, first hearing. Referred to APPR. suspense file.
04/28/15	From committee: Do pass and re-refer to Com. on APPR. (Ayes 8. Noes 2.) (April 27). Re-referred to Com. on APPR.
04/21/15	Re-referred to Com. on B. & F.
04/20/15	From committee chair, with author's amendments: Amend, and re-refer to Com. on B. & F. Read second time and amended.
03/23/15	Referred to Com. on B. & F.
03/02/15	Read first time.
03/01/15	From printer. May be heard in committee March 31.
02/27/15	Introduced. To print.

AMENDED IN SENATE AUGUST 18, 2015

AMENDED IN SENATE JULY 6, 2015

AMENDED IN ASSEMBLY JUNE 1, 2015

AMENDED IN ASSEMBLY APRIL 20, 2015

CALIFORNIA LEGISLATURE—2015–16 REGULAR SESSION

ASSEMBLY BILL No. 1326

Introduced by Assembly Member Dababneh

February 27, 2015

An act to repeal Section 107 of the Corporations Code, and to add Section 2178 to, and to add Division 11 (commencing with Section 26000) to, the Financial Code, relating to currency.

LEGISLATIVE COUNSEL'S DIGEST

AB 1326, as amended, Dababneh. Virtual currency.

~~Existing~~

(1) Existing law, the Money Transmission Act, prohibits a person from engaging in the business of money transmission in this state, or advertising, soliciting, or holding itself out as providing money transmission in this state, unless the person is licensed by the Commission of Business Oversight or exempt from licensure under the act. Existing law requires applicants for licensure to pay the commissioner a specified nonrefundable fee and to complete an application form requiring certain information. As security, existing law requires each licensee to deposit and maintain on deposit with the Treasurer cash in an amount not less than, or securities having a market value not less than, such amount as the commissioner may find and order from time to time as necessary to secure the faithful performance

of the obligations of the licensee with respect to money transmission in this state. Existing law requires a licensee at all times to own eligible securities, as defined, in a specified aggregate amount not less than the amount of all of its outstanding money received for transmission, as specified.

This bill would enact the Virtual Currency Act. The bill would prohibit a person from engaging in any virtual currency business, as defined, in this state unless the person is licensed by the Commissioner of Business Oversight or is exempt from the licensure requirement, as provided. The bill would require applicants for licensure, including an applicant for licensure and approval to acquire control of a licensee, to pay the commissioner a specified nonrefundable application fee and complete an application form required to include, among other things, information about the applicant, ~~prior~~ *previous* virtual currency services provided by the applicant, a sample form of receipt for transactions involving the business of virtual currency, and specified financial statements. The bill would make these licenses subject to annual renewal and would require a renewal fee paid to the commissioner in a specified amount. The bill would require licensees to annually pay the commissioner a specified amount for each licensee branch office. The bill would require applicants and licensees to pay the commissioner a specified hourly amount for the commissioner's examination costs, as provided. The bill would also require the commissioner to levy an assessment each fiscal year, on a pro rata basis, on licensees in an amount sufficient to meet the commissioner's expenses in administering these provisions and to provide a reasonable reserve for contingencies.

This bill would require each licensee to maintain at all times such capital as the commissioner determines, subject to specified factors, is sufficient to ensure the safety and soundness of the licensee, its ongoing operations, and maintain consumer protection. The bill would require each licensee to maintain a bond or trust account in United States dollars for the benefit of its consumers in the form and amount as specified by the commissioner.

This bill would authorize the commissioner to examine the business and any branch office of any licensee to ascertain whether the business is being conducted in a lawful manner and all virtual currency is properly accounted for. The bill would require a licensee to file a report with the commissioner within a specified period of time after the licensee knows about the occurrence of certain events relating to the virtual currency business and those persons connected to that business, and to also

maintain records as required by the commissioner for a specified period of time.

With regard to enforcement, among other things, this bill would, if it appears that a licensee is violating or failing to comply with these provisions or conducting business in an unsafe or injurious manner, authorize the commissioner to order the licensee to comply or discontinue those practices. The bill would also authorize the commissioner to issue an order suspending or revoking a license, or placing a licensee in receivership, if after notice and an opportunity for a hearing, the commissioner makes a specified finding. The bill would provide that every order, decision, or other official act of the commissioner is subject to review.

This bill would authorize the commissioner to impose a civil penalty for a violation of these provisions.

Within a specified period after the fiscal year, the bill would require a licensee to file with the commissioner a specified audit report. Within a specified period after the end of each calendar quarter, the bill would require a licensee to file with the commissioner a report containing financial statements verified by 2 of the licensee's principal officers.

By a specified date, the bill would require each licensee to file an annual report with the commissioner providing information regarding the licensee's business and operations within the state, as specified. The bill would also require each licensee to make other special reports to the commissioner. The bill would require these reports to be kept confidential. The bill would require the commissioner to prepare a report for publication on his or her Internet Web site summarizing the information from those reports and enforcement action information.

This bill would require a licensee to provide a specified consumer protection disclosure and receipt to its consumers.

This bill would authorize a virtual currency licensee in good standing that plans to engage in activities permitted under the Money Transmission Act to request that the commissioner convert his or her license into a license under the Money Transmission Act, as specified. ~~The~~

This bill would authorize a person or entity conducting virtual currency business with less than $1,000,000 in outstanding ~~obligations~~ *obligations, as defined,* and whose business model, as determined by the commissioner, represents low or no risk to consumers to ~~register with a $500 license fee~~ *pay a $500 application fee to the commissioner* and, if approved, receive a provisional license to conduct virtual

currency business. *The bill would authorize the commissioner to request reports and documents, to examine the provisional licensee, and gather information regarding the business and operations of provisional licensees. The bill would require reports and documents concerning the business and operations of provisional licensees to be kept confidential.*

This bill would require a licensee, under the Money Transmission Act, to report to the commissioner its plan to engage in any virtual currency business and request permission to engage in that business subject to specified requirements and conditions, as determined by the commissioner.

This bill would make these ~~provisions~~ *aforementioned provisions*, including the Virtual Currency ~~Act~~ *Act*, operative on July 1, 2016.

(2) Existing law, the General Corporation Law, prohibits a corporation, social purpose corporation, association, or individual from issuing or putting in circulation, as money, anything but the lawful money of the United States.

This bill would delete that prohibition.

(3) Existing constitutional provisions require that a statute that limits the right of access to the meetings of public bodies or the writings of public officials and agencies be adopted with findings demonstrating the interest protected by the limitation and the need for protecting that interest.

This bill would make legislative findings to that effect.

Vote: majority. Appropriation: no. Fiscal committee: yes. State-mandated local program: no.

The people of the State of California do enact as follows:

SECTION 1. Section 107 of the Corporations Code is repealed.

SEC. 2. Section 2178 is added to the Financial Code, to read:

2178. (a) Nothwithstanding any other law and consistent with subdivision (e) of Section 26004, a licensee shall report to the commissioner its plan to engage in any virtual currency business as described in Division 11 (commencing with Section 26000) and request, on a form provided by the commissioner, permission to engage in any virtual currency business without the issuance of a virtual currency license issued under Division 11 (commencing with Section 26000). However, the commissioner may require the licensee to increase its surety bond or eligible securities amounts

in an amount necessary to ensure the consumer protection of the additional business. The commissioner may also place, as a condition on the authorization to engage in any virtual currency business pursuant to Division 11 (commencing with Section 26000), any condition authorized by Section 2036.

(b) This section shall become operative on July 1, 2016.

SEC. 3. Division 11 (commencing with Section 26000) is added to the Financial Code, to read:

DIVISION 11. VIRTUAL CURRENCY

Chapter 1. General Provisions

26000. For purposes of this division, the following definitions shall apply:

(a) "Commissioner" means the Commissioner of Business Oversight.

(b) (1) "Virtual currency" means any type of digital unit that is used as a medium of exchange or a form of digitally stored value.

(2) Virtual currency does not include the following:

(A) Digital units that are used solely within online gaming platforms with no market or application outside of those gaming platforms.

(B) Digital units that are used exclusively as part of a consumer affinity or rewards program.

(C) Digital units that can be redeemed for goods, services, or for purchases with the issuer or other designated merchants, but cannot be converted into, or redeemed for, fiat currency.

(c) "Virtual currency business" means maintaining full custody or control of virtual currency in this state on behalf of others.

(d) "Fiat currency" means government-issued currency that is designated as legal tender through government decree, regulation, or law, that customarily refers to paper money and coin and is circulated, used, and accepted as money.

26001. For the purposes of carrying out the provisions of this division, the commissioner may adopt regulations pursuant to the Administrative Procedure Act (Chapter 3.5 (commencing with Section 11340) of Part 1 of Division 3 of Title 2 of the Government Code).

26001.5. This division shall be known and may be cited as the Virtual Currency Act.

Chapter 2. Licenses

26002. A person shall not engage in any virtual currency business in this state unless the person is licensed or exempt from licensure under this division.

26004. The following are exempt from the licensing requirement described in Section 26002:

(a) The United States or a department, agency, or instrumentality thereof, including any federal reserve bank and any federal home loan bank.

(b) Money transmission by the United States Postal Service or by a contractor on behalf of the United States Postal Service.

(c) A state, city, county, city and county, or any other governmental agency or governmental subdivision of a state.

(d) A commercial bank or industrial bank, the deposits of which are insured by the Federal Deposit Insurance Corporation or its successor, or any foreign (other nation) bank that is licensed under Chapter 20 (commencing with Section 1750) of Division 1.1 or that is authorized under federal law to maintain a federal agency or federal branch office in this state; a trust company licensed pursuant to Section 1042 or a national association authorized under federal law to engage in a trust banking business; an association or federal association, as defined in Section 5102, the deposits of which are insured by the Federal Deposit Insurance Corporation or its successor; and any federally or state chartered credit union, with an office in this state, the member accounts of which are insured or guaranteed as provided in Section 14858.

(e) Subject to Section 2178, an entity licensed as a money transmitter under the Money Transmission Act described in Division 1.2 (commencing with Section 2000).

(f) A merchant or consumer that utilizes virtual currency solely for the purchase or sale of goods or services.

(g) (1) A transaction in which the recipient of virtual currency is an agent of the payee pursuant to a preexisting written contract and delivery of the virtual currency to the agent satisfies the payor's obligation to the payee.

(2) For purposes of this subdivision, the following shall apply:

(A) "Agent" has the same meaning as that term is defined in Section 2295 of the Civil Code.

(B) "Payee" means the provider of goods or services, who is owed payment of money or other monetary value from the payor for the goods or services.

(C) "Payor" means the recipient of goods or services, who owes payment of money or monetary value to the payee for the goods or services.

(h) A person or entity developing, distributing, or servicing a virtual currency network software.

(i) A person or entity contributing software, connectivity, or computing power to a virtual currency network.

(j) A person or entity providing data storage or cyber security services for a licensed virtual currency business.

26006. (a) An applicant for licensure under this division shall pay to the commissioner a nonrefundable application fee of five thousand dollars ($5,000).

(b) An applicant for a license shall do so in a form and in a medium prescribed by the commissioner by order or regulation. The application shall state or contain all of the following:

(1) The legal name and residential business address of the applicant and any fictitious or trade name used by the applicant in conducting its business.

(2) A list of any criminal convictions of the applicant and any material litigation in which the applicant has been involved in the 10-year period next preceding the submission of the application.

(3) A description of any virtual currency services previously provided by the applicant and the virtual currency services that the applicant seeks to provide in this state.

(4) A list of other states in which the applicant is licensed to engage in the business of virtual currency and any license revocations, suspensions, or other disciplinary action taken against the applicant in another state.

(5) Information concerning any bankruptcy or receivership proceedings affecting the licensee.

(6) A sample form of receipt for transactions that involve money received for the business of virtual currency.

(7) The name and address of any bank through which the applicant's business will be conducted.

(8) A description of the source of money and credit to be used by the applicant to provide virtual currency services.

(9) The date of the applicant's incorporation or formation and the state or country of incorporation or formation.

(10) A certificate of good standing from the state or country in which the applicant is incorporated or formed.

(11) A description of the structure or organization of the applicant, including any parent or subsidiary of the applicant, and whether any parent or subsidiary is publicly traded.

(12) The legal name, any fictitious or trade name, all business and residential addresses, and the employment, in the 10-year period next preceding the submission of the application, of each executive officer, manager, director, or person that has control, of the applicant, and the educational background for each person.

(13) A list of any criminal convictions and material litigation in which any executive officer, manager, director, or person in control, of the applicant has been involved in the 10-year period next preceding the submission of the application.

(14) A copy of the applicant's audited financial statements for the most recent fiscal year and, if available, for the two-year period next preceding the submission of the application.

(15) A copy of the applicant's unconsolidated financial statements for the current fiscal year, whether audited or not, and, if available, for the two-year period next preceding the submission of the application.

(16) If the applicant is publicly traded, a copy of the most recent report filed with the United States Securities and Exchange Commission under Section 13 of the federal Securities Exchange Act of 1934 (15 U.S.C. Sec. 78m).

(17) If the applicant is a wholly owned subsidiary of:

(A) A corporation publicly traded in the United States, a copy of audited financial statements for the parent corporation for the most recent fiscal year or a copy of the parent corporation's most recent report filed under Section 13 of the federal Securities Exchange Act of 1934 (15 U.S.C. Sec. 78m) and, if available, for the two-year period next preceding the submission of the application.

(B) A corporation publicly traded outside the United States, a copy of similar documentation filed with the regulator of the parent corporation's domicile outside the United States.

(18) The applicant's plan for engaging in the business of virtual currency, including without limitation three years of pro forma financial statements.

(19) Any other information the commissioner requires with respect to the applicant.

(c) The commissioner may waive any of the information required under subdivision (b) or permit an applicant to submit other information instead of the required information.

(d) The nonrefundable application fee for filing an application for licensure and approval to acquire control of a licensee is three thousand five hundred dollars ($3,500). An applicant for licensure and approval shall comply with subdivision (b).

(e) A licensee, including a licensee described in subdivision (b), shall pay annually on or before July 1, a license renewal fee of two thousand five hundred dollars ($2,500).

(f) A licensee shall pay annually on or before July 1, one hundred twenty-five dollars ($125) for each licensee branch office in this state.

(g) Whenever the commissioner examines a licensee, the licensee shall pay, within 10 days after receipt of a statement from the commissioner, a fee of seventy-five dollars ($75) per hour for each examiner engaged in the examination plus, if it is necessary for any examiner engaged in the examination to travel outside this state, the travel expenses of the examiner.

(h) Whenever the commissioner examines an applicant, the applicant shall pay, within 10 days after receipt of a statement from the commissioner, a fee of seventy-five dollars ($75) per hour for each examiner engaged in the examination plus, if it is necessary for any examiner engaged in the examination to travel outside this state, the travel expenses of the examiner.

(i) Each fee for filing an application shall be paid at the time the application is filed with the commissioner. No fee for filing an application shall be refundable, regardless of whether the application is approved, denied, or withdrawn.

26008. (a) Each licensee shall maintain at all times such capital as the commissioner determines is sufficient to ensure the safety and soundness of the licensee and maintain consumer protection and its ongoing operations. In determining the minimum amount of capital that must be maintained by a licensee, the commissioner shall consider a variety of factors, including, but not limited to:

(1) The composition of the licensee's total assets, including the position, size, liquidity, risk exposure, and price volatility of each type of asset.

(2) The composition of the licensee's total liabilities, including the size and repayment timing of each type of liability.

(3) The actual and expected volume of the licensee's virtual currency business activity.

(4) Whether the licensee is already licensed or regulated by a state or federal entity, and whether the licensee is in good standing in such capacity.

(5) The amount of leverage employed by the licensee.

(6) The liquidity position of the licensee.

(7) The financial protection that the licensee provides for its consumers through its trust account or bond.

(b) Each licensee shall maintain a bond or trust account in United States dollars for the benefit of its consumers in the form and amount specified by the commissioner.

Chapter 3. Examinations and Records

26009. (a) The commissioner may at any time and from time to time examine the business and any branch office, within or outside this state, of any licensee in order to ascertain whether that business is being conducted in a lawful manner and whether all virtual currency held or exchanged is properly accounted for.

(b) The directors, officers, and employees of any licensee being examined by the commissioner shall exhibit to the commissioner, on request, any or all of the licensee's accounts, books, correspondence, memoranda, papers, and other records and shall otherwise facilitate the examination so far as it may be in their power to do so.

26010. The commissioner may consult and cooperate with other state or federal regulators in enforcing and administering this division. They may jointly pursue examinations and take other official action that they are otherwise empowered to take.

26011. A licensee shall file a report with the commissioner within five business days after the licensee has reason to know of the occurrence *of* any of the following events:

(a) The filing of a petition by or against the licensee under the United States Bankruptcy Code (11 U.S.C. Secs. 101-110, incl.) for bankruptcy or reorganization.

(b) The filing of a petition by or against the licensee for receivership, the commencement of any other judicial or administrative proceeding for its dissolution or reorganization, or the making of a general assignment for the benefit of its creditors.

(c) The commencement of a proceeding to revoke or suspend its virtual currency business license in a state or country in which the licensee engages in such business or is licensed to engage in such business.

(d) The cancellation or other impairment of the licensee's bond or trust account as required by subdivision (b) of Section 26008.

(e) A charge or conviction of the licensee or of an executive officer, manager, director, or person in control of the licensee for a felony.

26012. A licensee shall maintain any records as required by the commissioner for determining its compliance with this division for at least three years.

Chapter 4. Enforcement

26013. Any licensee may surrender its license by filing with the commissioner the license and a report with any information as the commissioner requires. The voluntary surrender of the license shall become effective at the time and upon the conditions as the commissioner specifies by order.

26014. (a) The commissioner may prepare written decisions, opinion letters, and other formal written guidance to be issued to persons seeking clarification regarding the requirements of this division.

(b) The commissioner shall make public on the commissioner's Internet Web site all written decisions, opinion letters, and other formal written guidance issued to persons seeking clarification regarding the requirements of this division. The commissioner may, at his or her discretion or upon request by an applicant or licensee, redact proprietary or other confidential information regarding an applicant or licensee from any decision, letter, or other written guidance issued in connection with an applicant or licensee.

26015. The commissioner may offer informal guidance to any prospective applicant for a license under this division, regarding the conditions of licensure that may be applied to that person. The commissioner shall inform any applicant that requests that guidance of the licensing requirements that will be required of that applicant, based on the information provided by the applicant concerning its plan to conduct business under this division, and the factors used to make that determination.

26016. At any time, if the commissioner deems it necessary for the general welfare of the public, he or she may exercise any power set forth in this division with respect to a virtual currency business, regardless of whether an application for a license has been filed with the commissioner, a license has been issued, or, if issued, the license has been surrendered, suspended, or revoked.

(a) If it appears to the commissioner that a licensee is violating or failing to comply with this division, the commissioner may direct the licensee to comply with the law by an order issued under the commissioner's official seal, or if it appears to the commissioner that any licensee is conducting its business in an unsafe or injurious manner, the commissioner may in like manner direct it to discontinue the unsafe or injurious practices. The order shall require the licensee to show cause before the commissioner, at a time and place to be fixed by the commissioner, as to why the order should not be observed.

(b) If, upon any hearing held pursuant to subdivision (a), the commissioner finds that the licensee is violating or failing to comply with any law of this state or is conducting its business in an unsafe or injurious manner, the commissioner may make a final order directing it to comply with the law or to discontinue the unsafe or injurious practices. A licensee shall comply with the final order unless, within 10 days after the issuance of the order, its enforcement is restrained in a proceeding brought by the licensee.

26017. (a) The commissioner may issue an order suspending or revoking a license, or taking possession of and placing a licensee in receivership, if after notice and an opportunity for hearing, the commissioner finds any of the following:

(1) The licensee is violating this division or a regulation adopted or an order issued under this division, or a condition of approval issued under this division.

(2) The licensee does not cooperate with an examination or investigation by the commissioner.

(3) The licensee engages in fraud, intentional misrepresentation, or gross negligence.

(4) The competence, experience, character, or general fitness of the licensee, or any director, officer, employee, or person in control of a licensee, indicates that it is not in the public interest to permit the person to provide virtual currency services.

(5) The licensee engages in an unsafe or unsound practice.

(6) The licensee is insolvent, suspends payment of its obligations, or makes a general assignment for the benefit of its creditors.

(7) The licensee has applied for an adjudication of bankruptcy, reorganization, arrangement, or other relief under any bankruptcy, reorganization, insolvency, or moratorium law, or any person has applied for any such relief under that law against the licensee and the licensee has by any affirmative act approved of or consented to the action or the relief has been granted.

(8) Any fact or condition exists that, if it had existed at the time ~~when~~ the licensee applied for its license, would have been grounds for denying the application.

(b) In determining whether a licensee is engaging in an unsafe or unsound practice, the commissioner may consider the size and condition of the licensee's provision of virtual currency services, the magnitude of the loss, the gravity of the violation of this division, and the previous conduct of the person involved.

26018. (a) Every order, decision, or other official act of the commissioner is subject to review in accordance with law.

(b) Whenever the commissioner has taken possession of the property and business of any licensee, the licensee, within 10 days after that taking, if it deems itself aggrieved thereby, may apply to the superior court in the county in which the head office of the licensee is located to enjoin further proceedings. The court, after citing the commissioner to show cause why further proceedings should not be enjoined and after a hearing and a determination of the facts upon the merits, may dismiss the application or enjoin the commissioner from further proceedings and direct the commissioner to surrender the property and business to the licensee.

26019. (a) If the commissioner finds that any of the factors set forth in Section 26017 is true with respect to any licensee and that it is necessary for the protection of the public interest, the commissioner may issue an order immediately suspending or revoking the licensee's license.

(b) Within 30 days after the license is suspended or revoked pursuant to subdivision (a), the licensee may file with the commissioner an application for a hearing on the suspension or revocation.

(c) If the commissioner fails to commence a hearing within 15 business days after the application is filed with the commissioner pursuant to subdivision (b) or within a longer period of time agreed to by the licensee, the suspension or revocation shall be deemed rescinded.

(d) Within 30 days after the hearing, the commissioner shall affirm, modify, or rescind the suspension or revocation. Otherwise, the suspension or revocation shall be deemed rescinded.

(e) The right of the licensee to petition for judicial review of the suspension or revocation shall not be affected by the failure of the licensee to apply to the commissioner for a hearing on the suspension or revocation pursuant to subdivision (b).

26020. The commissioner may assess a civil penalty against a person that violates this division or a regulation adopted or an order issued under this division in an amount not to exceed one thousand dollars ($1,000) for each violation or, in the case of a continuing violation, one thousand dollars ($1,000) for each day or part thereof during which the violation continues, plus this state's costs and expenses for the investigation and prosecution of the matter, including reasonable attorney's fees.

26022. The enforcement provisions of this division are in addition to any other enforcement powers that the commissioner may have under law.

26023. (a) The commissioner may by order or regulation grant exemptions from this section in cases where the commissioner finds that the requirements of this section are not necessary or may be duplicative.

(b) A licensee shall, within 90 days after the end of each fiscal year, or within any extended time as the commissioner may prescribe, file with the commissioner an audit report for the fiscal year that shall comply with all of the following provisions:

(1) The audit report shall contain audited financial statements of the licensee for or as of the end of the fiscal year prepared in accordance with United States generally accepted accounting principles and any other information as the commissioner may require.

(2) The audit report shall be based upon an audit of the licensee conducted in accordance with United States generally accepted auditing standards and any other requirements as the commissioner may prescribe.

(3) The audit report shall be prepared by an independent certified public accountant or independent public accountant who is not unsatisfactory to the commissioner.

(4) The audit report shall include or be accompanied by a certificate of opinion of the independent certified public accountant or independent public accountant that is satisfactory in form and content to the commissioner. If the certificate or opinion is qualified, the commissioner may order the licensee to take any action as the commissioner may find necessary to enable the independent or certified public accountant or independent public accountant to remove the qualification.

(c) Each licensee shall, not more than 45 days after the end of each calendar year quarter, or within a longer period as the commissioner may by regulation or order specify, file with the commissioner a report containing all of the following:

(1) Financial statements, including balance sheet, income statement, statement of changes in shareholders' equity, and statement of cashflows, for, or as of the end of, that calendar year quarter, verified by two of the licensee's principal officers. The verification shall state that each of the officers making the verification has ~~a~~ personal knowledge of the matters in the report and that each of them believes that each statement in the report is true.

(2) Other information as the commissioner may by regulation or order require.

(d) Each licensee shall file an annual report with the commissioner, on or before the 15th day of March, providing the relevant information that the commissioner reasonably requires concerning the business and operations conducted by the licensee within the state during the preceding calendar year. Each licensee shall also make other special reports to the commissioner that may

be required by the commissioner from time to time. The reports required by this subdivision shall be kept confidential pursuant to Chapter 3.5 (commencing with Section 6250) of Division 7 of Title 1 of the Government Code and any regulations adopted thereunder.

(e) The commissioner shall annually prepare a report for publication on his or her Internet Web site, summarizing consolidated information gained from the reports required pursuant to subdivision (d), documenting the number of licenses, including provisional licenses as described in Section 26032, outstanding during the prior calendar year, and summarizing the numbers and types of enforcement actions brought by the commissioner pursuant to this division during the prior calendar year.

26024. In addition to the fees provided in Section 26006, the commissioner shall levy an assessment each fiscal year, on a pro rata basis, on those licensees that at any time during the preceding calendar year engaged in this state in the virtual currency business in an amount that is, in his or her judgment, sufficient to meet the commissioner's expenses in administering the provisions of this division and to provide a reasonable reserve for contingencies.

Chapter 5. Miscellaneous Provisions

26025. A licensee shall disclose to consumers the following disclosure in a form and manner prescribed by the commissioner:

"Once submitted to the network, a virtual currency transaction will be unconfirmed for a period of time (usually less than one hour, but up to one day or more) pending sufficient confirmation of the transaction by the network. A transaction is not complete while it is in a pending state. Virtual currency associated with transactions that are in a pending state will be designated accordingly, and will not be included in your account balance or be available to conduct transactions.

The risk of loss in trading or holding virtual currency can be substantial. You should therefore carefully consider whether trading or holding virtual currency is suitable for you in light of your financial condition. In considering whether to trade or hold virtual currency, you should be aware that the price or value of virtual currency can change rapidly, decrease, and potentially even fall to zero.

(Insert company name) is licensed by the Department of Business Oversight to do business in California. If you have complaints with respect to any aspect of the virtual currency business conducted by (company name), you may contact the California Department of Business Oversight at its toll-free telephone number, 1-800-622-0620, by email at consumer.services@dbo.ca.gov, or by mail at the Department of Business Oversight, Consumer Services, 1515 K Street, Suite 200, Sacramento, CA 95814."

26026. (a) Upon completion of a transaction subject to this division, the licensee shall provide to the consumer a receipt containing the following information:

(1) The name and contact information of the licensee including a telephone number of the licensee where consumers can contact the licensee for questions or to register complaints.

(2) The type, value, date, and time of the transaction.

(3) The type and amount of any fees charged.

(4) The exchange rate, if applicable.

(5) A statement of the refund policy of the licensee.

(6) Additional information the commissioner may require.

(b) The receipt required by this section shall be made in English and in the language principally used by that licensee to advertise, solicit, or negotiate, either orally or in writing, if other than English.

(c) The receipt required by this section may be provided electronically for transactions that are initiated electronically or in which a consumer agrees to receive an electronic receipt.

26029. The commissioner may, by regulation or order, either unconditionally or upon specified terms and conditions or for specified periods, exempt from all or part of this division any person or transaction or class of persons or transactions, if the commissioner finds such action to be in the public interest and that the regulation of such persons or transactions is not necessary for the purposes of this division. The commissioner shall post on the commissioner's Internet Web site a list of all persons, transactions, or classes of person or transactions exempt pursuant to this section, and the provision or provisions of this division from which they are exempt.

26031. Notwithstanding any other law, a licensee in good standing under this division that plans to engage in activities permitted under the Money Transmission Act (Division 1.2 (commencing with Section 2000)) may request from the

commissioner in a form specified by the commissioner to convert their license into a license under Division 1.2 (commencing with Section 2000). A licensee's request to convert its license shall be accompanied by documentation or other evidence as determined by the commissioner that the licensee meets the requirements for licensure under Division 1.2 (commencing with Section 2000). If a licensee's request for a converted license is granted, the licensee shall be subject to Section 2178 in order to thereafter engage in any virtual currency business.

26032. (a) ~~A~~ *(1) In lieu of Section 26006, a* person or entity conducting virtual currency business with less than one million dollars ($1,000,000) in outstanding obligations and whose business model, as determined by the commissioner, represents low or no risk to consumers may ~~register with a five-hundred-dollar ($500) license fee with the~~ *pay an application fee of five hundred dollars ($500) to the* commissioner and, if approved, receive a provisional license to conduct virtual currency business. A person or entity that receives such a license shall also register with FinCEN as a money services business, if applicable.

(2) For the purposes of this section, "outstanding obligations" means the value under the full custody and control of the person or entity.

(b) In determining whether to issue a provisional license, the commissioner shall consider a variety of factors, including, but not limited to:

(1) The nature and scope of the applicant's business.

(2) The anticipated volume of business to be transacted by the applicant in California.

(3) The nature and scope of the risks that the applicant's business presents to consumers.

(4) The measures which the applicant has taken to limit or mitigate the risks its business presents.

(5) Whether the applicant is regulated or otherwise authorized by another governmental entity to engage in financial services or other business activities.

(c) ~~The~~ *Sections 26006, 26008, 26023, 26024, and 26031 shall not apply to a person or entity to which a provisional license has been issued. However, the* commissioner may require a provisional licensee to certify adherence to certain risk based performance

standards related to safety, soundness, and consumer protection as prescribed by the commissioner.

(d) Based upon the factors identified in subdivision (b) and the provisional licensee's history as a holder of a provisional license, the commissioner may at any time renew such license for an additional length of time or remove the provisional status from the license if the licensee meets all the requirements of this division. Unless the commissioner otherwise removes the provisional status of or renews such license, a provisional license shall expire two years after the date of issuance. If the commissioner renews a provisional license, the licensee shall pay a five-hundred-dollar ($500) renewal fee.

(e) The commissioner may request reports and documents and may ~~audit~~ *examine* the provisional licensee as needed to further consumer ~~protection and~~ *protection,* enhance safety and ~~soundness.~~ *soundness, and gather information regarding the business and operations of provisional licensees. Reports and documents concerning the business and operations of provisional licensees shall be kept confidential pursuant to Chapter 3.5 (commencing with Section 6250) of Division 7 of Title 1 of the Government Code and any regulations adopted thereunder. The commissioner shall include aggregated information about the business and operations of provisional licensees in the report required by and subject to subdivision (e) of Section 26023.*

(f) A provisional licensee shall notify the commissioner within 15 days of surpassing the threshold in subdivision (a) and shall, within 30 days from that notice, apply for a license pursuant to Chapter 2 (commencing with Section 26002).

(g) A provisional license may be suspended or revoked pursuant to Section 26017.

Chapter 6. Operative Date

26040. This division shall become operative on July 1, 2016.

SEC. 4. The Legislature finds and declares that Section 3 of this act, which adds Sections 26023 and 26032 to the Financial Code, imposes a limitation on the public's right of access to the meetings of public bodies or the writings of public officials and agencies within the meaning of Section 3 of Article I of the California Constitution. Pursuant to that constitutional provision,

the Legislature makes the following findings to demonstrate the interest protected by this limitation and the need for protecting that interest:

In order to allow the Commissioner of Business Oversight of the Department of Business Oversight to fully accomplish his or her goals, it is imperative to protect the interests of those persons submitting information to the department to ensure that any personal or sensitive business information that this act requires those persons to submit is protected as confidential information.

~~SEC. 2. No reimbursement is required by this act pursuant to Section 6 of Article XIII B of the California Constitution because the only costs that may be incurred by a local agency or school district will be incurred because this act creates a new crime or infraction, eliminates a crime or infraction, or changes the penalty for a crime or infraction, within the meaning of Section 17556 of the Government Code, or changes the definition of a crime within the meaning of Section 6 of Article XIII B of the California Constitution.~~

-

O

Date of Hearing: April 27, 2015

ASSEMBLY COMMITTEE ON BANKING AND FINANCE
Matthew Dababneh, Chair
AB 1326 (Dababneh) – As Amended April 20, 2015

SUBJECT: Virtual currency

SUMMARY: Requires the licensing of entities engaged in the business of virtual currency by the Department of Business Oversight (DBO). Specifically, **this bill**:

1) Defines "virtual currency" as any type of digital unit that is used as a medium of exchange or a form of digitally stored value or that is incorporated into payment system technology. Virtual currency shall be broadly construed to include digital units of exchange that (1) have a centralized repository or administrator, (2) are decentralized and have no centralized repository or administrator, or (3) may be created or obtained by computing or manufacturing effort. Virtual currency shall not be construed to include digital units that are used solely within online gaming platforms with no market or application outside of those gaming platforms, nor shall virtual currency be construed to include digital units that are used exclusively as part of a customer affinity or rewards program, and can be applied solely as payment redeemed for goods, services, or for purchases with the issuer or other designated merchants, but cannot be converted into, or redeemed for, fiat currency.

2) Defines "virtual currency business" as the conduct of either of the following types of activities involving a California resident:

    a) Storing, holding, or maintaining custody or control of virtual currency on behalf of others; or

    b) Providing conversion or exchange services of fiat currency into virtual currency or the conversion or exchange of virtual currency into fiat currency or other value, or the conversion or exchange of one form of virtual currency into another form of virtual currency.

3) Provides for the following exemptions:

    a) The United States or a department, agency, or instrumentality thereof, including any federal reserve bank and any federal home loan bank;

    b) Money transmission by the United States Postal Service or by a contractor on behalf of the United States Postal Service;

    c) A state, city, county, city and county, or any other governmental agency or governmental subdivision of a state;

    d) A commercial bank or industrial bank, the deposits of which are insured by the Federal Deposit Insurance Corporation (FDIC) or its successor, or any foreign (other nation) bank that is licensed under state law or that is authorized under federal law to maintain a federal agency or federal branch office in this state; a trust company licensed pursuant to

Section 1042 or a national association authorized under federal law to engage in a trust banking business; an association or federal association, as defined in Section 5102, the deposits of which are insured by the FDIC or its successor; and any federally or state chartered credit union, with an office in this state, the member accounts of which are insured or guaranteed as provided in Section 14858;

e) An entity licensed as a money transmitter under the Money Transmission Act;

f) A merchant or consumer that utilizes virtual currency solely for the purchase or sale of goods or services; or

g) A transaction in which the recipient of virtual currency is an agent of the payee pursuant to a preexisting written contract and delivery of the virtual currency to the agent satisfies the payor's obligation to the payee. "Agent" has the same meaning as that term as defined in Section 2295 of the Civil Code. "Payee" means the provider of goods or services, who is owed payment of money or other monetary value from the payor for the goods or services. "Payor" means the recipient of goods or services, who owes payment of money or monetary value to the payee for the goods or services.

4) Requires an applicant for a license to pay the commissioner of DBO (commissioner) a nonrefundable application fee of five thousand dollars ($5,000).

5) Provides that an applicant for a license shall do so in a form and in a medium prescribed by the commissioner by order or regulation.

6) Allows for the following licensing fees:

   a) A nonrefundable application fee for filing an application for licensure and approval to acquire control of a licensee is three thousand five hundred dollars ($3,500);

   b) A license renewal fee of two thousand five hundred dollars ($2,500); and

   c) A licensee shall pay annually on or before July 1, one hundred twenty-five dollars ($125) for each licensee branch office in this state.

7) Requires that each licensee shall maintain at all times such capital as the commissioner determines is sufficient to ensure the safety and soundness of the licensee and maintain consumer protection and its ongoing operations.

8) Specifies that a licensee shall not appoint or continue any person as agent, unless the licensee and the person have made a written contract that requires the agent to operate in full compliance with this division.

9) Provides that an agent shall not provide any virtual currency business outside the scope of activity permissible under the written contract between the agent and the licensee.

10) Requires each licensee to exercise reasonable supervision over its agents to ensure compliance with applicable laws, rules, and regulations with regard to the virtual currency

business.

11) Prohibits a licensee from appointing any person as an agent unless it has conducted a review of the proposed agent's fitness to act as an agent and has determined that the proposed agent and any persons who control the proposed agent are of good character and sound financial standing.

12) Requires a licensee to maintain records of this review for each agent while the agent is providing any virtual currency business on behalf of the licensee, and for three years after the relationship with the agent has terminated.

13) Prohibits a person, including an agent, from providing any virtual currency business on behalf of a person not licensed or not exempt from licensure under this division.

14) Specifies that a person that engages in that activity provides virtual currency business to the same extent as if the person was a licensee and shall be jointly and severally liable with the unlicensed or nonexempt person.

15) Allows the commissioner at any time and from time to time examine the business and any branch office, within or outside this state, of any licensee in order to ascertain whether that business is being conducted in a lawful manner and whether all virtual currency held or exchanged is properly accounted for.

16) Requires the directors, officers, and employees of any licensee being examined by the commissioner shall exhibit to the commissioner, on request, any or all of the licensee's accounts, books, correspondence, memoranda, papers, and other records and shall otherwise facilitate the examination so far as it may be in their power to do so.

17) Requires a licensee to file a report with the commissioner within five business days after the licensee has reason to know of any occurrence of the following events:

    a) The filing of a petition by or against the licensee under the United States Bankruptcy Code (11 U.S.C. Secs. 101-110, incl.) for bankruptcy or reorganization;

    b) The filing of a petition by or against the licensee for receivership, the commencement of any other judicial or administrative proceeding for its dissolution or reorganization, or the making of a general assignment for the benefit of its creditors;

    c) The commencement of a proceeding to revoke or suspend its virtual currency business license in a state or country in which the licensee engages in such business or is licensed to engage in such business;

    d) The cancellation or other impairment of the licensee's bond or trust account as required by subdivision (b) of Section 26008; or

    e) A charge or conviction of the licensee or of an executive officer, manager, director, or person in control of the licensee for a felony.

18) Requires a licensee to maintain any records as required by the commissioner for determining its compliance with this division for at least three years.

19) Allows a licensee to surrender its license by filing with the commissioner the license and a report with any information as the commissioner requires. The voluntary surrender of the license shall become effective at the time and upon the conditions as the commissioner specifies by order.

20) Gives authority to the commissioner to prepare written decisions, opinion letters, and other formal written guidance to be issued to persons seeking clarification regarding the requirements of this division.

21) Requires the commissioner to make public on the commissioner's Internet Web site all written decisions, opinion letters, and other formal written guidance issued to persons seeking clarification regarding the requirements of this division. The commissioner may, at his or her discretion or upon request by an applicant or licensee, redact proprietary or other confidential information regarding an applicant or licensee from any decision, letter, or other written guidance issued in connection with an applicant or licensee.

22) Allows the commissioner to offer informal guidance to any prospective applicant for a license under this division, regarding the conditions of licensure that may be applied to that person. The commissioner shall inform any applicant that requests that guidance of the licensing requirements that will be required of that applicant, based on the information provided by the applicant concerning its plan to conduct business under this division, and the factors used to make that determination.

23) Gives the commissioner authority, if the commissioner deems it necessary for the general welfare of the public, to exercise any power set forth in this division with respect to a virtual currency business, regardless of whether an application for a license has been filed with the commissioner, a license has been issued, or, if issued, the license has been surrendered, suspended, or revoked.

24) States that if it appears to the commissioner that a licensee is violating or failing to comply with this division, the commissioner may direct the licensee to comply with the law by an order issued under the commissioner's official seal, or if it appears to the commissioner that any licensee is conducting its business in an unsafe or injurious manner, the commissioner may in like manner direct it to discontinue the unsafe or injurious practices. The order shall require the licensee to show cause before the commissioner, at a time and place to be fixed by the commissioner, as to why the order should not be observed.

25) Provides that if, upon any hearing the commissioner finds that the licensee is violating or failing to comply with any law of this state or is conducting its business in an unsafe or injurious manner, the commissioner may make a final order directing it to comply with the law or to discontinue the unsafe or injurious practices. A licensee shall comply with the final order unless, within 10 days after the issuance of the order, its enforcement is restrained in a proceeding brought by the licensee.

26) Allows the commissioner to issue an order suspending or revoking a license, or taking possession of and placing a licensee in receivership, if after notice and an opportunity for

hearing, the commissioner finds any of the following:

a) The licensee does not cooperate with an examination or investigation by the commissioner;

b) The licensee engages in fraud, intentional misrepresentation, or gross negligence;

c) The competence, experience, character, or general fitness of the licensee, or any director, officer, employee, or person in control of a licensee, indicates that it is not in the public interest to permit the person to provide virtual currency services;

d) The licensee engages in an unsafe or unsound practice;

e) The licensee is insolvent, suspends payment of its obligations, or makes a general assignment for the benefit of its creditors;

f) The licensee has applied for an adjudication of bankruptcy, reorganization, arrangement, or other relief under any bankruptcy, reorganization, insolvency, or moratorium law, or any person has applied for any such relief under that law against the licensee and the licensee has by any affirmative act approved of or consented to the action or the relief has been granted; or,

g) Any fact or condition exists that, if it had existed at the time when the licensee applied for its license, would have been grounds for denying the application;

27) In determining whether a licensee is engaging in an unsafe or unsound practice, the commissioner may consider the size and condition of the licensee's provision of virtual currency services, the magnitude of the loss, the gravity of the violation, and the previous conduct of the person involved.

28) Allows the commissioner to assess a civil penalty against a person that violates this division or a regulation adopted or an order issued under this division in an amount not to exceed one thousand dollars ($1,000) for each violation or, in the case of a continuing violation, one thousand dollars ($1,000) for each day or part thereof during which the violation continues, plus this state's costs and expenses for the investigation and prosecution of the matter, including reasonable attorney's fees.

29) Specifies that a person that engages in unlicensed activity or intentionally makes a false statement, misrepresentation, or false certification in a record filed or required to be maintained under this division or that intentionally makes a false entry or omits a material entry in such a record is guilty of a felony.

30) Allows the commissioner, by order or regulation grant exemptions from this section in cases where the commissioner finds that the requirements of this section are not necessary or may be duplicative.

31) Requires a licensee, within 90 days after the end of each fiscal year, or within any extended time as the commissioner may prescribe, file with the commissioner an audit report for the

fiscal year.

32) Specifies that each licensee shall, not more than 45 days after the end of each calendar year quarter, or within a longer period as the commissioner may by regulation or order specify, file with the commissioner a report containing all of the following:

   a) Financial statements, including balance sheet, income statement, statement of changes in shareholders' equity, and statement of cashflows, for, or as of the end of, that calendar year quarter, verified by two of the licensee's principal officers. The verification shall state that each of the officers making the verification has a personal knowledge of the matters in the report and that each of them believes that each statement in the report is true; and,

   b) Other information as the commissioner may by regulation or order require.

33) Allows the commissioner to levy an assessment each fiscal year, on a pro rata basis, on those licensees that at any time during the preceding calendar year engaged in this state in the virtual currency business in an amount that is, in his or her judgment, sufficient to meet the commissioner's expenses in administering the provisions of this division and to provide a reasonable reserve for contingencies.

34) Requires a licensee to disclose to consumers the following disclosure in a form and manner prescribed by the commissioner:

   "Once submitted to the network, a virtual currency transaction will be unconfirmed for a period of time (usually less than one hour, but up to one day or more) pending sufficient confirmation of the transaction by the network. A transaction is not complete while it is in a pending state. Virtual currency associated with transactions that are in a pending state will be designated accordingly, and will not be included in your account balance or be available to conduct transactions.

   The risk of loss in trading or holding virtual currency can be substantial. You should therefore carefully consider whether trading or holding virtual currency is suitable for you in light of your financial condition. In considering whether to trade or hold virtual currency, you should be aware that the price or value of virtual currency can change rapidly, decrease, and potentially even fall to zero.

   (Insert company name) is licensed by the Department of Business Oversight to do business in California. If you have complaints with respect to any aspect of the virtual currency business conducted by (company name), you may contact the California Department of Business Oversight at its toll-free telephone number, 1-800-622-0620, by email at consumer.services@dbo.ca.gov, or by mail at the Department of Business Oversight, Consumer Services, 1515 K Street, Suite 200, Sacramento, CA 95814."

EXISTING LAW: Regulates the transmission of money under the money transmission act (Financial Code, Section 2000-2175)

FISCAL EFFECT: Unknown

COMMENTS:

The author has introduced this bill to ensure that entities that store virtual currency or offer the exchange of virtual currency with consumers are operated in a safe and sound manner. AB 1326 will protect consumers that utilize virtual currency services by ensuring that these businesses are able to protect consumer's virtual currency from potential loss. Additionally, this bill will provide regulatory certainty as many companies try to engage in the virtual currency business have sought out money transmission licenses only to be denied, or are even unsure if their business model fits into existing licensing structures for other financial services entities.

The New York State Department of Banking was the first regulatory agency to issue regulations concerning virtual currency. This launched nationwide efforts to look at whether the virtual currency business should be regulated. The Conference of State Banking Supervisors (CSBS) formed the CSBS Emerging Payments Task Force ("Task Force") to examine the intersection between state supervision and payments developments, and to identify areas for consistent regulatory approaches among states. This effort includes an assessment of virtual currency activities and outreach with a broad range of stakeholders. After engaging with industry participants, state and federal regulators, and other stakeholders, CSBS recommended that activities involving third party control of virtual currency, including for the purposes of transmitting, exchanging, holding, or otherwise controlling virtual currency, should be subject to state licensure and supervision.

Headlines concerning virtual currency have been dominated by Bitcoin with some of this attention resulting from negative publicity. The high profile *Silk Road* case in which federal law enforcement officials arrested the operator of an online illegal drug market place that facilitated the sale of drugs and other illegal goods through acceptance of Bitcoins. Bitcoins were used because it is a decentralized currency allowing users to be pseudonymous to some extent, even though every Bitcoin transaction is logged. Bitcoin is not the first, nor the only virtual currency. Numerous models of virtual currency have sprouted up over the last decade, and this growth has inspired additional questions by government officials and policy makers.

Bitcoin has received its share of negative attention from its wild price fluctuations, awareness against Bitcoin "Wallets" (as the individual software applications that manage bitcoin holdings) to being credited with being the currency of choice for criminal activity. As to the latter attribution, cash money is still the dominant and preferred source of anonymous payment for illegal activities. Some of the attention, specifically in relation to the risk associated with storing virtual currency has raised the attention of state regulators across the country.

Even though the core program that runs bitcoin has resisted six years of hacking attempts, the successful attacks on associated businesses have created the impression that bitcoin isn't a safe way to store money. Bitcoins exist purely as entries in an accounting system—a transparent public ledger known as the "blockchain" that records balances and transfers among special bitcoin "addresses." With bitcoin, the balances held by every user of the monetary system are instead recorded on a widely distributed, publicly displayed ledger that is kept up-to-date by thousands of independently owned, competing computers known as "miners."

What does a real world transaction look like such as buying a cup of coffee at your local coffee shop? If you pay with a credit card, the transaction seems simple enough: You swipe your card, you grab your cup, and you leave. The financial system is just getting started with you and the coffee shop. Before the store actually gets paid and your bank balance falls, more than a half-

dozen institutions—such as a billing processor, the card association your bank, the coffee shop's bank, a payment processor, the clearinghouse network managed by the regional Federal Reserve Banks—will have shared part of your account information or otherwise intervened in the flow of money. If all goes well, your bank will confirm your identity and good credit and send payment to the coffee shop's bank two or three days later. For this privilege, the coffee shop pays a fee of between 2% and 3%.

Now let's pay in Bitcoin. If you don't already have bitcoins, you will need to buy some from one of a host of online exchanges and brokerages, using a simple transfer from your regular bank account. You will then assign the bitcoins to a wallet, which functions like an online account. Once inside the coffee shop, you will open your wallet's smartphone app and hold its QR code reader up to the coffee shop's device. This allows your embedded secret password to unlock a bitcoin address and publicly informs the bitcoin computer network that you are transferring $1.75 worth of bitcoin (currently about 0.0075 bitcoin) to the coffee shop's address. This takes just seconds, and then you walk off with your coffee. Next, in contrast to the pay with credit/debit system, your transaction is immediately broadcast to the world (in alphanumeric data that can't be traced to you personally). Your information is then gathered up by bitcoin "miners," the computers that maintain the system and are compensated, roughly every 10 minutes, for their work confirming transactions. The computer that competes successfully to package the data from your coffee purchase adds that information to the blockchain ledger, which prompts all the other miners to investigate the underlying transaction. Once your bona fides are verified, the updated blockchain is considered legitimate, and the miners update their records accordingly. It takes from 10 minutes to an hour for this software-driven network of computers to formally confirm a transfer from your blockchain address to that of the coffee shop—compared with a two- to three-day wait for the settlement of a credit-card transaction. Some new digital currencies are able to finalize transactions within seconds. There are almost zero fees, and the personal information of users isn't divulged. This bitcoin feature especially appeals to privacy advocates: Nobody learns where you buy coffee. The advantages of digital currency are far more visible in emerging markets. It allows migrant workers, for example, to bypass fees that often run to 10% or more for the international payment services that they use to send money home to their families. Although many companies now accept bitcoin (the latest and biggest being Microsoft Corp.), global usage of the digital currency averaged just $50 million a day in 2014. Over that same period, Visa and MasterCard processed some $32 billion a day. The market capitalization for BitCoin is almost at $4 billion with virtual currency Ripple the next largest at over $340 million.

FinCEN Guidance on Virtual Currencies

FinCEN issued interpretive guidance earlier this year to clarify how the Bank Secrecy Act (BSA) and FinCEN regulations apply to users, administrators and exchangers of virtual currencies. Under the regulatory framework, virtual currency is defined as having some but not all of the attributes of "real currency" and therefore, virtual currency does not have legal tender status in any jurisdiction. Specifically, the FinCEN guidance addresses convertible virtual currency which either has a real currency equivalent value or serves as a substitute for real currency.

The roles of persons (including legal entities) involved in virtual currency transactions are defined by FinCEN as follows:

- User: A person who obtains virtual currency to purchase goods or services

- Exchanger: A person engaged as a business in the exchange of virtual currency for real currency, funds or other virtual currency
- Administrator: A person engaged as a business in issuing into circulation a virtual currency and who has the authority to redeem and withdraw from circulation such virtual currency

A person, or legal entity, may act in more than one of these capacities. Further, it is important to note that "obtaining" virtual currency covers much more than the scenario of a "user" who merely purchases virtual currency. Depending on the model of the particular currency, a party could "obtain" virtual currency through various acts including earning, harvesting, mining, creating, auto-generating, manufacturing or purchasing.

The threshold issue is whether actions will subject a person or legal entity to BSA's registration, reporting and recordkeeping regulations that apply to money services businesses (MSBs). A user who obtains convertible virtual currency and uses it to purchase real or virtual goods or services is not subject to MSB compliance because such activity does not meet the definition of "money transmission services" and the user would not be a "money transmitter."

However, an administrator or exchanger engages in money transmission services and, as a result, is a "money transmitter" under FinCEN definitions by (1) accepting and transmitting convertible virtual currency or (2) buying or selling convertible virtual currency. As a money transmitter, the administrator or exchanger would generally be subject to MSB reporting and recordkeeping.

Further, the FinCEN guidance expressly addresses the category of de-centralized virtual currency – the Bitcoin model – and states that "a person is an exchanger and a money transmitter if the person accepts such de-centralized convertible virtual currency from one person and transmits it to another person as part of the acceptance and transfer of currency, funds, or other value that substitutes for currency."

In the area of foreign exchange, accepting real currency in exchange for virtual currency is not subject to FinCEN regulations applicable to "dealers in foreign exchange" since a forex transaction involves exchanging the currency of two countries and virtual currency does not constitute legal tender as a currency of a country.

The author's office has been meeting with various stakeholders and will continue to work out the various details of this legislation as it moves forward. Some key issues that still need to be resolved:

1) Further strengthen and clarify definition of "virtual currency business."

2) Clarify the factors that will be used to determine capitalization requirements.

3) Specify clear bonding and security amounts and factors used to make that determination.

4) Examine issues relating to start-up companies.

Previous Legislation.

AB 129 (Dickinson), chapter 74, statutes of 2014 clarified California law to ensure that alternative currency, including virtual currency would not be potentially deemed illegal tender.

REGISTERED SUPPORT / OPPOSITION:

Support

None on file.

Opposition

None on file.

Analysis Prepared by: Mark Farouk / B. & F. / (916) 319-3081

ASSEMBLY THIRD READING
AB 1326 (Dababneh)
As Amended June 1, 2015
Majority vote

Committee	Votes	Ayes	Noes
Banking	8-2	Dababneh, Achadjian, Brown, Chau, Gatto, Low, Ridley-Thomas, Mark Stone	Hadley, Kim
Appropriations	12-5	Gomez, Bonta, Calderon, Daly, Eggman, Eduardo Garcia, Gordon, Holden, Quirk, Rendon, Weber, Wood	Bigelow, Chang, Gallagher, Jones, Wagner

SUMMARY: Requires the licensing of entities engaged in the business of virtual currency by the Department of Business Oversight (DBO). Specifically, **this bill**:

1) Defines "virtual currency" as any type of digital unit that is used as a medium of exchange or a form of digitally stored value. Virtual currency does not include digital units that are used solely within online gaming platforms with no market or application outside of those gaming platforms, nor shall virtual currency be construed to include digital units that are used exclusively as part of a customer affinity or rewards program, and can be applied solely as payment redeemed for goods, services, or for purchases with the issuer or other designated merchants, but cannot be converted into, or redeemed for, fiat currency.

2) Defines "virtual currency business" as the conduct of either of the following types of activities involving a California resident:

   a) Maintaining full custody or control of virtual currency on behalf of others; or

   b) Providing conversion or exchange services of fiat currency into virtual currency or the conversion or exchange of virtual currency into fiat currency or other value, or the conversion or exchange of one form of virtual currency into another form of virtual currency.

3) Defines "fiat currency" as government-issued currency that is designated as legal tender through government decree, regulation, or law that customarily refers to paper money and coin that is circulated and used and accepted as money.

4) Provides for the following exemptions:

   a) The United States or a department, agency, or instrumentality thereof, including any federal reserve bank and any federal home loan bank;

   b) Money transmission by the United States Postal Service or by a contractor on behalf of the United States Postal Service;

   c) A state, city, county, city and county, or any other governmental agency or governmental subdivision of a state;

d) A commercial bank or industrial bank, the deposits of which are insured by the Federal Deposit Insurance Corporation (FDIC) or its successor, or any foreign (other nation) bank that is licensed under state law or that is authorized under federal law to maintain a federal agency or federal branch office in this state; a trust company licensed pursuant to Financial Code Section 1042 or a national association authorized under federal law to engage in a trust banking business; an association or federal association, as defined in Financial Code Section 5102, the deposits of which are insured by the FDIC or its successor; and any federally or state chartered credit union, with an office in this state, the member accounts of which are insured or guaranteed as provided in Financial Code Section 14858;

e) An entity licensed as a money transmitter under the Money Transmission Act;

f) A merchant or consumer that utilizes virtual currency solely for the purchase or sale of goods or services;

g) A transaction in which the recipient of virtual currency is an agent of the payee pursuant to a preexisting written contract and delivery of the virtual currency to the agent satisfies the payor's obligation to the payee. "Agent" has the same meaning as that term as defined in Civil Code Section 2295. "Payee" means the provider of goods or services, who is owed payment of money or other monetary value from the payor for the goods or services. "Payor" means the recipient of goods or services, who owes payment of money or monetary value to the payee for the goods or services;

h) A person or entity developing, distributing, or servicing a virtual currency network software;

i) A person or entity contributing software, connectivity, or computing power to a virtual currency network; or,

j) A person or entity providing data storage or cyber security services for a licensed virtual currency business.

5) Requires an applicant for a license to pay the commissioner of DBO (commissioner) a nonrefundable application fee of $5,000.

6) Provides that an applicant for a license shall do so in a form and in a medium prescribed by the commissioner by order or regulation.

7) Allows for the following licensing fees:

a) A nonrefundable application fee for filing an application for licensure and approval to acquire control of a licensee is $3,500;

b) A license renewal fee of $2,500; and

c) A licensee shall pay annually on or before July 1, $125 for each licensee branch office in this state.

8) Requires that each licensee shall maintain at all times such capital as the commissioner determines is sufficient to ensure the safety and soundness of the licensee and maintain consumer protection and its ongoing operations.

9) Specifies that a licensee shall not appoint or continue any person as agent, unless the licensee and the person have made a written contract that requires the agent to operate in full compliance with this division.

10) Provides that an agent shall not provide any virtual currency business outside the scope of activity permissible under the written contract between the agent and the licensee.

11) Requires each licensee to exercise reasonable supervision over its agents to ensure compliance with applicable laws, rules, and regulations with regard to the virtual currency business.

12) Prohibits a licensee from appointing any person as an agent unless it has conducted a review of the proposed agent's fitness to act as an agent and has determined that the proposed agent and any persons who control the proposed agent are of good character and sound financial standing.

13) Requires a licensee to maintain records of this review for each agent while the agent is providing any virtual currency business on behalf of the licensee, and for three years after the relationship with the agent has terminated.

14) Prohibits a person, including an agent, from providing any virtual currency business on behalf of a person not licensed or not exempt from licensure under this division.

15) Specifies that a person that engages in that activity provides virtual currency business to the same extent as if the person was a licensee and shall be jointly and severally liable with the unlicensed or nonexempt person.

16) Allows the commissioner at any time and from time to time examine the business and any branch office, within or outside this state, of any licensee in order to ascertain whether that business is being conducted in a lawful manner and whether all virtual currency held or exchanged is properly accounted for.

17) Requires the directors, officers, and employees of any licensee being examined by the commissioner shall exhibit to the commissioner, on request, any or all of the licensee's accounts, books, correspondence, memoranda, papers, and other records and shall otherwise facilitate the examination so far as it may be in their power to do so.

18) Requires a licensee to file a report with the commissioner within five business days after the licensee has reason to know of any occurrence of the following events:

    a) The filing of a petition by or against the licensee under the United States Bankruptcy Code (11 United States Code Sections 101 to 110, inclusive) for bankruptcy or reorganization;

    b) The filing of a petition by or against the licensee for receivership, the commencement of any other judicial or administrative proceeding for its dissolution or reorganization, or the making of a general assignment for the benefit of its creditors;

    c) The commencement of a proceeding to revoke or suspend its virtual currency business license in a state or country in which the licensee engages in such business or is licensed to engage in such business;

    d) The cancellation or other impairment of the licensee's bond or trust account as required by Financial Code Section 26008(b); or

e) A charge or conviction of the licensee or of an executive officer, manager, director, or person in control of the licensee for a felony.

19) Requires a licensee to maintain any records as required by the commissioner for determining its compliance with this division for at least three years.

20) Allows a licensee to surrender its license by filing with the commissioner the license and a report with any information as the commissioner requires. The voluntary surrender of the license shall become effective at the time and upon the conditions as the commissioner specifies by order.

21) Gives authority to the commissioner to prepare written decisions, opinion letters, and other formal written guidance to be issued to persons seeking clarification regarding the requirements of this division.

22) Requires the commissioner to make public on the commissioner's Internet Web site all written decisions, opinion letters, and other formal written guidance issued to persons seeking clarification regarding the requirements of this division. The commissioner may, at his or her discretion or upon request by an applicant or licensee, redact proprietary or other confidential information regarding an applicant or licensee from any decision, letter, or other written guidance issued in connection with an applicant or licensee.

23) Allows the commissioner to offer informal guidance to any prospective applicant for a license under this division, regarding the conditions of licensure that may be applied to that person. The commissioner shall inform any applicant that requests that guidance of the licensing requirements that will be required of that applicant, based on the information provided by the applicant concerning its plan to conduct business under this division, and the factors used to make that determination.

24) Gives the commissioner authority, if the commissioner deems it necessary for the general welfare of the public, to exercise any power set forth in this division with respect to a virtual currency business, regardless of whether an application for a license has been filed with the commissioner, a license has been issued, or, if issued, the license has been surrendered, suspended, or revoked.

25) States that if it appears to the commissioner that a licensee is violating or failing to comply with this division, the commissioner may direct the licensee to comply with the law by an order issued under the commissioner's official seal, or if it appears to the commissioner that any licensee is conducting its business in an unsafe or injurious manner, the commissioner may in like manner direct it to discontinue the unsafe or injurious practices. The order shall require the licensee to show cause before the commissioner, at a time and place to be fixed by the commissioner, as to why the order should not be observed.

26) Provides that if, upon any hearing the commissioner finds that the licensee is violating or failing to comply with any law of this state or is conducting its business in an unsafe or injurious manner, the commissioner may make a final order directing it to comply with the law or to discontinue the unsafe or injurious practices. A licensee shall comply with the final order unless, within 10 days after the issuance of the order, its enforcement is restrained in a proceeding brought by the licensee.

27) Allows the commissioner to issue an order suspending or revoking a license, or taking possession of and placing a licensee in receivership, if after notice and an opportunity for hearing, the commissioner finds any of the following:

   a) The licensee does not cooperate with an examination or investigation by the commissioner;

   b) The licensee engages in fraud, intentional misrepresentation, or gross negligence;

   c) The competence, experience, character, or general fitness of the licensee, or any director, officer, employee, or person in control of a licensee, indicates that it is not in the public interest to permit the person to provide virtual currency services;

   d) The licensee engages in an unsafe or unsound practice;

   e) The licensee is insolvent, suspends payment of its obligations, or makes a general assignment for the benefit of its creditors;

   f) The licensee has applied for an adjudication of bankruptcy, reorganization, arrangement, or other relief under any bankruptcy, reorganization, insolvency, or moratorium law, or any person has applied for any such relief under that law against the licensee and the licensee has by any affirmative act approved of or consented to the action or the relief has been granted; or,

   g) Any fact or condition exists that, if it had existed at the time when the licensee applied for its license, would have been grounds for denying the application;

28) In determining whether a licensee is engaging in an unsafe or unsound practice, the commissioner may consider the size and condition of the licensee's provision of virtual currency services, the magnitude of the loss, the gravity of the violation, and the previous conduct of the person involved.

29) Allows the commissioner to assess a civil penalty against a person that violates this division or a regulation adopted or an order issued under this division in an amount not to exceed $1,000 for each violation or, in the case of a continuing violation, $1,000 for each day or part thereof during which the violation continues, plus this state's costs and expenses for the investigation and prosecution of the matter, including reasonable attorney's fees.

30) Specifies that a person that engages in unlicensed activity or intentionally makes a false statement, misrepresentation, or false certification in a record filed or required to be maintained under this division or that intentionally makes a false entry or omits a material entry in such a record is guilty of a felony.

31) Allows the commissioner, by order or regulation grant exemptions from this section in cases where the commissioner finds that the requirements of this section are not necessary or may be duplicative.

32) Requires a licensee, within 90 days after the end of each fiscal year, or within any extended time as the commissioner may prescribe, file with the commissioner an audit report for the fiscal year.

33) Specifies that each licensee shall, not more than 45 days after the end of each calendar year quarter, or within a longer period as the commissioner may by regulation or order specify, file with the commissioner a report containing all of the following:

    a) Financial statements, including balance sheet, income statement, statement of changes in shareholders' equity, and statement of cashflows, for, or as of the end of, that calendar year quarter, verified by two of the licensee's principal officers. The verification shall state that each of the officers making the verification has a personal knowledge of the matters in the report and that each of them believes that each statement in the report is true; and,

    b) Other information as the commissioner may by regulation or order require.

34) Allows the commissioner to levy an assessment each fiscal year, on a pro rata basis, on those licensees that at any time during the preceding calendar year engaged in this state in the virtual currency business in an amount that is, in his or her judgment, sufficient to meet the commissioner's expenses in administering the provisions of this division and to provide a reasonable reserve for contingencies.

35) Requires a licensee to disclose to consumers the following disclosure in a form and manner prescribed by the commissioner:

    Once submitted to the network, a virtual currency transaction will be unconfirmed for a period of time (usually less than one hour, but up to one day or more) pending sufficient confirmation of the transaction by the network. A transaction is not complete while it is in a pending state. Virtual currency associated with transactions that are in a pending state will be designated accordingly, and will not be included in your account balance or be available to conduct transactions.

    The risk of loss in trading or holding virtual currency can be substantial. You should therefore carefully consider whether trading or holding virtual currency is suitable for you in light of your financial condition. In considering whether to trade or hold virtual currency, you should be aware that the price or value of virtual currency can change rapidly, decrease, and potentially even fall to zero.

    (Insert company name) is licensed by the Department of Business Oversight to do business in California. If you have complaints with respect to any aspect of the virtual currency business conducted by (company name), you may contact the California Department of Business Oversight at its toll-free telephone number, 1-800-622-0620, by email at consumer.services@dbo.ca.gov, or by mail at the Department of Business Oversight, Consumer Services, 1515 K Street, Suite 200, Sacramento, CA 95814.

EXISTING LAW: Regulates the transmission of money under the money transmission act (Financial Code Sections 2000 to 2175)

FISCAL EFFECT: According to the Assembly Appropriations Committee, estimated annual General Fund administrative costs to DBO of approximately $3.3 million to establish, manage, and enforce the licensing regime, eventually offset by application, renewal, and location fees as well as pro rata assessments to offset administrative costs.

COMMENTS:

The author has introduced this bill to ensure that entities that store virtual currency or offer the exchange of virtual currency with consumers are operated in a safe and sound manner. This bill will protect consumers that utilize virtual currency services by ensuring that these businesses are able to protect consumer's virtual currency from potential loss. Many companies operating in the virtual currency space have sought out regulatory and statutory certainty regard their operations. This bill will provide this certainty by establishing a clear regulatory framework that mirrors other types of financial services regulation.

The New York State Department of Banking was the first regulatory agency to issue regulations concerning virtual currency. This launched nationwide efforts to look at whether the virtual currency business should be regulated. The Conference of State Banking Supervisors (CSBS) formed the CSBS Emerging Payments Task Force (Task Force) to examine the intersection between state supervision and payments developments, and to identify areas for consistent regulatory approaches among states. This effort includes an assessment of virtual currency activities and outreach with a broad range of stakeholders. After engaging with industry participants, state and federal regulators, and other stakeholders, CSBS recommended that activities involving third party control of virtual currency, including for the purposes of transmitting, exchanging, holding, or otherwise controlling virtual currency, should be subject to state licensure and supervision.

Recently amendments provide greater clarity and attempt to ensure continued innovation. These amendments address questions raised in the Assembly Banking and Finance Committee on April 27, 2015, and clarify the following:

1) Revise definition of "virtual currency" to remove ambiguous and redundant terms.

2) Revise definition of "virtual currency business" as having full custody and control of virtual currency on behalf of others.

3) Exempt from licensing a person or entity that develops, distributes virtual currency network software, provides computer power or provides data storage of cyber security services..

Previous Legislation.

AB 129 (Dickinson), Chapter 74, Statutes of 2014 clarified California law to ensure that alternative currency, including virtual currency would not be potentially deemed illegal tender.

Analysis Prepared by: Mark Farouk / B. & F. / (916) 319-3081 FN: 0000797

SENATE COMMITTEE ON
BANKING AND FINANCIAL INSTITUTIONS
Senator Marty Block, Chair
2015 - 2016 Regular

Bill No:	AB 1326	**Hearing Date:**	July 15, 2015
Author:	Dababneh		
Version:	July 6, 2015 Amended		
Urgency:	No	**Fiscal:**	Yes
Consultant:	Eileen Newhall		

Subject: Virtual currency.

SUMMARY Establishes a framework for the licensing and regulation of virtual currency businesses by the Department of Business Oversight (DBO), effective July 1, 2016.

DESCRIPTION

1. Provides that a licensee under the Money Transmission Act (MTA), who wishes to engage in a virtual currency business without a virtual currency license, must seek permission to do so from the Commissioner of Business Oversight (commissioner). Authorizes the commissioner to approve such requests, as specified, and clarifies that the commissioner may require a licensee granted such approval to increase its surety bond or amount of eligible securities above those required under the MTA, or impose any additional conditions on the authorization, as specified.

2. Authorizes a licensee in good standing under the virtual currency law to apply to the commissioner to convert its license into a MTA license, as specified.

3. Creates a new division under the Financial Code to regulate virtual currency businesses, effective July 1, 2016 (Division 11), as follows:

    a. Defines virtual currency as any type of digital unit that is used as a medium of exchange or a form of digitally stored value.

    b. Provides that virtual currency does not include any of the following:

        i. Digital units that are used solely within online gaming platforms, with no market or application outside of those gaming platforms.

        ii. Digital units that are used exclusively as part of a consumer affinity or rewards program.

        iii. Digital units that can be redeemed for goods, services, or for purchases with the issuer or other designated merchants, but cannot be converted into, or redeemed for fiat currency. Fiat currency is defined as government-issued currency that is designated as legal tender through government decree, regulation, or law, that customarily refers to paper

money and coin and is circulated, used, and accepted as money.

c. Defines virtual currency business as maintaining full custody or control of virtual currency in California on behalf of others.

d. Prohibits a person from engaging in any virtual currency business in California unless that person is licensed under Division 11 of the Financial Code or is exempt from licensure under that division.

   i. Establishes exemptions from licensure under the division for the United States or any federal department, agency, or instrumentality; state and local governments; depository institutions, as specified; licensed money transmitters; merchants or consumers that utilize virtual currency solely for the purchase or sale of goods or services; and transactions in which the recipient of virtual currency is an agent of the payee pursuant to a preexisting written contract, and delivery of the virtual currency to the agent satisfies the payor's obligation to the payee.

   ii. Authorizes the commissioner to approve additional exemptions, either partial or full, to persons, transactions, or both, by regulation or order, either unconditionally or upon specified terms and conditions, or for specified periods. Requires the commissioner to post on DBO's web site a list of all persons, transactions, or classes of persons or transactions exempted by the commissioner, and the provision or provisions of the division from which they are exempt.

e. Requires virtual currency business licensees to provide the following disclosure to consumers in a form and manner prescribed by the commissioner: "Once submitted to the network, a virtual currency transaction will be unconfirmed for a period of time (usually less than one hour, but up to one day or more) pending sufficient confirmation of the transaction by the network. A transaction is not complete while it is in a pending state. Virtual currency associated with transactions that are in a pending state will be designated accordingly, and will not be included in your account balance or be available to conduct transactions.

   "The risk of loss in trading or holding virtual currency can be substantial. You should therefore carefully consider whether trading or holding virtual currency is suitable for you in light of your financial condition. In considering whether to trade or hold virtual currency, you should be aware that the price or value of virtual currency can change rapidly, decrease, and potentially even fall to zero.

   "(insert company name) is licensed by the Department of Business Oversight to do business in California. If you have complaints with respect to any aspect of the virtual currency business conducted by (company name), you may contact the California Department of Business Oversight at its toll-free telephone number, 1-800-622-0620, by email at consumer.services@dbo.ca.gov, or by mail at the Department of Business Oversight, Consumer Services, 1515 K Street, Suite 200, Sacramento, CA

95814."

f. Requires licensees to provide receipts to consumers upon completion of virtual currency transactions. Receipts must include the name and contact information for the licensee; the type, value, date, and time of the transaction; the type and amount of any fees charged; the exchange rate, if applicable; a statement of the licensee's refund policy; and any additional information required by the commissioner. Receipts must be provided in English and in the language principally used by the licensee to advertise, solicit, or negotiate, if other than English.

g. Requires licensees to maintain levels of capital that the commissioner determines are sufficient to ensure the safety and soundness of the licensees, and to maintain consumer protection and their ongoing operations. Additionally requires licensees to maintain bonds or trust accounts in United States dollars for the benefit of their consumers, in forms and amounts specified by the commissioner.

h. Authorizes the commissioner to examine the business and branch office of each licensee, whether in California or outside the state, to ascertain whether the business is being conducted in a lawful manner and whether all virtual currency held or exchanged is properly accounted for. Provides the commissioner with broad authority to bring enforcement action against a licensee or a person required to be licensed, who does not hold such a license.

i. Requires each licensee to annually submit an audit report to the commissioner, prepared by an independent certified public accountant or independent public accountant, as specified. Additionally requires each licensee to submit specified financial statements to the commissioner on an annual basis, verified by two of the licensee's principal officers.

j. Authorizes the commissioner to levy fees and assessments on licensees sufficient to cover the commissioner's costs to administer the virtual currency law and provide a reasonable reserve for contingencies.

k. In lieu of many of the aforementioned requirements, authorizes a person or entity conducting virtual currency business with less than $1 million in outstanding obligations, whose business model represents no or low risk to consumers, as determined by the commissioner, to apply for and be granted a provisional virtual currency license. Grants the commissioner full discretion to prescribe the terms and conditions applicable to a provisional licensee and to suspend or revoke a provisional license, as specified. Provides that a provisional license is effective for two years and may be renewed by the commissioner. Requires a provisional licensee to notify the commissioner within 15 days after it surpasses the $1 million threshold and to apply for a virtual currency license within 30 days following that notice.

EXISTING LAW

1. Provides for the Money Transmission Act (MTA), administered by DBO (Division 1.2 of the Financial Code), which establishes a framework for the licensing and regulation of money transmitters, as specified (Financial Code Sections 2000 et seq.). The MTA defines money transmission as selling or issuing payment instruments, selling or issuing stored value, or receiving money for transmission (Financial Code Section 2003).

COMMENTS

1. Purpose: AB 1326 is intended to ensure that entities which store virtual currency or offer consumers the opportunity to exchange their virtual currency for fiat currency are operated in a safe and sound manner. It is also intended to provide regulatory certainty to companies who are engaging in or planning to engage in virtual currency businesses.

2. Background: Virtual currency, also called digital currency, has been defined by several different financial authorities. One of the most comprehensive definitions was developed by the European Banking Authority in 2014. In its Opinion on Virtual Currencies, issued July 4, 2014, the EBA defined virtual currency as "a digital representation of value that is neither issued by a central bank or a public authority, nor necessarily attached to a fiat currency, but is accepted by natural or legal persons as a means of payment and can be transferred, stored or traded electronically" (http://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf).

   Bitcoin is perhaps the most well-known among virtual currencies, but other virtual currencies exist, including Ripple, Stellar, Litecoin, Darkcoin, Peercoin, Primecoin, Dogecoin, and others. Increasing numbers of companies are offering services that support the use of virtual currencies (e.g., Coinbase, Circle, BitGo, Bitnet, Blockstream, Chain.com, Gem, Mirror, Xapo, and others). This bill establishes a regulatory framework intended to cover certain companies that offer services which support the use of virtual currencies; it does not purport to regulate the developers of existing or new virtual currencies.

3. Efforts by Other Regulators to Regulate Virtual Currency: Because of the increasing exposure of and interest in virtual currencies and their related businesses, federal and other state regulators have begun to issue guidance and enact rules in this area. In March, 2013, the federal Financial Crimes Enforcement Network (FinCEN) issued guidance to address the extent to which a person's conduct related to convertible virtual currency brings them within the Bank Secrecy Act's (BSA's) definition of a money transmitter and triggers a requirement to register with FinCEN as a money services business (MSB). Every MSB is required to have an anti money-laundering program in place and has the obligation to file a Suspicious Activity Report with FinCEN whenever a transaction they facilitate is "suspicious," as defined, and in an amount of $2,000 or more.

According to FinCEN, to the extent a user creates or "mines" a convertible virtual currency solely for a user's own purposes, the user is not a money transmitter under the BSA. Further, a company purchasing and selling convertible virtual currency as an investment exclusively for the company's benefit is also not a money transmitter. However, the administrator of a centralized repository of convertible virtual currency is a money transmitter to the extent that it allows transfers of value between persons or from one location to another. Additionally, any exchanger that uses its access to the convertible virtual currency services provided by the administrator to accept and transmit the convertible virtual currency on behalf of others, including transfers intended to pay a third party for virtual goods and services, is also a money transmitter.

The Conference of State Bank Supervisors, an association of state financial regulators, has also addressed the regulation of virtual currency. In December 2014, CSBS issued a draft model state regulatory framework for virtual currency activities (http://www.csbs.org/regulatory/ep/Documents/CSBS%20Draft%20Model%20Regulatory%20Framework%20for%20Virtual%20Currency%20Proposal%20--%20Dec.%2016%202014.pdf). The eight components in CSBS' draft framework include licensing requirements; a mechanism for states to share state licensing and enforcement data; financial strength and stability requirements; consumer protection; cybersecurity; compliance with BSA and anti-money laundering rules; recordkeeping and financial reporting; and regulatory supervision. Most of the eight components are addressed by AB 1326.

In June, 2015, New York became the first state in the country to finalize rules for virtual currency companies. New York defines virtual currency as "any type of digital unit that is used as a medium of exchange or a form of digitally stored value" and states that the term should be broadly construed to include digital units of exchange that have a centralized repository or administrator, are decentralized and have no centralized repository or administrator, or may be created or obtained by computing or manufacturing effort.

New York defines "virtual currency business activity" as the conduct of any one of the following types of activities involving New York or a New York resident: a) receiving virtual currency for transmission or transmitting virtual currency, except where the transaction is undertaken for non-financial purposes and does not involve the transfer of more than a nominal amount of virtual currency; b) storing, holding, or maintaining custody or control of virtual currency on behalf of others; c) buying and selling virtual currency as a customer business; d) performing exchange services as a customer business; or e) controlling, administering, or issuing a virtual currency. All entities that engage in virtual currency business activity and are not covered by an exemption from New York's virtual currency rules are required to obtain a BitLicense from the New York Department of Financial Services.

Because of the expansive definitions and limited exemptions contained in New York's rules, those rules have been criticized by many virtual currency businesses. Several virtual currency businesses contacted by Committee staff have indicated they will be forced to suspend business to customers based in New York, because

they cannot afford to operate under New York's regulatory regime.

AB 1326 is structured in ways that attempt to avoid some of the criticism virtual currency businesses have voiced about New York's rules. For example, New York requires virtual currency businesses to hold both BitLicenses and money transmission licenses. AB 1326 recognizes that some virtual currency businesses may not be engaged in activities which require an MTA license in California; for that reason, the bill does not require all virtual currency businesses to hold MTA licenses. Second, New York regulates network administrators, software providers, and exchange services, all of which are exempted from California's virtual currency law.

4. Regulation of An Emerging Industry: This bill and the other regulatory efforts summarized above illustrate a tension common to the regulation of emerging industries. Those who craft rules regulating emerging industries must balance the importance of protecting consumers against the risk of stunting the growth of a young industry through over-regulation. They must balance the importance of avoiding barriers to entry among startups against the danger of establishing an unlevel playing field among industry participants, which favors certain business models over others. Finally, they must balance industry participants' desire to minimize litigation risk through the establishment of clear rules of conduct against regulatory compliance costs.

   Many within the virtual currency industry want California to lead the nation in enacting a law which encourages innovation and allows startups to be established and grown without undue regulatory interference. They point to New York's rules as problematic for their industry and want California to enact an alternative regulatory framework to which other states can look when crafting their own laws. Others would prefer that California give the virtual currency industry more time to evolve before deciding whether to regulate it.

   AB 1326 attempts to provide balance the myriad competing interests cited above. However, the extent to which the bill will succeed in protecting consumers, without discouraging innovation among virtual currency businesses or creating an insurmountable barrier to entry among new applicants will only be known once the bill has been operative for a few years. If this bill is enacted, it will be important for the Legislature to track the progress of the regulatory regime the bill creates, and be willing to modify it as needed, to ensure that the correct balance is achieved.

5. Unresolved Issues: A variety of interested parties have expressed strong opinions regarding a variety of issues addressed by this bill. Two issues remain extremely contentious.

   First, there is no consensus to date regarding the way in which "virtual currency business" should be defined. At present, the bill defines virtual currency business as "maintaining full custody or control of virtual currency in California on behalf of others." While most industry participants believe that this bill's definition is vastly superior to the very broad definition used by New York, some have criticized this bill's definition as being too vague. For example, the term "full custody and control" can be a challenging concept to interpret when applied to a virtual currency

business that offers a virtual currency wallet which requires multiple parties to independently approve a withdrawal before it can be authorized. Some suggest that no single entity has full control over the wallet in this situation, because multiple parties must independently agree to a withdrawal before it can be made. Others counter that *all* of the entities in this situation have full control, because each can independently prevent a withdrawal by failing to authorize it. Clarification of this bill's definition of virtual currency business, either in statute or through regulation, will be critical if this bill becomes law.

Another issue of great importance to the regulated community, whose details remain the subject of controversy, is the availability and nature of a regulatory framework specifically directed toward start-ups. Colloquially, industry members argue that two programmers tinkering with code in a basement should not be regulated in the same manner as a multi-million dollar company with thousands of customers. To address this concern, the July 6th amendments added language authorizing the commissioner to award provisional licenses to small businesses determined by the commissioner to pose low or no risk to consumers. The July 6th amendments give the commissioner sole control to determine which rules will apply to each provisional license holder. The expectation is that businesses awarded provisional licenses will be able to operate under a less expensive and less restrictive regulatory scheme than larger or riskier businesses, although the details of the regulatory scheme(s) applicable to provisional licensees will be left to the commissioner to decide.

Although one might suspect that most industry participants would welcome the availability of a less costly, less restrictive license for certain start-ups, several small businesses reached out to the author's office and Committee staff, requesting an even less restrictive regulatory scheme than the one added to the bill on July 6th. These businesses would prefer registration to licensure and would prefer to substitute a set of best practices applicable to all registrants for the business-specific rules that AB 1326 authorizes the commissioner to apply.

6. Input from DBO: Numerous issues in AB 1326 would benefit from input by the regulator who will be responsible for administering the new law. However, as of the date this analysis was prepared, DBO was not authorized by the Governor's Office to offer official input regarding the bill. Informal conversations with DBO staff suggest that the Department expects to propose several amendments to the author, but the content and timing of those amendments are unknown at the present time. If this Committee chooses to pass AB 1326, it may wish to reserve its ability to call the measure back for a re-hearing, once the content of DBO's amendments is known and the status of the unresolved issues summarized above is clearer.

7. Summary of Arguments in Support:

   a. Coin Center is a nonprofit research and advocacy center focused on public policy issues affecting decentralized digital currencies, such as Bitcoin. The organization supports AB 1326, because the bill acknowledges that virtual currency businesses may have business models that do not involve money transmission and should not be required to hold money transmission licenses.

"Decentralized digital currencies, such as Bitcoin, are an exciting new innovation with a great many potential uses – from simple value transfer, to property title and copyright ownership recordation, identity management, and even the creation of self-executing contracts. Some uses of digital currency technology look exactly like money transmission, an activity that requires licensing in California as in almost every other state. However, many other possible uses of the technology have little or nothing to do with money transmission and pose little or no risk to consumers. A smart approach to regulating digital currency businesses would distinguish between these possible uses and only require licensing for those who engage in activities that are truly like traditional money transmission. AB 1326 – better than any other legislative proposal we have seen – accomplishes this. As a result, it preserves important consumer protections while not saddling cutting-edge innovation with unjustified regulatory burdens."

Coin Center believes that AB 1326's definition of a virtual currency business as one that maintains *full* custody or control of virtual currency on behalf of others makes a very important distinction. "The specific use of the words 'full custody' is very important because decentralized digital currency technology allows for divided control of assets. Such divided control for the first time makes possible financial services in which consumers do not give up control of their funds. By removing the need to completely trust a service provider, this innovation is a potential boon to cybersecurity and consumer protection."

Coin Center also believes that the exemptions from licensing contained in AB 1326 are well-crafted. "These exemptions, along with the bill's definition of 'virtual currency business,' if enacted, will provide the kind of regulatory clarity and certainty that will encourage investment in, and development of, these innovative technologies while at the same time ensuring that consumers have access to safe and reliable cutting-edge services."

b. Coinbase is the world's leading Bitcoin service provider; its mission is to make Bitcoin as easy as possible for the average person to understand and use. "We believe AB 1326 brings greater regulatory certainty for digital currency businesses, provides necessary protections for consumers, and creates a nurturing environment for small startups to build their businesses in the Golden State. Moreover, it eliminates a regulatory 'grey zone' that currently exists for our industry and gives businesses greater clarity. As a California based company, we are happy to see the state leading the nation in creating policy that will foster technological innovation and economic growth."

Coinbase is particularly supportive of the provisional licensing that AB 1326 would authorize. Provisional licensing "provides small digital currency startups or those with limited consumer exposure the ability to start and operate their businesses with an unencumbered runway. This section provides these businesses a low barrier to entry by means of registration, self-certified compliance with risk based performance standards, and a low fee. From there, they can focus on building and growing solutions for consumers and not worry about overly burdensome regulations and related expenses. While Coinbase would not be eligible for this licensing due to our

relative size, we strongly support the inclusion and believe it's extremely important to the overall health of the ecosystem. This provision will help seed the next round of the nation's most groundbreaking and innovative technologies companies, and make California one of the nation's most attractive places for digital currency businesses to grow and thrive."

c. The Electronic Transactions Association supports the bill, because it will "help create regulatory and legal certainty for digital currency companies in California and encourage them to call California home. By enacting this legislation, California would join a handful of states throughout the country, including North Carolina, Connecticut, New Jersey, and others which are also working on legislation to provide greater regulatory certainty for virtual currency businesses, important guardrails for consumers, and flexibility for financial innovators."

8. Summary of Arguments in Opposition:

a. The Electronic Frontier Foundation (EFF) opposes AB 1326 on the grounds that the bill is premature, technically inaccurate in spots, and will do more harm than good. "Virtual currencies are still developing, and this bill threatens to both stunt the growth of this innovative industry and hamper the enthusiasm driving consumer interest. Also, privacy and free speech are central issues in the virtual currency space, which the bill fails to adequately consider."

Among EFF's concerns: "AB 1326's definition of 'virtual currency business,' while much improved, remains both vague and overbroad. For instance, the question of who maintains 'full custody and control' of virtual currencies will likely prove to be complicated and will implicate multiple parties specified in a 'smart contract.' The vague language of the bill will leave those in the virtual currency space unclear about their obligations and may also deter those who are thinking about getting involved in the nascent industry."

"Although the bill attempts to exempt video game currencies from regulation, we believe it fails to do so. Any game currency that can be shared, traded, or gifted among users may result in market value outside the game, whether or not the company's terms allow for these transactions. Because the definition of 'virtual currency business' includes maintaining full custody of the currency, this bill could require any video game company that offers an in-game currency feature to submit to this regulatory scheme."

Finally, "the statutorily prescribed disclosure statement is wrong in its description of how Bitcoin works. For example, there is no fixed amount of time after which a transaction is 'confirmed;' six confirmation blocks (roughly one hour) is simply a popular choice. In addition, for many other virtual currencies (such as Stellar, Ripple, or Tendermint), the notion of confirmation time is completely different and transactions are confirmed within seconds. More generally, it is a mistake to mandate this kind of technical description given the large variety of possible technical designs."

b. The Copia Institute, a Silicon Valley-based think tank, writes, "Innovation only exists when those who have ideas can go out and try to execute them, quickly, with as few barriers as possible. Each hurdle weeds out more and more innovators before they have a chance to breathe the open air of the marketplace, and find out whether or not they've truly created something useful. So we should be concerned when governments create unnecessary 'permission' requirements without clear benefit...We should be exceptionally careful when implementing rules that have the potential to shape – or strangle – the very roots of innovation. New York, for instance, has already established BitLicense regulation, chilling Bitcoin innovation in the state that is the financial center of the world."

"At this stage of the game, creating licensing regimes and putting permission barriers on innovation is very, very premature. Everyone is still figuring out just what the blockchain is good for, and it's a long and varied list. Blockchain technology was crafted to solve a difficult currency problem, but it has enabled all sorts of powerful new apps and services that are often much more secure and useful than the alternatives...On top of that, because Bitcoin is programmable, many of the biggest concerns that regulators are expressing can be dealt with in the code itself. Rules can be built into the code without having to rely on a centralized bureaucracy."

"We should be very wary about deciding to put layers of government bureaucracy on things that can be accomplished in the code itself....Silicon Valley was built on permissionless innovation, especially on the internet. Saddling new core infrastructure like Bitcoin and the blockchain with a permission-based framework sets the wrong tone entirely, and virtually ensures that Silicon Valley won't be home to the leading innovators in this new and exciting space."

9. <u>Amendments:</u>

a. Although the licensing framework contained in AB 1326 is quite comprehensive, it does not include an annual reporting requirement, as is common among DBO licensees. An amendment is recommended to require licensees to submit information to DBO on an annual basis regarding their virtual currency activities, and to require DBO to annually summarize that information, along with information regarding the numbers and types of businesses to which licenses and provisional licenses have been issued and the types of enforcement actions brought by the commissioner against virtual currency licensees.

Page 18, between lines 32 and 33, insert: (d) Each licensee shall file an annual report with the commissioner, on or before the 15th day of March, giving the relevant information that the commissioner reasonably requires concerning the business and operations conducted by the licensee within the state during the preceding calendar year. Each licensee shall also make other special reports to the commissioner that may be required by the commissioner from time to time. The reports required by this subdivision shall be kept confidential pursuant to Chapter 3.5 (commencing with Section 6250)

of Division 7 of Title 1 of the Government Code and any regulations adopted thereunder.
(e) The commissioner shall annually prepare a report for publication on his or her internet Web site, summarizing consolidated information gained from the reports required pursuant to subdivision (d), documenting the number of regular and provisional licenses outstanding during the prior calendar year, and summarizing the numbers and types of enforcement actions brought by the commissioner pursuant to this division during the prior calendar year.

b. Language applicable to the provisional license requires amendment to clarify that the provisional license is *in lieu of* a regular license, define the term "outstanding obligations," and make other technical and clarifying changes.

Page 20, lines 30 through 38, amend as follows: (a) ***In lieu of Section 26006, a*** ~~A~~ person or entity conducting virtual currency business with less than one million dollars ($1,000,000) in outstanding obligations and whose business model, as determined by the commissioner, represents low or no risk to consumers, may ***pay an application fee of five hundred dollars ($500)*** ~~register with a five-hundred-dollar ($500) licensee fee~~ to the commissioner and, if approved, receive a provisional license to conduct virtual currency business. ***For purposes of this section, outstanding obligations mean value under the full custody and control of the person or entity.*** A person or entity that receives such a license shall also register with FinCEN as a money services business, if applicable.

Page 21, after "(c)", insert: Sections 26006, 26008, 26023, 26024, and 26031 shall not apply to a person or entity to which a provisional license has been issued.

Page 21, line 29, strike "audit" and insert: examine

Page 21, line 30, after "protection" strike "and enhance safety and soundness", and insert the following: , enhance safety and soundness, and gather information regarding the business and operations of provisional licensees. Reports concerning the business and operations of provisional licensees shall be kept confidential pursuant to Chapter 3.5 (commencing with Section 6250) of Division 7 of Title 1 of the Government Code and any regulations adopted thereunder. The commissioner shall include information about the business and operations of provisional licensees in the report required pursuant to subdivision (d) of Section 26023.

10. Prior and Related Legislation:

a. AB 129 (Dababneh), Chapter 74, Statues of 2014: Deleted the provision which prohibited any individual or entity from issuing or putting into circulation, as money, anything but the lawful money of the United States.

LIST OF REGISTERED SUPPORT/OPPOSITION

Support

Coinbase
Coin Center
Electronic Transactions Association

Opposition

Electronic Frontier Foundation
The Copia Institute

-- END --

SENATE COMMITTEE ON APPROPRIATIONS
Senator Ricardo Lara, Chair
2015 - 2016 Regular Session

AB 1326 (Dababneh) - Virtual currency

Version: August 18, 2015
Urgency: No
Hearing Date: August 24, 2015
Policy Vote: B. & F.I. 7 - 0
Mandate: No
Consultant: Jolie Onodera

This bill meets the criteria for referral to the Suspense File.

Bill Summary: AB 1326 would establish a framework for the licensing and regulation of virtual currency businesses, as defined, by the Department of Business Oversight (DBO), effective July 1, 2016.

Fiscal Impact: First-year and ongoing costs of $3.5 million (Special Fund*) to establish, manage, and enforce the licensing and regulatory regime, estimated to be offset in whole or in part by application renewal, and location fees as well as pro rata assessments to offset administrative costs. First-year costs are potentially not fully covered by licensing fees given the estimated number of applications, and could be borne by the General Fund. The DBO anticipates ongoing costs will be fully offset by the application, renewal, and location fees, as well as the pro rata assessment authority provided for in this measure.

*Financial Institutions Fund

Background: Existing law pursuant to the Money Transmission Act (MTA) prohibits a person from engaging in the business of money transmission in this state, or advertising, soliciting, or holding itself out as providing money transmission in this state, unless the person is licensed by the Commission of Business Oversight or exempt from licensure under the Act. (Financial Code §§ 2000-2176.)

As explained in the Senate Committee on Banking and Financial Institutions analysis dated July 15, 2015: "Virtual currency, also called digital currency, has been defined by several different financial authorities. One of the most comprehensive definitions was developed by the European Banking Authority (EBA) in 2014. In its *Opinion on Virtual Currencies*, issued July 4, 2014, the EBA defined virtual currency as a digital representation of value that is neither issued by a central bank or a public authority, nor necessarily attached to a fiat currency, but is accepted by natural or legal persons as a means of payment and can be transferred, stored or traded electronically."

Bitcoin is perhaps the most well-known among virtual currencies, but other virtual currencies exist, including Ripple, Stellar, Litecoin, Darkcoin, Peercoin, Primecoin, Dogecoin, and others. Increasing numbers of companies are offering services that support the use of virtual currencies (e.g., Coinbase, Circle, BitGo, Bitnet, Blockstream, Chain.com, Gem, Mirror, Xapo, and others). This bill establishes a regulatory framework intended to cover certain companies that offer services which support the use of virtual currencies; it does not purport to regulate the developers of existing or new virtual currencies.

Proposed Law: This bill would establish the Virtual Currency Act, a framework for the licensing and regulation of virtual currency businesses, as defined, by the DBO, effective July 1, 2016. In summary, this bill:

- Provides that a licensee under the MTA, who wishes to engage in a virtual currency business without a virtual currency license, must seek permission to do so from the Commissioner of Business Oversight (commissioner). Authorizes the commissioner to approve such requests, as specified, and clarifies that the commissioner may require a licensee granted such approval to increase its surety bond or amount of eligible securities above those required under the MTA, or impose any additional conditions on the authorization, as specified.
- Authorizes a licensee in good standing under the Virtual Currency Act to apply to the commissioner to convert its license into a MTA license, as specified.
- Creates a new division under the Financial Code to regulate virtual currency businesses, effective July 1, 2016, as follows:
    - Defines "virtual currency" as any type of digital unit that is used as a medium of exchange or a form of digitally stored value.
    - Provides that digital units used or redeemed for specified purposes are not considered virtual currency.
    - Defines "virtual currency business" as maintaining full custody or control of virtual currency in California on behalf of others.
- Prohibits a person from engaging in any virtual currency business in California unless that person is licensed or otherwise exempt under the bill's provisions.
- Establishes specified exemptions from licensure including any federal department or agency, state and local governments, depository institutions, and licensed money transmitters.
- Authorizes the commissioner to approve additional exemptions, as specified, and requires DBO to post on its website a list of all persons or transactions exempted by the commissioner, and the provisions from which they are exempt.
- Requires a non-refundable application fee for licensure of $5,000.
- Requires a non-refundable application fee of $3,500 for licensure and approval to acquire control of a licensee.
- Requires an annual licensure renewal fee of $2,500, and an additional $125 for each licensee branch office in this state.
- Requires licensees to pay $75 per hour for each DBO examiner engaged in an examination of a licensee, as specified.
- Authorizes the commissioner to examine the business and branch office of each licensee at any time and from time to time, to ascertain whether the business is being conducted in a lawful manner and whether all virtual currency held or exchanged is properly accounted for. Provides the commissioner with broad authority to bring enforcement action against a licensee or a person required to be licensed, who does not hold such a license.
- Authorizes the commissioner to assess a civil penalty for violations of the virtual currency law of up to $1,000 per violation, or in the case of a continuing violation, $1000 per day while the violation continues.
- Requires each licensee to annually submit an audit report to the commissioner, as specified.
- Requires each licensee to file an annual report with the commissioner, as specified, and requires the DBO to annually prepare a report consolidating the annual reports from licensees for publication on the DBO website.

- Authorizes the commissioner to levy fees and assessments on licensees sufficient to cover the commissioner's costs to administer the virtual currency law and provide a reasonable reserve for contingencies.
- In lieu of the $5,000 non-refundable application fee, authorizes a person or entity conducting virtual currency business with less than $1 million in outstanding obligations, as specified, to pay an application fee of $500 to apply for and be granted a provisional virtual currency license. Grants the commissioner full discretion to prescribe the terms and conditions applicable to a provisional licensee and to suspend or revoke a provisional license, as specified. Exempts a provisions licensee from various requirements of the Virtual Currency Act, and provides that a provisional license is effective for two years and may be renewed for a $500 renewal fee.
- Repeals Section 107 of the Corporations Code, which was enacted under AB 129 (2014), but was inadvertently chaptered out by the subsequent enactment of SB 1301 (2014).

Related Legislation: AB 129 (Dababneh) Chapter 74/2014 repealed Corporations Code § 107, which prohibited a corporation, flexible purpose corporation, association, or individual from issuing or placing into circulation, as money, anything other than the lawful money of the United States.

SB 1301 (DeSaulnier) Chapter 694/2014, among its provisions, renamed "flexible purpose corporations" as "social purpose corporations ," thereby chaptering out the provisions of AB 129.

Staff Comments: The DBO has indicated estimated first-year and ongoing costs of $3.5 million to fulfill the obligations associated with licensing and examining virtual currency businesses. This cost estimate includes 22 positions, including one Deputy Commissioner of Virtual Currency, three Financial Institutions Managers, eight Senior Financial Institutions Examiners, eight Financial Institutions Examiners, one Associate Government Program Analyst, and one staff services analyst, as well as the associated operating expenses for these positions.

It is anticipated that approximately 75 virtual currency companies will seek licensure with the Department, with 40 applications in the first year and 35 the next, with far fewer applicants in subsequent years. Initial workload of the DBO will focus on processing the applications of prospective licensees (typically a six-month process), followed by licensee examinations.

The DBO anticipates the cost of oversight of these companies will be fully offset by the application, renewal, and location fees, as well as the pro rata assessment authority (to offset costs of overseeing virtual currency licensees) provided by the bill.

-- END --

SENATE RULES COMMITTEE AB 1326
Office of Senate Floor Analyses
(916) 651-1520 Fax: (916) 327-4478

THIRD READING

Bill No: AB 1326
Author: Dababneh (D)
Amended: 8/18/15 in Senate
Vote: 21

SENATE BANKING & F.I. COMMITTEE: 7-0, 7/15/15
AYES: Block, Vidak, Galgiani, Hall, Hueso, Lara, Morrell

SENATE APPROPRIATIONS COMMITTEE: 6-1, 8/27/15
AYES: Lara, Bates, Beall, Hill, Leyva, Mendoza
NOES: Nielsen

ASSEMBLY FLOOR: 55-22, 6/3/15 - See last page for vote

SUBJECT: Virtual currency

SOURCE: Author

DIGEST: This bill establishes a framework for the licensing and regulation of virtual currency businesses by the Department of Business Oversight (DBO), effective July 1, 2016.

ANALYSIS: Existing law provides for the Money Transmission Act (MTA), administered by DBO (Division 1.2 of the Financial Code), which establishes a framework for the licensing and regulation of money transmitters, as specified (Financial Code Sections 2000 et seq.). The MTA defines money transmission as selling or issuing payment instruments, selling or issuing stored value, or receiving money for transmission (Financial Code Section 2003).

This bill:

1) Creates a new division under the Financial Code to regulate virtual currency businesses, effective July 1, 2016 (Division 11), as follows:

   a) Defines virtual currency as any type of digital unit that is used as a medium of exchange or a form of digitally stored value.

   b) Provides that virtual currency does not include any of the following:

      i) Digital units that are used solely within online gaming platforms, with no market or application outside of those gaming platforms.

      ii) Digital units that are used exclusively as part of a consumer affinity or rewards program.

      iii) Digital units that can be redeemed for goods, services, or for purchases with the issuer or other designated merchants, but cannot be converted into, or redeemed for fiat currency. Fiat currency is defined as government-issued currency that is designated as legal tender through government decree, regulation, or law, that customarily refers to paper money and coin and is circulated, used, and accepted as money.

   c) Defines virtual currency business as maintaining full custody or control of virtual currency in California on behalf of others.

   d) Prohibits a person from engaging in any virtual currency business in California unless that person is licensed under Division 11 of the Financial Code or is exempt from licensure under that division, as specified.

   e) Requires virtual currency business licensees to provide a specified disclosure to consumers informing them of the potential risks of virtual currency and instructing them on how to file complaints with DBO. Additionally requires licensees to provide receipts to consumers upon completion of virtual currency transactions, as specified.

   f) Requires licensees to maintain levels of capital that the Commissioner of DBO (commissioner) determines are sufficient to ensure the safety and soundness of the licensees, and to maintain consumer protection and their ongoing operations. Additionally requires licensees to maintain bonds or trust accounts in United States dollars for the benefit of their consumers, in

forms and amounts specified by the commissioner.

g) Authorizes the commissioner to examine the business and branch office of each licensee, whether in California or outside the state, to ascertain whether the business is being conducted in a lawful manner and whether all virtual currency held or exchanged is properly accounted for. Provides the commissioner with broad authority to bring enforcement action against a licensee or a person required to be licensed, who does not hold such a license.

h) Requires each licensee to submit an annual report regarding its business and operations, as specified, and to submit an annual audit report to the commissioner, prepared by an independent certified public accountant or independent public accountant, as specified.

i) Authorizes the commissioner to levy fees and assessments on licensees sufficient to cover the commissioner's costs to administer the virtual currency law and provide a reasonable reserve for contingencies.

j) Authorizes, in lieu of many of the aforementioned requirements, a person or entity conducting virtual currency business with less than $1 million in outstanding obligations, whose business model represents no or low risk to consumers, as determined by the commissioner, to apply for and be granted a provisional virtual currency license. Grants the commissioner full discretion to prescribe the terms and conditions applicable to a provisional licensee and to suspend or revoke a provisional license, as specified. Provides that a provisional license is effective for two years and may be renewed by the commissioner. Requires a provisional licensee to notify the commissioner within 15 days after it surpasses the $1 million threshold and to apply for a virtual currency license within 30 days following that notice.

2) Provides that an MTA licensee who wishes to engage in a virtual currency business without a virtual currency license must seek permission to do so from the commissioner. Authorizes the commissioner to approve such requests, as specified, and clarifies that the commissioner may require a licensee granted such approval to increase its surety bond or amount of eligible securities above those required under the MTA, or impose any additional conditions on the authorization, as specified.

3) Authorizes a licensee in good standing under the virtual currency law to apply to the commissioner to convert its license into a MTA license, as specified.

Background

Definition. Virtual currency, also called digital currency, has been defined by several different financial authorities. One of the most comprehensive definitions was developed by the European Banking Authority (EBA) in 2014. In its Opinion on Virtual Currencies, issued July 4, 2014, the EBA defined virtual currency as "a digital representation of value that is neither issued by a central bank or a public authority, nor necessarily attached to a fiat currency, but is accepted by natural or legal persons as a means of payment and can be transferred, stored or traded electronically" (http://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf).

Bitcoin is perhaps the most well-known among virtual currencies, but other virtual currencies exist, including Ripple, Stellar, Litecoin, Darkcoin, Peercoin, Primecoin, Dogecoin, and others. Increasing numbers of companies are offering services that support the use of virtual currencies (e.g., Coinbase, Circle, BitGo, Bitnet, Blockstream, Chain.com, Gem, Mirror, Xapo, and others). This bill establishes a regulatory framework intended to cover certain companies that offer services which support the use of virtual currencies; it does not purport to regulate the developers of existing or new virtual currencies.

Other state regulations. In June, 2015, New York became the first state in the country to finalize rules for virtual currency companies. New York defines virtual currency as "any type of digital unit that is used as a medium of exchange or a form of digitally stored value" and states that the term should be broadly construed to include digital units of exchange that have a centralized repository or administrator, are decentralized and have no centralized repository or administrator, or may be created or obtained by computing or manufacturing effort.

New York defines "virtual currency business activity" as the conduct of any one of the following types of activities involving New York or a New York resident: 1) receiving virtual currency for transmission or transmitting virtual currency, except where the transaction is undertaken for non-financial purposes and does not involve the transfer of more than a nominal amount of virtual currency; 2) storing, holding, or maintaining custody or control of virtual currency on behalf of others; 3) buying and selling virtual currency as a customer business; 4) performing exchange services as a customer business; or 5) controlling, administering, or

issuing a virtual currency. All entities that engage in virtual currency business activity and are not covered by an exemption from New York's virtual currency rules are required to obtain a BitLicense from the New York Department of Financial Services.

Because of the expansive definitions and limited exemptions contained in New York's rules, those rules have been criticized by many virtual currency businesses. Several virtual currency businesses have indicated they will be forced to suspend business to customers based in New York, because they cannot afford to operate under New York's regulatory regime.

Comments

Regulation of an emerging industry. AB 1326 is intended to ensure that entities which store virtual currency or offer consumers the opportunity to exchange their virtual currency for fiat currency are operated in a safe and sound manner. It is also intended to provide regulatory certainty to companies who are engaging in or planning to engage in virtual currency businesses.

Many within the virtual currency industry want California to lead the nation in enacting a law which encourages innovation and allows startups to be established and grown without undue regulatory interference. They point to New York's rules as problematic for their industry and want California to enact an alternative regulatory framework to which other states can look when crafting their own laws. Others would prefer that California give the virtual currency industry more time to evolve before deciding whether to regulate it.

Unresolved issues. A variety of interested parties have expressed strong opinions regarding a variety of issues addressed by this bill. Two issues remain extremely contentious.

First, there is no consensus to date regarding the way in which "virtual currency business" should be defined. At present, this bill defines virtual currency business as "maintaining full custody or control of virtual currency in California on behalf of others." While most industry participants believe that this bill's definition is vastly superior to the very broad definition used by New York, some have criticized this bill's definition as being too vague. For example, the term "full custody and control" can be a challenging concept to interpret when applied to a virtual currency business that offers a virtual currency wallet which requires multiple parties to independently approve a withdrawal before it can be authorized.

Some suggest that no single entity has full control over the wallet in this situation, because multiple parties must independently agree to a withdrawal before it can be made. Others counter that *all* of the entities in this situation have full control, because each can independently prevent a withdrawal by failing to authorize it. Clarification of this bill's definition of virtual currency business, either in statute or through regulation, will be critical if this bill becomes law.

Another issue of great importance to the regulated community, whose details remain the subject of controversy, is the availability and nature of a regulatory framework specifically directed toward start-ups. Colloquially, industry members argue that two programmers tinkering with code in a basement should not be regulated in the same manner as a multi-million dollar company with thousands of customers. To address this concern, the July 6th amendments added language authorizing the commissioner to award provisional licenses to small businesses determined by the commissioner to pose low or no risk to consumers. The July 6th amendments give the commissioner sole control to determine which rules will apply to each provisional license holder. The expectation is that businesses awarded provisional licenses will be able to operate under a less expensive and less restrictive regulatory scheme than larger or riskier businesses, although the details of the regulatory scheme(s) applicable to provisional licensees will be left to the commissioner to decide.

Although one might suspect that most industry participants would welcome the availability of a less costly, less restrictive license for certain start-ups, several small businesses reached out to the author's office, requesting an even less restrictive regulatory scheme than the one added to this bill on July 6th. These businesses would prefer registration to licensure and would prefer to substitute a set of best practices applicable to all registrants for the business-specific rules that AB 1326 authorizes the commissioner to apply.

FISCAL EFFECT: Appropriation: No Fiscal Com.: Yes Local: No

According to the Senate Appropriations Committee, first-year and ongoing costs of $3.5 million (Special Fund*) to establish, manage, and enforce the licensing and regulatory regime, estimated to be offset in whole or in part by application renewal, and location fees as well as pro rata assessments to offset administrative costs. First-year costs are potentially not fully covered by licensing fees given the estimated number of applications, and could be borne by the General Fund. The DBO anticipates ongoing costs will be fully offset by the application, renewal, and

location fees, as well as the pro rata assessment authority provided for in this measure.

*Financial Institutions Fund

SUPPORT: (Verified 8/27/15)

Coinbase
Coin Center
Electronic Transactions Association

OPPOSITION: (Verified 8/27/15)

Electronic Frontier Foundation
The Copia Institute

ARGUMENTS IN SUPPORT: Coin Center is a nonprofit research and advocacy center focused on public policy issues affecting decentralized digital currencies, such as Bitcoin. The organization supports AB 1326, because this bill acknowledges that virtual currency businesses may have business models that do not involve money transmission and should not be required to hold money transmission licenses. "Decentralized digital currencies, such as Bitcoin, are an exciting new innovation with a great many potential uses – from simple value transfer, to property title and copyright ownership recordation, identity management, and even the creation of self-executing contracts. Some uses of digital currency technology look exactly like money transmission, an activity that requires licensing in California as in almost every other state. However, many other possible uses of the technology have little or nothing to do with money transmission and pose little or no risk to consumers. A smart approach to regulating digital currency businesses would distinguish between these possible uses and only require licensing for those who engage in activities that are truly like traditional money transmission. AB 1326 – better than any other legislative proposal we have seen – accomplishes this. As a result, it preserves important consumer protections while not saddling cutting-edge innovation with unjustified regulatory burdens."

Coinbase is the world's leading Bitcoin service provider. "We believe AB 1326 brings greater regulatory certainty for digital currency businesses, provides necessary protections for consumers, and creates a nurturing environment for small startups to build their businesses in the Golden State. Moreover, it eliminates a regulatory 'grey zone' that currently exists for our industry and gives businesses greater clarity. As a California based company, we are happy to see the state

leading the nation in creating policy that will foster technological innovation and economic growth."

Coinbase is particularly supportive of the provisional licensing that AB 1326 authorizes. Provisional licensing "provides small digital currency startups or those with limited consumer exposure the ability to start and operate their businesses with an unencumbered runway. This section provides these businesses a low barrier to entry by means of registration, self-certified compliance with risk based performance standards, and a low fee. From there, they can focus on building and growing solutions for consumers and not worry about overly burdensome regulations and related expenses. While Coinbase would not be eligible for this licensing due to our relative size, we strongly support the inclusion and believe it's extremely important to the overall health of the ecosystem. This provision will help seed the next round of the nation's most groundbreaking and innovative technologies companies, and make California one of the nation's most attractive places for digital currency businesses to grow and thrive."

ARGUMENTS IN OPPOSITION: The Copia Institute, a Silicon Valley-based think tank, writes, "At this stage of the game, creating licensing regimes and putting permission barriers on innovation is very, very premature. Everyone is still figuring out just what the blockchain is good for, and it's a long and varied list... We should be very wary about deciding to put layers of government bureaucracy on things that can be accomplished in the code itself....Silicon Valley was built on permissionless innovation, especially on the internet. Saddling new core infrastructure like Bitcoin and the blockchain with a permission-based framework sets the wrong tone entirely, and virtually ensures that Silicon Valley won't be home to the leading innovators in this new and exciting space."

The Electronic Frontier Foundation opposes AB 1326 on the grounds that this bill is premature, technically inaccurate in spots, and will do more harm than good. "Virtual currencies are still developing, and this bill threatens to both stunt the growth of this innovative industry and hamper the enthusiasm driving consumer interest. Also, privacy and free speech are central issues in the virtual currency space, which the bill fails to adequately consider."

ASSEMBLY FLOOR: 55-22, 6/3/15
AYES: Alejo, Bloom, Bonilla, Bonta, Brown, Burke, Calderon, Campos, Chau, Chiu, Chu, Cooley, Cooper, Dababneh, Daly, Dodd, Eggman, Frazier, Cristina Garcia, Eduardo Garcia, Gatto, Gipson, Gomez, Gonzalez, Gordon, Gray, Roger Hernández, Holden, Irwin, Jones-Sawyer, Lackey, Levine, Linder, Lopez, Low,

Mathis, McCarty, Medina, Mullin, Nazarian, O'Donnell, Perea, Quirk, Rendon, Ridley-Thomas, Rodriguez, Salas, Santiago, Mark Stone, Ting, Weber, Wilk, Williams, Wood, Atkins

NOES: Achadjian, Baker, Bigelow, Brough, Chang, Chávez, Dahle, Beth Gaines, Gallagher, Grove, Hadley, Harper, Jones, Kim, Maienschein, Mayes, Melendez, Obernolte, Olsen, Patterson, Steinorth, Wagner

NO VOTE RECORDED: Travis Allen, Thurmond, Waldron

Prepared by: Eileen Newhall / B. & F.I. / (916) 651-4102
8/30/15 19:27:49

****** END ******

Date of Hearing: May 13, 2015

ASSEMBLY COMMITTEE ON APPROPRIATIONS
Jimmy Gomez, Chair
AB 1326 (Dababneh) – As Amended April 20, 2015

Policy Committee: Banking and Finance Vote: 8 - 2

Urgency: No State Mandated Local Program: Yes Reimbursable: No

SUMMARY:

This bill creates a licensing and regulatory regime for entities engaged in the business of virtual or digital currency with the Department of Business Oversight (DBO). In summary, this bill:

1) Broadly defines "virtual currency" to include any digital unit used as a medium of exchange or a form of digitally stored value, or is incorporated into payment system technology, whether traded through a centralized administrator or fully decentralized. The bill exempts virtual currencies used exclusively within online gaming platforms or customer rewards programs that cannot be redeemed or converted into fiat currency.

2) Defines "virtual currency business" as storing, holding, maintaining custody, or controlling virtual currency on behalf of others, or providing version or exchange services into other currency, whether fiat or virtual, or other value. The bill exempts federal, state, and municipal government entities; certain state, federal, and foreign banks and credit unions; licensed money transmitters; and merchants and consumers in the ordinary course of purchases and sales of goods and services, and their agents.

3) Requires an applicant to pay the Commissioner of DBO (Commissioner) the following nonrefundable fees: $5,000 initial application fee; $3,500 application fee for licensure and approval to acquire control of a licensee; $2,500 annual renewal license fee; and $125 annual license fee for each branch office.

4) Allows the Commissioner to levy assessments each fiscal year, on a pro rata basis, against licensees in an amount sufficient to meet the Commissioner's expenses in administering this section and provide a reasonable reserve for contingencies.

5) Authorizes the Commissioner to establish capital requirements for licensees; requires licensees to exercise reasonable oversight of its agents, keep records of agent reviews, and include contractual compliance requirements for any authorized agents.

6) Requires licensees to file annual audit reports with the Commissioner within 90 days of the end of each fiscal year, and quarterly financial statements, verified by 2 principal officers, within 45 days of the end of each fiscal quarter.

7) Authorizes the Commissioner to examine the business and any branch office of any licensee to ascertain compliance, requires licensees to furnish to the Commissioner, upon request, any or all accounts, books, and other records; and requires licensees to maintain any records as required by the Commissioner for a minimum of 3 years.

8) Requires licensees to report to the Commissioner within 5 days: any bankruptcy petition or other proceeding for insolvency, dissolution, or reorganization; any proceeding to revoke or suspend its virtual currency business license in another jurisdiction; any cancellation or impairment of bond or trust accounts; or any felony charges against a director or executive.

9) Authorizes the Commissioner to issue formal and informal guidance on compliance with the licensing regime, and make that advice publicly accessible online.

10) Provides the Commissioner with broad authority to issue orders and enforce virtual currency rules against licensees and nonlicensees, including revocation of licenses under specified circumstances and assessing civil penalties against violators; and creates felonies for certain unlicensed activities and intentional misrepresentation of activities.

11) Requires licensees to make certain disclosures to consumers; establishes regulatory rule-making authority with the Commissioner to implement the requirements of the licensing regime.

FISCAL EFFECT:

Estimated annual GF administrative costs to DBO of approximately $3.3 million to establish, manage, and enforce the licensing regime, eventually offset by application, renewal, and location fees as well as pro rata assessments to offset administrative costs.

COMMENTS:

1) **Purpose.** According to the author, this bill is designed to ensure entities that manage virtual currency or offer virtual currency exchange are operated in a sound manner and protect consumers' virtual currency from potential loss. This bill also provides regulatory certainty for virtual currency businesses, especially those that have applied for money transmission licenses or remain unsure where their business model fits into existing regulatory regimes.

2) **Bitcoin, Briefly.** The best known virtual currency is Bitcoin, though it is neither the first nor the only example. Bitcoins is a decentralized, digital currency that allows users to transact directly, without an intermediary. Transactions are encrypted to preserve integrity and pseudonymous, and all transactions are recorded and verified in a public ledger known as the block chain. The block chain and its integrity are maintained by thousands of independent users known as miners, who offer computational power to verify and record transactions. Miners are rewarded for this effort with newly-created bitcoins. This core system has proven robust during its six years of operation, with no successful hacking attempts to date.

   A number of companies offer bitcoin management and credential storage applications for consumers, merchants, and traders, the most consumer-facing of which are known as digital or bitcoin wallets. Digital wallets hold the cryptographic key credentials needed to transact in bitcoins, and are essential intermediaries in any bitcoin transaction. Bitcoin managers may also offer currency exchange services with a number of different fiat currencies. A number of high-profile attacks on bitcoin intermediaries have recently drawn the attention of regulators with respect to the overall security of transacting in digital currencies. While these attacks have not compromised the integrity of the bitcoin system itself, they have resulted in a number of bitcoin thefts (accomplished by accessing the cryptographic keys) and disruptions to intermediary activity.

3) **Other Regulation Efforts.** Following the first issue of regulations by the New York State Department of Banking on virtual currencies, the Conference of State Banking Supervisors formed a task force to examine state regulation of payment systems and seek consistent regulation among states for certain areas. The task force engaged with a number of industry participants, state and federal regulators, and other stakeholders, and recommended that activities involving third party control of virtual currency, including transmitting, exchanging, holding, or otherwise controlling virtual currency, should be subject to state licensure and supervision. Some industry participants believe AB 1326 could serve as a model for regulation in other states.

   The US Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) also issued interpretive guidance on the application of the federal Bank Secrecy Act to users, administrators, and exchangers of virtual currencies. As part of the guidance, FinCEN concluded virtual currencies do not have legal tender status in any jurisdiction, and are not "real currencies" for purposes of the Act, meaning that pure exchangers of virtual currency for fiat currency are not subject to foreign exchange dealer regulations. However, the FinCEN guidance did clarify that businesses engaged in accepting and transmitting virtual currency and/or buying and selling virtual currency may be "money transmitters" under current regulations, and subject to the reporting and recordkeeping rules that apply to money services businesses.

4) **Of Silk and Coin.** The Silk Road case drew international attention to bitcoin and its potential to facilitate illicit activity. Silk Road was an online black market for trading in illegal drugs that utilized the anonymizing software Tor in conjunction with bitcoin to facilitate anonymous sales and purchases. Bitcoin transactions are pseudonymous in that transactions are not recorded by name. Transactions are recorded in a distributed, public ledger, however, and can be traced to individuals and computers, unlike traditional cash. Use of anonymizing software, which disguises the identity of a computer and/or user, allows a person to transact with effective anonymity.

   It is the combination of Tor and bitcoin that made Silk Road possible. Cash remains a far more common means of transacting in illicit activity than digital or virtual currencies. As noted above, standard bitcoin transactions can ultimately be traced to individuals and computers, and bitcoin's protection against duplication arguably makes it more stable than traditional cash. However, certain intermediaries that manage and facilitate digital currency transactions may have significant vulnerabilities, and this bill is intended to form a regulatory framework to mitigate those problems.

Analysis Prepared by: Joel Tashjian / APPR. / (916) 319-2081