I. Introduction .............................................................................................................................................. 2

II. Background ............................................................................................................................................... 2
   A. Bitcoin Developments ........................................................................................................................... 2
   B. Early Regulatory and Law Enforcement Problems .................................................................................. 4
      1. Silk Road .................................................................................................................................................. 4
      2. Mount Gox ................................................................................................................................................ 5

III. U.S. Regulatory Initiatives .......................................................................................................................... 6
   A. The Financial Crime Enforcement Network ............................................................................................. 6
      1. Virtual Currency Guidance ...................................................................................................................... 6
      2. Ripple Labs Consent Decree .................................................................................................................... 8
   B. New York Department of Financial Services – Creating a BitLicense and Trust Company
      Digital Currency Exchange Charter ............................................................................................................ 9
   C. The Office of the Comptroller of the Currency – The Fintech Charter .................................................. 12
   D. The Regulation of Virtual Currency Business Act .................................................................................. 16

IV. International Regulatory Developments ..................................................................................................... 18
   A. The European Union: The European Bank Authority ............................................................................. 18
   B. The United Kingdom ................................................................................................................................. 20
   C. The Basel Committee on Banking Supervision ...................................................................................... 22
   D. China .......................................................................................................................................................... 23
   E. Japan .......................................................................................................................................................... 24
      1. Funds Settlement Law .............................................................................................................................. 24
      3. Anti-money Laundering Regulation: Act on the Prevention of Transfer of Criminal
         Proceeds (the “AMLA”) .......................................................................................................................... 26

V. Conclusion ..................................................................................................................................................... 26
I. Introduction

In the context of a widely publicized explosion of new technology and innovation designed to disrupt the marketplace of traditional financial institutions in delivering financial services, the number of financial technology ("fintech") companies in the U.S. and U.K. alone has grown in recent years to more than 4,000, and investment in this sector has grown from $1.8 billion to $24 billion worldwide in just the last five years.\(^1\) The financial services industry is experiencing rapid technological changes as it seeks to meet and anticipate business opportunities and needs, consumer demands and expectations, and demographic trends. In particular, the advent of virtual currencies, beginning with Bitcoin in 2008, has quickly exploded into an emerging financial ecosystem composed of non-government based legal tender, showing exciting possibilities for peer-to-peer payment systems, money transmission, mobile payment systems, and investment opportunities, for not only purchasers and sellers of virtual currencies, but also investors in virtual currency business activity, and perhaps more significantly, consumers. As such, virtual currency presents potential business opportunities for both innovative fintech companies and technologies emerging in this new financial ecosystem, as well as the banking and financial services industry.

However, the advent of virtual currencies has also brought significant concerns about potential illegal and fraudulent activities related to these currencies that have forced the attention of governments, regulators, and law enforcement authorities worldwide to focus on the implications of these currencies. This focus has been dominated by concerns about, among other things, virtual currency use in illegal activities such as narcotics trafficking, terrorism and money laundering activities, customer theft and data breaches, to even the existential threats posed by virtual currency in relation to government backed fiat currencies and the global economy.

In this light, the growing legal and regulatory challenges seem clear: balancing an approach that fosters responsible development of an innovative technology with potentially significant benefits with the need for an effective legal and regulatory framework that protects consumers, businesses, and the financial system.

This article will discuss and analyze the background of virtual currency – primarily Bitcoin’s development – law enforcement and regulatory problems that have arisen in connection with virtual currency business activities, and the government responses in addressing the legal regulatory framework and challenges related to virtual currencies, both in the U.S. and in countries with major financial services industries.

II. Background

A. Bitcoin Developments

Overview of Bitcoin

In 2008, Satoshi Nakamoto — the mysterious creator of bitcoin — triggered a potential revolution in global currencies, payment systems, financial services, and fintech business and regulation by publishing an eight-page paper entitled Bitcoin: A Peer-to-Peer Electronic Cash System.\(^2\) This paper offered a clear enough

---

1 See Remarks by Thomas J. Curry, Comptroller of the Currency, Regarding Special Purpose National Bank Charters for Fintech Companies, Georgetown University Law Center (December 2, 2016) and Section III.C. and accompanying footnotes, infra.

2 Nakamoto, Satoshi, Bitcoin: A Peer-to-Peer Electronic Cash System (October 31, 2008). Much controversy and discussion has surrounded the true identity of Satoshi Nakamoto, and to date, no one has come forward to claim that they are Nakamoto. See, e.g., Who is Satoshi Nakamoto?, Coindesk.com (Last updated February 19, 2016). While this article focuses primarily on legal and regulatory issues associated with bitcoin as the first virtual currency, there has been an explosion of virtual currencies in recent years, including but not limited to ether, litecoin, peercoin, freecoin, ripple and linden dollar, dogecoin, primecoin, darkcoin, primecoin, and others. See Bajpai, Prableen, The Five Most Important Virtual Currencies Other Than Bitcoin, Investopedia (December 10, 2014); Cohen; Reuren, The Top 30 Crypto-Currency Market Capitalizations In One Place, Forbes (November 27, 2013).
thesis; proposing a “purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution.”

The first bitcoin was created in 2009 after Nakamoto released the Bitcoin Network source code (the software and protocol that created and launched the Bitcoin Network). Since its introduction, the Bitcoin Network has been under active development by a group of contributors currently headed by Wladimir J. van der Laan, who was appointed project maintainer by Satoshi Nakamoto in 2010. As an “open source” project, Bitcoin is not represented by an official organization or authority.

While technically complex from a technology perspective, bitcoin is essentially a digital asset that is issued by, and transmitted through, the decentralized, open source protocol of the peer-to-peer Bitcoin. The Bitcoin Network hosts the decentralized public transaction ledger, known as the Blockchain, on which all bitcoin is recorded. No single entity owns or operates the Bitcoin Network, the infrastructure of which is collectively maintained by a decentralized user base. Bitcoin can be used to pay for goods and services or can be converted to flat currencies, such as the U.S. dollar, at rates determined on Bitcoin Exchanges or in individual end-user-to-end-user transactions under a barter system.

Bitcoin is “stored” or reflected on the digital transaction ledger known as the “Blockchain,” which is a digital file stored in a decentralized manner on the computers of each Bitcoin Network user. The Bitcoin Network software source code includes the protocols that govern the creation of bitcoin and the cryptographic system that secures and verifies Bitcoin transactions. The Blockchain is a canonical record of every bitcoin, every Bitcoin transaction (including the creation or “mining” of new bitcoin), and every Bitcoin address associated with a quantity of bitcoin. The Bitcoin Network and Bitcoin Network software programs can interpret the Blockchain to determine the exact bitcoin balance, if any, of any public Bitcoin address listed in the Blockchain as having taken part in a transaction on the Bitcoin Network. The Bitcoin Network utilizes the Blockchain to evidence the existence of bitcoin in any public Bitcoin address. A Bitcoin private key controls the transfer or “spending” of bitcoin from its associated public Bitcoin address. A Bitcoin wallet is a collection of private keys and their associated public Bitcoin addresses.

The Blockchain is comprised of a digital file, downloaded and stored, in whole or in part, on all Bitcoin Network users’ software programs. The file includes all blocks that have been solved by miners and is updated to include new blocks as they are solved. As each newly solved block refers back to and “connects” with the immediately prior solved block, the addition of a new block adds to the Blockchain in a manner similar to a new link being added to a chain. Each new block records outstanding Bitcoin transactions, and outstanding transactions are settled and validated through such recording; the Blockchain represents a complete, transparent, and unbroken history of all transactions of the Bitcoin Network. Each Bitcoin transaction is a broadcast to the Bitcoin Network and recorded in the Blockchain.

The Bitcoin Network is decentralized and does not rely on either governmental authorities or financial institutions to create, transmit, or determine the value of bitcoin. Rather, bitcoin is created and allocated by the Bitcoin Network protocol through a “mining” process subject to a strict, well-known issuance schedule. The value of bitcoin is determined by the supply of and demand for bitcoin, as well as the number of merchants that accept them.

---

3 Id. at 1.
4 For an in-depth discussion of bitcoin, see U.S. Securities and Exchange Commission Amendment No. 6 to Form S-1. Winklevoss Bitcoin Trust, Registration No. 333-189752, filed June 29, 2016 at pp. 32-60. (Proposed bitcoin exchange traded fund). Most of the bitcoin description in this section is attributed to disclosure in this SEC filing.
B. Early Regulatory and Law Enforcement Problems

1. Silk Road

Silk Road was an online black market, and the first “dark net market” best known as a platform for selling illegal drugs and other illicit goods and services purchased with bitcoin. As such, Silk Road placed an unfavorable spotlight on both the “dark net” or “dark web” — hidden or so-called overlay networks that can only be accessed with specific software or authorizations, usually through either peer-to-peer file sharing networks, or privacy networks such as Tor, and perhaps more significantly, the ability to anonymously use bitcoin for illegal transactions — particularly since Silk Road, in fact, accepted only bitcoin.

Silk Road, founded in February 2011 by Ross Ulbricht, quickly began to gain public notoriety and internet buzz, including scrutiny from a U.S. Senator, who publicly asked U.S. law enforcement authorities, including the U.S. Department of Justice and Drug Enforcement Administration, to shut it down. Its notoriety was further exacerbated by the fact that its founder went by the swashbuckling pseudonym “Dread Pirate Roberts,” espousing a libertarian goal for Silk Road posted at its website “[t]o grow into a force to be reckoned with that can challenge the powers that be and at last give people the option to choose freedom over tyranny.” By 2013 it had nearly one million account users, facilitating over a 2.5 year period 1.2 million transactions worth 9.5 million bitcoins — or about $1.2 billion in total money exchanged.

After a lengthy government investigation by a host of U.S. federal agencies and other governments, in October 2013, the Federal Bureau of Investigation shut down the website and arrested Ross Ulbricht, prosecuting him for omnibus violations of federal drug and anti-money laundering laws and ordering him to pay restitution of $683 million transactions worth 9.5 million bitcoins — or about $1.2 billion in total money exchanged.

---


6 See generally Wood, Jessica, The Darknet: A Digital Copyright Revolution, 16 Rich. J.L. and Tech. 16 (2010);

7 Miller, Fessa, How Can I Stay Anonymous with Tor?, Life Hacker (January 10, 2014); Torpay, Kyle, BlockChain Info Launches Tor Hidden Service, Inside BitCoins (December 2, 2011).

8 See, e.g., Eha, Brain Patrick, Could the Silk Road Closure Be Good for Bitcoin?, New Yorker (October 25, 2013); Gayathri, Amrutha, From marijuana to LSD, now illegal drugs delivered on your doorstep, International Business Times (June 11, 2011); Chen, Aarian, The Underground Website Where You Can Buy Any Drug Imaginable, Gawker (June 15, 2011).


10 The name “Dread Pirate Roberts” was apparently taken from a character in the 1987 movie The Princess Bride, who was feared for his ruthlessness and sword fighting prowess, and well known for taking no prisoners.

11 Anderson, Nate and Foriva, Cyrus, How the Feds took down the Dread Pirate Roberts, Ars Technica (October 10, 2013).

12 Id.

13 In announcing indictments of parties related to the Silk Road website, it is interesting to note that the U.S. Attorney prosecuting the case made the following statement of thanks in his press release:

Mr. Bharara praised the outstanding investigative work of the FBI and its New York Special Operations and Cyber Division, as well as the outstanding investigative work of the DEA’s New York Organized Crime Drug Enforcement Strike Force, which comprises agents and officers of the DEA, the IRS, the New York City Police Department, U.S. Immigration and Customs Enforcement’s (“ICE”) Homeland Security Investigations (“HSI”), the New York State Police, the Bureau of Alcohol, Tobacco, Firearms and Explosives, the U.S. Secret Service, the U.S. Marshals Service, Office of Foreign Assets Control, and NY Department of Taxation. Mr. Bharara also thanked the ICE-HIS Chicago-O’Hare office for its assistance and support, as well as the Department of Justice’s Computer Crime and Intellectual Property Section and Office of International Affairs. Additionally, Mr. Bharara praised the foreign law enforcement partners whose contributions to the success of the investigation and prosecution have been invaluable, namely, the Australian Federal Police, the Irish Republic’s Computer Crime Investigation Unit of the An Garda Siochana, the Reykjavik Metropolitan Police of the Republic of Iceland, and the French Republic’s Central Office for the Fight Against Crime Linked to Information Technology and Communication.

See Press Release, Manhattan U.S. Attorney Announces Charges Against Three Individuals in Virginia, Ireland and Australia for Their Roles in Running the “Silk Road Website, U.S. Attorney, S.D.N.Y. (December 20, 2013). (Silk Road Indictment).
million, representing all sales of illegal items on Silk Road.\textsuperscript{14} He was convicted on numerous other charges, including illegal drug sales, and was sentenced to life in prison without the possibility of parole.\textsuperscript{15} Subsequently, others associated with the website were also prosecuted.\textsuperscript{16} In connection with these prosecutions, the government seized almost $30 million in bitcoins, which it subsequently sold in auction transactions.\textsuperscript{17}

2. \textbf{Mount Gox}

The Mount Gox website, Mtgox.com, was originally registered in 2007 by Jed McCaleb, an American entrepreneur, as a domain name for the purpose of turning it into a trading site for game cards of a popular online game, Magic: The Gathering. The site was live for only a few months, but McCaleb never followed through.\textsuperscript{18} However, in late 2010, he decided to repurpose the domain as one of the first exchanges for the purchase and sale of Bitcoin.\textsuperscript{19} After realizing the time and attention required to run the site, he sold it, while apparently retaining a 12 percent interest, to Mark Karpeles, who, after revising the site's backend software, turned it into the world's most popular Bitcoin exchange, headquartered in Tokyo.\textsuperscript{20} Notwithstanding a security breach due to hacking in June 2011 that forced the site offline for several days—in the context of other emerging Bitcoin exchanges that had been hacked, lost customer funds, and simply folded—by 2013, Mt. Gox became a preeminent Bitcoin trading exchange.\textsuperscript{21} During 2013, Bitcoin prices took off, climbing from $13 to more than $1,200 at their peak. By April 2013, at about the same time the Silk Road situation was attracting government scrutiny and press attention, Mt. Gox had grown to handle 70 percent of the world's Bitcoin trades,\textsuperscript{22} and Mt. Gox suspended trading on April 11-12 for a "market cool-down."\textsuperscript{23}

In May 2013, CoinLab filed a $75 million lawsuit against Mt. Gox, alleging a breach of contract.\textsuperscript{24} The companies had formed a partnership in February 2013 under which CoinLab handled all of Mt. Gox's U.S. services.\textsuperscript{25} CoinLab's lawsuit contends that Mt. Gox failed to allow them to move existing customers from Mt. Gox to CoinLab.\textsuperscript{26}

On May 15, 2013, the U.S. Department of Homeland Security (DHS) issued a warrant to seize money from Mt. Gox's U.S. subsidiary's account with payment processor Dwolla.\textsuperscript{27} The warrant suggests the U.S. Immigration and Customs Enforcement, an investigative branch of the DHS, felt that the subsidiary, which was not licensed by the U.S. Financial Crimes Enforcement Network (FinCEN), was operating as an unregistered money transmitter in


\textsuperscript{15} See Weiss, Benjamin, \textit{Ross Ulbricht, Creator of Silk Road Website, is Sentenced to Life in Prison}, New York Times (May 29, 2015).

\textsuperscript{16} See Silk Road Indictment. Interestingly, Ulbricht was also accused of paying for the killing of five people, although none were actually killed, and he was never prosecuted regarding these allegations.


\textsuperscript{18} Id. See also, Abrams, Rachel; Goldstein, Matthew; Tabuchi, Hiroko, \textit{Erosion of Faith was Death Knell for Mt. Gox}, New York Times (February 28, 2014).

\textsuperscript{19} Id.

\textsuperscript{20} Id. See also, Abrams, Rachel; Goldstein, Matthew; Tabuchi, Hiroko, \textit{Erosion of Faith was Death Knell for Mt. Gox}, New York Times (February 28, 2014).

\textsuperscript{21} See The Inside Story at pp. 4-5.

\textsuperscript{22} Id. Karpeles apparently owned 88 percent of Mt. Gox's $50 million in Bitcoin. Id.

\textsuperscript{23} Id. Karpeles apparently owned 88 percent of Mt. Gox's $50 million in Bitcoin. Id.

\textsuperscript{24} Chen, Adrian, \textit{Massive Bitcoin Business Partnership Devolves Into $75 Million Lawsuit}, Gawker Media (May 2, 2013).

\textsuperscript{25} Id.

\textsuperscript{26} Id.

\textsuperscript{27} Dillet, Romain, \textit{Feds Seize Assets From Mt. Gox's Dwolla Account, Accuse It Of Violating Money Transfer Regulations}, TechCrunch, AOL, Inc. (May 16, 2013).
the U.S. Between May and July, more than $5 million were seized. On June 29, 2013, nonetheless, Mt. Gox received its money services business (MSB) license from FinCEN.

However, it was reported in November 2013 that Mt. Gox customers were experiencing delays of weeks to months in withdrawing funds from their accounts, and cashing out became difficult to impossible. Things grew worse, and on February 7, 2014, Mt. Gox halted all withdrawals. Less than two weeks later, it suspended trading, closed its website and exchange service, and filed for a form of bankruptcy protection under Japanese law to allow courts to seek a buyer. In April 2014, the company began liquidation proceedings. It announced that around 850,000 bitcoins belonging to customers and the company were missing and likely stolen, an amount valued at more than $450 million at the time, having been hacked and stolen over a number of years. Although 200,000 bitcoins have since been “found,” the reason(s) for the disappearance — theft, fraud, mismanagement, or a combination of these — remain precisely unclear.

Significantly, six other major bitcoin exchanges had released a joint statement distancing themselves from Mt. Gox, shortly before Mt. Gox’s website went offline, amid steep drops in bitcoin prices and new demands for government regulation of the bitcoin industry.

III. U.S. Regulatory Initiatives

A. The Financial Crime Enforcement Network

1. Virtual Currency Guidance

The U.S. Treasury Department’s Financial Crime Enforcement Network (“FinCEN”), charged with the mission of safeguarding the U.S. financial system from illicit use and combating money laundering, has issued key federal guidance clarifying how FinCEN will apply the Bank Secrecy Act and other anti-money laundering laws to virtual currencies. Following FinCEN’s prior guidance on money services business in 2013, FinCEN released guidance on the application of FinCEN’s regulation to parties administering, exchanging, or using virtual currencies. In general, the guidance provides that “administrators and exchangers” of “convertible virtual currencies” are subject to the money transmitters (MT) rules, while “users” of virtual currencies are exempt. In so doing, FinCEN’s guidance built on its MT rules.

The guidance provides that a user is a person that obtains virtual currency to purchase goods or services. An exchanger is a person engaged as a business in the exchange of virtual currency for real currency, funds, or

28 Id.
29 Id.
30 Buterin, Vitalik, Mt. Gox Gets FinCEN MSB License, Bitcoin Magazine, Coin Publishing Ltd. (June 29, 2013).
31 Rise and Fall.
32 McLannahan, Ben, Bitcoin exchange Mt Gox files for bankruptcy protection, Financial Times, February 28, 2014; Abrams, Rachel; Goldstein, Matthew; Tabuchi, Hiroko, Erosion of Faith was Death Knell for Mt. Gox, New York Times (February 28, 2014).
33 Id. (http://www.theverge.com/2014/4/16/5619636/mt-gox-asks-for-permission-to-liquidate).
34 Id.
35 Id.
37 See https://www.fincen.gov/about/mission. FinCEN will also “promote national security through the collection analysis and dissemination of financial intelligence and strategic use of financial authorities.” Id.
38 See 6 FR 43585 (July 21, 2011).
40 Id.
other virtual currency. An administrator is a person engaged as a business in issuing (putting into circulation) a virtual currency, and who has the authority to redeem (to withdraw from circulation) such virtual currency.

A user who obtains convertible virtual currency and uses it to purchase real or virtual goods or services is not an MSB under FinCEN’s regulations. Such activity, in and of itself, does not fit within the definition of “money transmission services,” and therefore is not subject to FinCEN’s registration, reporting, and recordkeeping regulations for MSBs.

An administrator or exchanger that (1) accepts and transmits a convertible virtual currency or (2) buys or sells convertible virtual currency for any reason is a money transmitter under FinCEN’s regulations, unless a limitation to or exemption from the definition applies to the person. FinCEN’s regulations define the term “money transmitter” as a person that provides money transmission services, or any other person engaged in the transfer of funds. The term “money transmission services” means “the acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means.”

The definition of a money transmitter does not differentiate between real currencies and convertible virtual currencies. Accepting and transmitting anything of value that substitutes for currency makes a person a money transmitter under the regulations implementing the BSA.

FinCEN divided the activities of administrators and exchangers regarding convertible virtual currencies to which FINCEN regulations apply into three categories:

- Dealing in e-currencies and e-precious metals by transmitting funds between a customer and a third party that is not part of the currency or commodity transaction;
- Administering a centralized convertible virtual currency and facilitating the transfer of virtual convertible currency between locations, or from one person to another in a centralized repository; and
- Transacting in a de-centralized convertible virtual currency by (i) creating units of a virtual convertible currency with no central repository and (ii) selling those units to another person for real currency or its equivalent; or by facilitating the exchange of a de-centralized convertible virtual currency from one person to a third party for currency, funds, or other value.

FinCEN also stated that because a convertible virtual currency is not a “real” currency, FinCEN’s Prepaid Access regulations do not apply to a person who accepts or transmits a convertible virtual currency. The definition of “prepaid access” under the regulations is limited to “access to funds or the value of funds.” Similarly, FinCEN’s regulations regarding dealers in foreign exchange do not apply to accepting real currency in exchange for

---

41 Id.
42 Id.
43 Id.
44 Id.
45 Id.
46 Id.
47 Id.
48 Id.
convertible virtual currency (and vice versa) because those regulations only apply to the exchange of one real currency for another real currency.\footnote{Id.}

FinCEN’s new guidance did not eliminate existing exceptions to the definition of a money transmitter. According to FinCEN, determining if a person is a “money transmitter” still depends on the specific facts and circumstances surrounding a person’s activity. A person who accepts currency, funds, or other value from one person and transmits such currency, funds, or other value to another location or person, is still not a money transmitter if the person is:

\begin{itemize}
  \item A provider of network access services to money transmitters;
  \item A provider of bill payment services between a creditor or seller;
  \item An operator of clearance and settlement systems among regulated institutions;
  \item A transporter of physical currency (such as armored car services and couriers);
  \item A prepaid access provider; or
  \item A person who accepts and transmits funds only integral to the sale of goods or the provision of services (other than money transmission services) by the person who is accepting and transmitting the funds.\footnote{Id.}
\end{itemize}

As such, a person meeting the definition of an “administrator” or “exchanger” of a convertible virtual currency would not be subject to FinCEN regulation if one of the exceptions above applies.

2. Ripple Labs Consent Decree

On May 5, 2015, Ripple Labs (Ripple) entered into a consent decree with the Financial Crime Enforcement Network (FinCEN), under which Ripple admitted to conduct that violated U.S. anti-money laundering (AML) laws and agreed to take remedial measures to prevent future violations.\footnote{See In the Matter of Ripple of Labs, Inc. and XRP II, LLC, No-2015-05 Assessment of Civil Monetary Penalty, U.S. Department of the Treasury Financial Crimes Enforcement Network (May 5, 2015) ("In the Matter of Ripple Labs").} Concurrently, Ripple entered into an almost identical settlement agreement with the U.S. Attorney’s Office for the Northern District of California, U.S. Department of Justice (DOJ), under which Ripple further agreed to cooperate with the DOJ in any investigations and prosecutions into AML violations associated with Ripple’s conduct.\footnote{See Settlement Agreement Regarding Ripple Labs, U.S. Attorney for Northern California, U.S. Department of Justice (May 5, 2015) ("DOJ Consent Decree").} FinCEN assessed a $700,000 civil money penalty (CMP) against Ripple, of which $450,000 was satisfied by Ripple’s forfeiture to the DOJ of that amount.\footnote{In the Matter of Ripple Labs at 4.}

As the first BSA action against a virtual currency exchange by FinCEN, the size of the CMP was viewed as substantial, given that in recent years other money transmission businesses (MTs) have been fined smaller amounts for repeated AML violations over several years; notably Ripple and its affiliates were operating as MTs for only two years.\footnote{See Attachment A and B to DOJ Consent Decree.} The statement of facts and violations attached to the consent decree and settlement agreement sent a clear message that FinCEN and the DOJ expect full compliance by virtual currency companies with all BSA/AML requirements applicable to MTs,\footnote{Id.} citing that under recent guidance on virtual currency

\begin{thebibliography}{10}
\bibitem{Id.} Id.
\bibitem{Id.} Id.
\bibitem{See In the Matter of Ripple of Labs, Inc. and XRP II, LLC, No-2015-05 Assessment of Civil Monetary Penalty, U.S. Department of the Treasury Financial Crimes Enforcement Network (May 5, 2015) ("In the Matter of Ripple Labs").}
\bibitem{See Settlement Agreement Regarding Ripple Labs, U.S. Attorney for Northern California, U.S. Department of Justice (May 5, 2015) ("DOJ Consent Decree").}
\bibitem{In the Matter of Ripple Labs at 4.}
\bibitem{See Attachment A and B to DOJ Consent Decree.}
\bibitem{Id.}
\end{thebibliography}
activities from FinCEN, virtual currency sales activities obliged Ripple to register as MTs and to fulfill certain requirements applicable to MTs.\textsuperscript{56} These requirements include maintenance of an AML policy and appointment of an AML compliance officer, as well as numerous recordkeeping, monitoring, and reporting requirements.\textsuperscript{57} Although Ripple did eventually fulfill many of these requirements after becoming an MT, it was penalized for the interim period of several months when it was not compliant, as well as for failing to adhere to the requirements of its AML policy in connection with several sales.\textsuperscript{58}

The consent decree and settlement agreement also specified certain remedial measures to be taken by Ripple, including the creation and implementation of an AML training program, an external audit of Ripple’s AML program, enhancement of Ripple’s AML screening and monitoring capabilities, and retroactive examination of transactions for previously-undetected money laundering activity, along with filing any required Suspicious Activity Reports on such activity.\textsuperscript{59} Despite mandating general compliance with BSA/AML laws, the remedial measures also specifically call for compliance with the so-called Funds Travel Rule.\textsuperscript{60}

The “Travel” Rule generally requires regulated financial institutions (including MTs) to retain and include in payment instructions certain information related to the payment and its participants, so that a funds transfer can be traced from end to end even if it passes through multiple intermediary financial institutions.\textsuperscript{61} Traditional payment systems such as credit card, ACH, and wire are closed systems, set up to support the entry and transmission of the required information fields between participants, who must be regulated depository institutions. However, most cryptocurrencies are “open” systems, and users do not need to go through a financial institution in order to effect transactions. Commentators have observed that finding out whether any given counterparty is a financial institution and complying with the resulting Travel Rule requirements, while maintaining the privacy (and indeed personal safety) of individuals, presents an ongoing challenge for cryptocurrency businesses.\textsuperscript{62}

B. New York Department of Financial Services – Creating a BitLicense and Trust Company Digital Currency Exchange Charter

On August 12, 2013, The New York Department of Financial Services (“NYDFS”), citing New York’s “long history of promoting technical innovation – both within the financial sector and across our economy,” announced that it had launched an inquiry into the appropriate regulatory guidelines that it should put in place for virtual currencies.\textsuperscript{63} Based on the fact that it had already conducted “significant preliminary work” regarding the announced inquiry, including making requests for information from virtual currency firms,\textsuperscript{64} the NYDFS expressed

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{56} Id.
\item Id.
\item Id.
\item Id.
\item Id.
\item Id.
\item See FIN-2014-R011, Request for Administrative Ruling on the Application of FinCEN’s Regulations to a Virtual Currency Trading Platform, October 27, 2014. This position was reiterated in a second October 2014 Administrative Ruling (See FIN-2014-R012, Request for Administrative Ruling on the Application of FinCEN’s Regulations to a Virtual Currency Payment System, October 27, 2014).
\item See, e.g., Yuen, Dsu-Wei, FinCEN and Department of Justice Settle Anti-Money Laundering Charges Against Crypto-Currency Company Ripple Labs, Payment Law Advisor, Davis Wright Tremaine LLP (May 13, 2015); Marshall, Laura Colombell and Bowen, Amy Sims, FinCEN Announces First BSA Enforcement Action Against Virtual Currency Exchanger, Hunton & Williams (May 2015).
\item NYDFS, Notice of Inquiry on Virtual Currencies (August 12, 2013).
\item See N.Y.BL Title 23, Section 200.1-22.
\end{itemize}
\end{footnotesize}
concern that “at a minimum” virtual currency exchanges may be engaging in money transmission as defined in N.Y. law, “an activity that is licensed and regulated by DFS.”

While referencing the unique opportunities and challenges presented by Bitcoin and other virtual currencies, NYDFS nevertheless stressed instances “where the cloak of anonymity provided by virtual currencies has helped segment dangerous criminal activity,” such as drug smuggling, money laundering, gun running, and child pornography. As such, NYDFS observed that if virtual currencies remain a “Virtual Wild West” for “narco trafficking and other criminals,” it would not only threaten U.S. national security, but also “the very existence of the virtual currency industry as a legitimate business enterprise.”

As such, NYDFS cited three reasons for putting in place regulatory safeguards that would 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.” 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; so 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.”

On November 14, 2013, the NYDFS announced, “as the next step in its inquiry” that it would hold a public hearing on virtual currency regulation. With an asserted focus on the interconnection between money transmission regulations and virtual currency, NYDFS noted that the hearings would also focus on the possibility and feasibility of NYDFS issuing a “BitLicense” specific to virtual currency transactions and activities, which would include anti-money laundering and consumer protection requirements for licensed entities.

As a follow up to a year-long process, including two days of public hearings on January 28-29, 2014, where NYDFS heard from virtual currency investors, law enforcement agencies, and academics on virtual currency issues, the NYDFS subsequently announced in March 2014 a public order (“NYDFS VC Order”) initiating a process for accepting licensing applications for virtual currency exchanges under the N.Y. banking laws. Citing “a demonstrated need for stronger oversight of virtual currency exchanges” after the Mt. Gox collapse, NYDFS opted to offer a digital currency exchange banking charter pursuant to its authority to grant limited, special

65 Id.  
66 Id.  
67 Id.  
68 Id.  
69 Id.  
70 Wile, Rob, New York Will Be Holding Hearings on Bitcoin, buisnessinsider.com (November 4, 2013) (containing full text of NYDFS announcement).  
71 Id.  
72 See Order Pursuant to New York Banking Law §§ 2-b, 24, 32102-a and 4001-b and Financial Services Law §§ 301(c) and 302(a), In the Matter of Virtual Currency Exchanges, New York Department of Financial Services (March 11, 2014).
purpose trust company charters. The NYDFS VC Order also stressed that their new charter “should include strong legal and operational controls,” including “robust BSA/AML requirements.”

Following the submission of a number of applications, on May 7, 2015, NYDFS granted a charter to itBit Trust Company LLC to operate as a commercial Bitcoin exchange, the first virtual currency company to receive such a charter from NYDFS. In granting approval, the NYDFS press release stressed that it had conducted a “rigorous review” of the application, including, but not limited to, the company’s “anti-money laundering, capitalization, consumer protection and cyber security standards,” and also noted that itBit would be required to meet the obligation for operating a trust company under N.Y. law, as well as those under the final N.Y. Bit License regulations.

Prior to the itBit approval, on July 17, 2014, NYDFS proposed a BitLicense regulatory framework for virtual currency firms. These first-of-a-kind rules provided comprehensive regulatory regimes applicable to a wide variety of virtual currency businesses. The framework, which includes consumer protection, anti-money laundering, DFS examination and suspension requirements, and cyber security rules, books, records, financial disclosure capital adequacy, and audit requirements, was met with a mixed reaction by the virtual currency industry, which expressed concerns that regulations could stifle innovation in their recent industry, while realizing that the then-recent Mt. Gox scandal had reinforced regulatory and law enforcement concerns about the virtual currency business.

In the proposed rules, NYDFS stated that, among the issues related to the potential issuance of a BitLicense, it was considering:

- What specific types of virtual currency transactions and activities should require a BitLicense?
- Should entities that are issued a BitLicense be required to follow specifically tailored anti-money laundering guidelines?
- Should entities that are issued a BitLicense be required to follow specifically tailored consumer protection guidelines?

---

73 Id.
74 Id.
76 NYDFS itBit Press Release at 1. Since approving the itBit Charter, the NYDFS has approved a second virtual currency exchange charter to Gemini Trust Company LLC. See NYDFS Press Release, NYDFS Grants Charter to Gemini Bitcoin Exchange Founded by Cameron and Tyler Winklevoss (October 5, 2015).
78 Id at 1. NYDFS specifically referenced the fact that the same week NYDFS issued its notice of inquiry on virtual currencies a national magazine published an interview with an alleged key figure in the “black market drug website” Silk Road, who cited the virtual currency Bitcoin as a key ingredient in the site’s efforts to commit illegal acts. See also “Meet the Dread Pirate Roberts, The Man behind Booming Black Market Drug Website, Silk Road,” Forbes, Anay Greenberg, August 14, 2013, see: http://www.forbes.com/sites/andygreenberg/2013/08/14/meet-the-dread-pirate-roberts-the-man-behind-booming-black-market-drug-website-silk-road/ and Section II.B.1. and accompanying notes, supra.
79 Id.
- Should entities that are issued a BitLicense be required to follow specifically tailored regulatory examination requirements?

In December 2014, DFS outlined an updated BitLicense framework that incorporated feedback from the first round of public comments. The updated proposal contained a series of changes and clarifications, including the creation of a two-year transitional BitLicense to assist startups. The additional comment period for the revised BitLicense framework ended in March 2015, and final rules were adopted in June 2015.\(^\text{80}\)

C. The Office of the Comptroller of the Currency – The Fintech Charter

In the wake of a multi-year effort by the New York Department of Financial Services to pioneer the establishment of a regulatory framework for a special purpose, fintech trust charter focused on virtual currency business activities, the Office of Comptroller of the Currency (the “OCC”) has sought to take a lead in this area by announcing in 2016 initiatives designed to create an optional charter for fintech business activities. Following an initiative announced in August 2105 by the OCC to develop a “comprehensive framework” to improve the OCCs ability to “identify and understand trends and innovations in financial services,” as well as the “evolving needs of consumers of financial services,” the OCC in March 2016 published a paper entitled Supporting Responsible Innovation in the Federal Banking System: An OCC Perspective (“OCC Innovation Paper”).\(^\text{81}\)

Noting, among other things, the broad innovation in financial services taking place “outside the banking industry,” often in “unregulated or lightly regulated fintech companies,” the OCC Innovation Paper stressed that the fintech companies are growing rapidly, and attracting increased investment both in the U.S. and globally.\(^\text{82}\) The OCC Innovation Paper concluded that bank and nonbank innovators, through “strategic and prudent collaboration,” could benefit by employing their respective advantages — nonbank innovators can gain access to funding sources and large customer bases and banks can gain access to new technologies.\(^\text{83}\)

The OCC Innovation Paper became the springboard for the OCC’s subsequent efforts to create a fintech charter. To date, however, a number of issues have arisen with respect to the OCC’s project. First, while OCC special purpose banks such as trust and credit card banks are exempt from parent company regulation under the Bank Holding Company Act, it is not clear whether the Federal Reserve Board would be comfortable with the creation of a new bank charter exempt from the BHCA. Second, state regulators have raised significant concerns as to whether the project is a preemption Trojan horse, i.e., a way to route nonbank lending and other activities around state usury and other consumer laws through a national charter.\(^\text{84}\) Third, virtual currency companies and trade groups have urged that such charters be structured so as to be user-friendly for virtual currency activities.\(^\text{85}\) Finally, there has been speculation about potential FDIC concerns about regulation and receivership of non-depository fintech charters; notably, the OCC recently proposed a rule that would make clear that the OCC would handle all OCC uninsured national bank failures.\(^\text{86}\)

\(^{80}\) Id.


\(^{82}\) OCC Innovation Paper at 3.

\(^{83}\) Id.

\(^{84}\) See Lalita Clozel, State Regulators Balk at OCC Fintech Charter, American Banker (August 19, 2016).


\(^{86}\) See 81 F.R. 177 at 62835 (September 13, 2016) (proposed rule addressing how the OCC would conduct the receivership of an uninsured national bank) (“Proposed Trust Bank Receivership Rules”). In that rulemaking, referring to the OCC Innovation Paper, the OCC stated that – in undertaking the rulemaking, one of its reasons is considering how best to implement a regulatory framework that is
Nonetheless, on December 7, 2016, the OCC announced that it would move forward with chartering fintech companies that offer bank products and services to become special purpose material facts. Accompanying this decision, the OCC published a paper entitled Exploring Special Purpose National Bank Charters for Fintech Companies (“OCC Fintech Charter Paper”), discussing the issues and conditions that the agency will consider in granting special purpose national bank charters, with a request for public comment. In so doing, the OCC raised a number of significant points and issues related to attributes and regulation of the new charter:

- The OCC identified the potential universe of fintech companies that may explore such a charter as marketplace lenders providing consumer and small business loans, payment-related services, companies engaged in digital currencies and distributed ledger technology, and financial planning and wealth manager products and services.

- OCC fintech chartered banks would be held to the “same rigorous standards of safety and soundness, fair access and fair treatment of customers” that apply to all national banks.

- The OCC may need to take into account “differences in business models and the applicability of certain laws.” It specifically cited as an example a fintech company with a special purpose national bank charter “that does not take deposits, and therefore is not insured by the Federal Deposit Insurance Corporation, [and thus] would not be subject to laws that apply only to depository institutions.” As such, the OCC Fintech Charter Paper clarifies prior confusion in this area by making clear that OCC policy is that special purpose national banks that do not engage in deposit taking are not required to obtain deposit insurance.

- Notably, the OCC did not take the position that creating a national bank fintech charter required a notice and public comment rulemaking process, nor is one being proposed. As such, the OCC will be issuing such charters under its existing authority to grant special purpose national bank charters. Whether this position opens the OCC to the possibility of legal challenges of its authority to do so without a rulemaking process subject to the Administrative Procedure Act remains to be seen.

- A special purpose national bank that conducts administrative activities other than the trust and fiduciary activities must conduct at least one of the following core banking functions: receiving deposits, paying

---


89 OCC Fintech Press Release (public comments may be submitted through January 15, 2017).


91 Id.

92 Id.

93 Id.

94 Id. Notably, after some prior confusion about whether the OCC would require deposit insurance for national trust banks, the OCC’s recent Proposed Trust Bank Receivership Rules also stated:

There are only a small number of uninsured national banks in operation today. The OCC, however, retains the authority to grant new charters to entities whose business plan does not call for them to obtain deposit insurance if the OCC determines that the entities have a reasonable chance of succeeding and can operate in a safe and sound manner, among other considerations. 81 F.R. 62835 (emphasis added).

95 OCC Fintech Charter Paper at 3; see also 12 U.S.C. 1 et seq. and 1461 et seq. (OCC authority to grant national bank charters, including for special purpose national banks).
checks or lending money.\textsuperscript{96} Interestingly, the OCC generally observed that “there is no legal limitation on the type of” special purpose “for which a national bank charter may be granted, so long as the entity engages in fiduciary activities or in activities that include receiving deposits, paying checks or lending money.” In so doing, it also stated that the OCC has the legal authority to construe these activities to include a wide range of bank permissible technology-based innovations in financial services — including considering on a case-by-case basis the permissibility of a new activity that a company seeking a special purpose charter wishes to conduct.\textsuperscript{97}

- In general, a special purpose national bank will be subject to the same laws, regulations, examinations, reporting requirements, and ongoing regulation and supervision as other national banks, industry, lending and consumer financial, BSA/AMC and other anti-money laundering laws, OFAC rules and sanctions, prohibitions on engaging in unfair or deceptive acts or practices under Section 5 of the Federal Trade Commission Act and unfair, deceptive, or abusive acts or practices under Section 1036 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (“Dodd-Frank Act”) and bank chartering regulations and licencing policies.\textsuperscript{98}

- A special purpose national bank also has the same “status and attributes” under federal law as a full service national bank; notably this includes limits on state visitorial powers, federal preemption (including the OCC preemption regulations) and federal judicial precedents to determine “if and how” a state law applies\textsuperscript{99}, and “hot button” issues addressed in the Dodd-Frank Act.\textsuperscript{100}

- The Community Reinvestment Act and certain provisions of the Federal Deposit Insurance Act that only apply to depository institutions would not apply to an uninsured special purpose trust bank.

- Coordination with other regulations may be required, such as with the Federal Revenue Board, to become members of the Federal Revenue System and contain the scope and requirements of the Bank Holding Company Act e.g., to qualify for one of the exemptions from the definition of “bank” with the BHCA (and thus, any parent company or control entity is exempt from regulation as a bank holding company)\textsuperscript{101}; the FDIC, where a fintech company proposes to access deposits other than trust funds; and the Consumer Financial Protection Bureau, as appropriate for compliance with federal consumer financial laws.\textsuperscript{102}

- The OCC sets our “baseline supervising expectations” to meet “high supervising standards.” These standards include safety and soundness requirements, as well as requirements to provide fair access to financial services, treat customers fairly, and comply with all applicable laws and regulations; baseline

\textsuperscript{96} Id.  See also 12 CFR § 5.20(e)(1) (required banking activities).
\textsuperscript{97} Id. at 3-4 and accompanying notes.
\textsuperscript{99} Id. at 5.
\textsuperscript{100} In this regard, the OCC stated:

For example, under these statutes, rules and precedents, state laws would not apply if they would require a national bank to be licensed in order to engage in certain types of activity or business. Examples of state laws that would generally apply to national banks include state laws on anti-discrimination, fair lending, debt collection, taxation, zoning, criminal laws, and torts. In addition, any other state laws that only incidentally affect national banks’ exercise of their federally authorized powers to lend, take deposits, and engage in other federally authorized activities are not preempted. Moreover, the OCC has taken the position that state laws aimed at unfair or deceptive treatment of customers apply to national banks.  Id.  See also Section 1044 of the Dodd-Frank Act.

\textsuperscript{101} See 12 U.S.C. 1841 (exemptions from “bank” definition under the BHCA such as for trust banks).
\textsuperscript{102} Id. at 6 and accompanying notes.
supervisory expectations stress the importance of a detailed business plan, governance, capital, liquidity, compliance risk management, financial inclusion, and recovery resolution planning.\(^{103}\)

- Distinct from any CRA obligatory special purpose bank applicants that seek to engage in lending activities must demonstrate a commitment to “financial inclusion” that supports “fair access to financial services and fair treatment of customers.”\(^ {104}\) As such, the OCC cited the fact that the problems of “financially insured and underserved is a global problem,” citing definitions of “financial inclusion” by both the World Bank and Basel Committee on Banking Supervision.\(^ {105}\)

- The OCC will resume business plans to include alternate business “recovery and exit strategies,” stress test scenarios, and worst-case resolution plans.\(^ {106}\) This is an interesting development to the extent that such required planning requires stress tests and resolution planning otherwise generally applicable only to currently systematically important financial institutions (SIFI’s) under the Dodd-Frank Act.\(^ {107}\)

- As part of the OCC chartering process, the OCC will impose a number of standard requirements on a bank when it grants preliminary approval, as well as other candidates as appropriate.\(^ {108}\)

- As has been done with other special purpose national banks such as trust funds, the OCC may modify or adapt capital and other legal requirements to different types of business models.\(^ {109}\) This would lead to a process of negotiation on appropriate capital levels on certain business activities, although obviously any new OCC precedents will be revised as it grants new charters for particular business models.

- Finally, the OCC requested public “feedback” (ostensibly as opposed to “comments” if it were a seeking notice and comment in a public rulemaking, rather than a paper) on a wide range of issues.\(^ {110}\)

\(^{103}\) Id. at 6-7 and accompanying notes.

\(^{104}\) Id. at 8 and accompanying notes.

\(^{105}\) Id. at 12, footnote 30 stated:

The problem of financially unserved and underserved sectors of society is a global issue. The World Bank has described “financial inclusion” to mean that “individuals and businesses have access to useful and affordable financial products and services that meet their needs—transactions, payments, savings, credit and insurance—delivered in a responsible and sustainable way.” See The World Bank Financial Inclusion Overview page at http://www.worldbank.org/en/topic/financialinclusion/overview. Separately, recent final guidance from the Basel committee on Banking Supervision addresses financial inclusion, focusing on unserved and underserved customers. See Guidance on the application of the Core Principals for Effective Banking Supervision to the regulation and supervision of institutions relevant to financial inclusion (September 2016) at http://www.bis.org/bcbs/publ/d383.pdf.

\(^{106}\) Id. at 12 and accompanying notes.

\(^{107}\) See U.S.C. 5384(a)(11) (Orderly Liquidation Authority for failing SIFIs).

\(^{108}\) Id. at 14 and accompanying notes. See also e.g., OCC Conditioned Approval #1143. Change in Bank Control Notice by Stifel Financial Corp. to Acquire Barclays Wealth Trustees (U.S.), NA, Wilmington, Delaware (Charter #24955) OCC Control Number: 2015-NE-CBCa-144361 (January 2016).

\(^{109}\) Id. at 14 and accompanying notes.

\(^{110}\) Id. at 15-16. Specifically the OCC asked for feedback in the following.

1. What are the public policy benefits of approving fintech companies to operate under a national bank charter? What are the risks?

2. What elements should the OCC consider in establishing the capital and liquidity requirements for an uninsured special purpose national bank that limits the type of assets it holds?

3. What information should a special purpose national bank provide to the OCC to demonstrate its commitment to financial inclusion to individuals, businesses and communities? For instance, what new or alternative methods (e.g., products, services) might a special purpose national bank establish in furtherance of its support for financial inclusion? How could an uninsured special purpose bank that uses innovative methods to develop or deliver financial products or services in a virtual or physical community demonstrate its commitment to financial inclusion?

4. Should the OCC seek a financial inclusion commitment from an uninsured special purpose national bank that would not engage in lending, and if so, how could such a bank demonstrate a commitment to financial inclusion?

5. How could a special purpose national bank that is not engaged in providing banking services to the public support financial inclusion?
Within a few days of the announcement, the NYDFS Superintendent issued a public statement strongly opposing the charter and any efforts “to federalize what states have been doing – and doing well – for over a quarter of a century,” asserting that “History has demonstrated that states, not the federal government, have the requisite knowledge and experience to effectively regulate nondepository financial services providers and guard against predatory and abusive practices,” thereby setting the stage for a potentially contentious debate about the OCC Fintech charter with the states.

**D. The Regulation of Virtual Currency Business Act**

In February 2016, The National Conference of Commissioners on Uniform State Laws (“NCCUSL”) published a discussion draft of the Regulation of Virtual Currency Business Act (“VC Business Act”). As with its other similar projects, the VC Currency Act is designed to provide a uniform state law governing the operation of a business, wherever located, that engages in the “virtual currency business.” The term virtual currency business is broadly defined to include offering virtual currency transfer and storage services, facilitating virtual currency transfers, offering the conversion of virtual currency, or otherwise offering services and products that assist residents of a state or jurisdiction to acquire, convert, or transfer virtual currency. It similarly provides broad definitions of terms such as virtual currency, virtual currency business activity, and what constitutes a transfer of virtual currency.

The commentary (“Comment”) to the VC Business Act notes that the overall goal of the project is to capture within the scope of the draft Act activities that meet the definition of “virtual currency business activity,” with this definition, as well as “virtual currency,” remaining “central to this exercise.”

---

6. Should the OCC use its chartering authority as an opportunity to address the gaps in protections afforded individuals versus small business borrowers, and if so, how?

7. What are potential challenges in executing or adapting a fintech business model to meet regulatory expectations, and what specific conditions governing the activities of special purpose national banks should the OCC consider?

8. What actions should the OCC take to ensure special purpose national banks operate in a safe and sound manner and in the public interest?

9. Would a fintech special purpose national bank have any competitive advantages over full-service banks the OCC should address? Are there risks to full-service banks from fintech companies that do not have bank charters?

10. Are there particular products or services offered by fintech companies, such as digital currencies, that may require different approaches to supervision to mitigate risk for both the institution and the broader financial system?

11. How can the OCC enhance its coordination and communication with other regulators that have jurisdiction over a proposed special purpose national bank, its parent company, or its activities?

12. Certain risks may be increased in a special purpose national bank because of its concentration in a limited number of business activities. How can the OCC ensure that a special purpose national bank sufficiently mitigates these risks?

13. What additional information, materials, and technical assistance from the OCC would a prospective fintech applicant find useful in the application process?

---


112 Regulation of Virtual Currency Business Acts, National Conference of Commissioners on Uniform State Laws (February 19-21, 2016 Drafting Committee Meeting).

113 See Draft Section 102.

114 VC Currency Act Draft Section 102(a)-(d).

115 Id. at Draft Section 103(24).

116 Id. at Draft Section 103(25).

117 Id. at Draft Section 103(19).

118 VC Business Act comments at p. 9. The comments noted that questions arise including whether the “virtual currency” definition should include “e-precious metals” and e-certificates for precious metals that can be transferred from one owner to another. Id. In so doing, the Comment noted that FinCEN issued guidance in August 2015 that extended its March 2013 guidance concerning what types of business
In considering other issues such as how to include an “on-ramp” for new entrants to the virtual currency business, de minimus exceptions, and whether to differentiate principal vs. intermediary activities, a final question presented concerned coverage or exclusion of trust companies who receive their charters and powers from States. The Comment noted that New York State issued a trust company charter to ItBit in 2015. ItBit’s ability to engage in transactions with residents of other States was challenged by other States and, thus, for this draft, information about inclusion or exclusion of trust companies is “bracketed” until the Drafting Committee can further discuss this issue with particularity.119

As such, the Comment raises the question of what happens when one State creates a special purpose digital currency exchange trust charter, but other states do not recognize it as such, i.e., a trust company subject to typical reciprocity arrangements or that otherwise regulates such business as a money transaction, not a trust company.120 To date, however, no effort has been made by states to invoke reciprocity arrangements governing the interstate activities of traditional trust companies.121

In this regard, the Draft VC Business Act specifically addresses reciprocal licensing arrangements, providing three (3) Alternatives for reciprocity, instructing that “a jurisdiction should select one.”122

The Draft VC Business Act also addresses a wide range of business and regulatory aspects of such businesses, including licensing and applications,123 net worth/minimum capital requirements,124 authority to conduct regulatory examinations,125 cooperation and data sharing authority,126 change in control and merger regulatory standards and approvals,127 records maintenance,128 confidentiality,129 license suspension and revocation,130 cease and desist orders,131 civil money penalties,132 end user disclosure protections,133 and compliance policies with procedures.134 Interestingly enough, important topics such as cyber security programs and activity with virtual currency render the business a “money services business” for the purposes of federal AML requirements under 31 C.F.R. Part X. See Application of FinCEN’s Regulations to Persons Issuing Physical or Digital Negotiable Certificates of Ownership of Precious Metals FinCEN Ruling FIN-2015-R001 (August 14, 2015). The 2015 guidance included e-precious metals and e-certificates for precious metals. The VC Business Act includes both in the definitions of “virtual currency” and “virtual currency business activity.

---

119 See Cozel, Lalita, Are Trust Charters the Key to Simplifying Fintech Regulations, American Banker (November 8, 2016) (discussing the fact that the only two digital currency exchanges licensed by New York State as special purpose trust companies have had significant challenges making the case to regulators of their trust status outside New York, causing uncertain scenarios for these companies “in a number of states that simply do not have experience with digital currency or digital currency exchange;” quoting V. Gerard Comizio, Paul Hastings LLP. Id.)

120 See Conference of State Bank Supervisors, Uniform Application for Interstate Trust Activities of State-Chartered Trust Institutions; Nationwide Cooperative Agreement for Supervision and Examination of Multi-State Trust Institutions. Draft Sections 201-203.

123 Draft Sections 201-203, 205-206.

124 Draft Section 207.

125 Draft Section 301.

126 Draft Section 302.

127 Draft Section 303.

128 Draft Section 304.

129 Draft Section 305.

130 Draft Section 501.

131 Draft Section 502.

132 Draft Section 503.

133 Draft Section 504.

134 Draft Section 702.
monitoring, business continuity with disaster recovery program requirements, and permissible investments have been reserved for further discussion by the Committee. ¹³⁵

It remains to be seen whether the VC Currency Act is timely adopted as a model code, and, if so, whether it becomes an influential model for state legislatures in adopting virtual currency legislation.

IV. International Regulatory Developments

Outside of the U.S., virtual currency laws, regulations, and policies are emerging globally. This section will survey a few select jurisdictions with major impact on the global financial services industry: 1) The European Union, 2) The United Kingdom, 3) China and 4) Japan, and the Basel Committee on Banking Supervision. While this survey is by no means comprehensive, only a handful of countries have specific regulations applicable to virtual currency use; at least forty jurisdictions, exclusive of the European Union, have ventured to varying extents into the regulation of virtual currency.¹³⁶

A. The European Union: The European Bank Authority

In the wake of the 2008 global financial crisis, the European Union (EU) established the European Banking Authority (EBA) as an independent EU authority designed to, among other things, ensure effective and consolidated prudential regulation and supervision across the EU banking sector.¹³⁷ The main task of the EBA is to contribute to the creation of the so-called European Single Rulebook in banking, whose objective is to provide a single set of harmonized prudential rules for financial institutions throughout the EU, promote the convergence of regulatory practices, and assess the risks and vulnerabilities in the EU banking sector — the world’s first supranational financial services regulator.¹³⁸ In its short time in existence, the EBA has weighed in heavily on virtual currencies. First, in December 2013, the EBA issued Warning to Consumers on Virtual Currencies.¹³⁹

The asserted reason for the publication was to issue a “warning to highlight the possible risks associated with buying, holding or trading virtual currencies,” such as Bitcoin.¹⁴⁰ The publication highlighted the possible risks, including the possibility of “losing your money” in the context of the fact that “no specific regulatory protections exist” that would cover losses if a platform that exchanges or holds a customer’s virtual currencies fails or goes out of business.

In encouraging consumers to understand the risks associated with virtual currencies, the publication stressed the following potential risks:

- “you may lose your money” as an exchange platform, including through theft and hacking by third parties
- “your money may be stolen from your digital wallet”
- “you are not protected” when using virtual currencies as a means of payments

¹³⁵ See Draft Sections 401, 402, 801, and 802 [Reserved].
¹³⁸ Id. - The EBA was established as part of the European System of Financial Supervision, and, pursuant to EU Regulation 1093/2010, took over all existing responsibilities and tasks of the Committee of European Banking Supervisors.
¹³⁹ European Banking Authority, Warning to Consumers on Virtual Currencies (12 December 2013).
¹⁴⁰ Id. at 1.
“the value of your virtual currency can change quickly, and could even drop to zero”

Transactions in virtual currency may be misused for criminal activities, including money laundering, and

Holding virtual currency may have tax implications, including value added and/or capital gains tax.\textsuperscript{141}

Finally customers were warned that, in buying virtual currencies, consumers should not use “real” money that they cannot afford to lose, not keep large amounts of money in a digital wallet for extended periods of time, and become familiar with the ownership, business model, transparency, and public perceptions of any digital currency trading exchange platform they may consider using.\textsuperscript{142}

As a follow up, the EBA in July 2014 issued its \textit{Opinion on Virtual Currencies}\textsuperscript{143} ("VC Opinion"). Stressing that one of the tasks of the EBA is to “monitor new and existing financial activities," and adopt appropriate regulations and guidance, the EBA noted that the EBA’s 2013 “public warning on VCs left unaddressed the question of whether VCs can or should be regulated."\textsuperscript{144} While noting that there are some potential benefits of VCs, for example, reduced transaction cost, faster transaction speed, and financial inclusion, the risks, by contrast, “are manifold," identifying more than 70 perceived risks across several categories, including risks to users; risks to non-user market participants; risks to financial integrity, such as money laundering and other financial crime; risks to existing payment systems in conventional fiat currencies; and risks to regulatory authorities.\textsuperscript{145} Noting that a regulatory approach that addresses VC risks comprehensively would require “a substantial body of regulation" as part of having a “‘long term’ regime" in place, it made two recommendations for mitigating “some of the more pressing risks."\textsuperscript{146}

First, the EBA recommended that all EU national regulatory authorities discourage credit and financial institutions, payment institutions, and e-money institutions from buying, selling, or holding VCs for their own account.\textsuperscript{147} In addition, the EBA also recommended that EU legislators consider declaring market participants at the direct interface between conventional and virtual currencies, such as virtual currency exchanges, to become so-called ‘obliged entities’ under the EU Anti-Money Laundering Directive and thus, subject to its anti-money laundering and counter terrorist financing requirements.\textsuperscript{148}

As a result, and prompted by the terrorist attacks in France in 2015, the European Commission adopted proposals in response to the EU Council’s conclusions of February 2016 on the fight against the financing of terrorism, which underlined the importance of achieving rapid progress in legislative actions, including in the field of virtual currencies, and which called on the Commission to submit targeted amendments to EU Law.\textsuperscript{149} A parallel resolution and report was published by the European Parliament ("EP") in May 2016, in which the EP proposed, \textit{inter alia}, that the Commission develop recommendations for any legislation needed to regulate the VC sector.\textsuperscript{150}

\textsuperscript{141} Id. at 2-3.

\textsuperscript{142} Id. at 3.

\textsuperscript{143} EBA Opinion on Virtual Currencies, EBA/OP/2014/08; see http://www.eba.europa.eu/-/eba-proposes-potential-regulatory-regime-for-virtual-currencies-but-also-advises-that-financial-institutions-should-not-buy-hold-or-sell-them-whilst-n.

\textsuperscript{144} VC Opinion at 5.

\textsuperscript{145} Id. at 5.

\textsuperscript{146} Id.

\textsuperscript{147} Id. at 5-6.

\textsuperscript{148} Id.


In response to the legislative initiatives, the EBA in August 2016 published an opinion responding to the commission proposal and set out seven proposals that the EU commission and co-legislators should take into account when finalizing the VC amendments to EU law. These proposals included recommendations regarding the scope of VC licensing, enforcement sanctions, control standards, information exchange, and application of AML laws.

B. The United Kingdom

In August 2014, the U.K. government announced a program looking into the particular benefits and risks associated with digital currencies and underlying technology, with a particular focus on the question of regulation. In November 2014, the government published a request for public comment to gather views and evidence on these questions, receiving over 120 responses from members of the public who use digital currencies, digital currency developers, businesses providing digital currency-related services, banks, payment scheme companies, academics, consultancies, and other government departments and agencies.

In March 2015, HM Treasury published a report, Digital currencies: response to the call for information (“HM Treasury Report”) that summarized the response, and more significantly, reached certain conclusions regarding next steps related to potential digital currency regulation.

The HM Treasury Report noted that two factors in particular were highlighted as the main challenge faced by digital currency businesses setting up in the UK, and many respondents saw these issues as connected. Most mentioned the lack of a regulatory framework for digital currencies, commenting that this has caused some uncertainty for businesses and has made it difficult for the industry to prove its credibility and legitimacy. The second theme that emerged in responses was that the digital currency firms have encountered difficulties in opening bank accounts in the UK. Many businesses described how they have been forced to open bank accounts overseas, which results in day-to-day business being slower and drives up costs.

---


152 Id.

153 See Chancellor’s speech at the launch of the new trade body for Fintech, Innovative Finance, the Rt. Hon George Osborne (August 6, 2014).

154 See HM Treasury, Digital currencies: call for information (November 3, 2014). It is interesting to note that the call for information also asked for views on the impact of FinCEN application of anti-money laundering regulations to administrators and exchangers of digital currencies. On the whole, responses from digital currency firms (including a number which operate and are regulated in the U.S.) were positive, reporting that regulation has increased the legitimacy of digital currency firms, helped firms establish banking partnerships and investment, and deterred criminals. Despite this, however, various submissions commented that there is a lack of clarity about which categories of business activity are captured by FinCEN requirements, and some said that the process of registering in multiple American states has been burdensome and has forced smaller firms to exit the market. Id. at 13.

A number of submissions also commented on the proposed ‘BitLicense’ framework that has been put forward by the New York Department of Financial Services. Digital currency firms answering on this agreed that the proposed BitLicense regime, at least as initially drafted, “would be too wide in scope and would impose very high compliance costs on digital currency firms and risk damaging the sector.” Id.


156 Id. at 14.

157 Id.

158 Id. at 19.
Submissions from the U.K. banking sector also highlighted a lack of regulation as a key reason for hesitation amongst banks to take on digital currency firms as customers, and many digital currency firms also discussed the issue of access to banking as closely related to the question of regulation.¹⁵⁹

On the question of what steps the government could take to support the industry, many responses focused on the question of “bringing the sector into regulation.”¹⁶⁰ Nearly two thirds of responses considered the question of whether the government should introduce regulation of any kind; over 80% of these contributions said that the sector should be brought into some form of regulation.¹⁶¹

The HM Treasury Report concluded that the government considers that digital currencies represent an interesting development in payments technology, with distributed, peer-to-peer networks and the use of cryptographic techniques “making possible the efficient and secure transfer of digital currency funds between users,” with potential advantages clearest for purposes such as micro-payments and cross-border transactions.¹⁶² However, while the technology offers considerable potential, The HM Treasury Report also concluded that digital currencies have so far been adopted by a relatively small number of consumers and retailers around the world, and both the technology, and the industry that has grown up around it, “are still in a nascent state,”¹⁶³ with the evidence suggesting that the market in which digital currency firms are operating is not functioning as well as it could, and “there is a good case for proportionate regulation” at this time to provide a supportive environment for legitimate digital currency users and businesses.¹⁶⁴

Notably, The HM Treasury Report also extensively discussed concerns about potential risks presented by digital currency in relation to crime, money laundering, terrorist financing, tax evasion, and sanctions evasion cited by commenters, and how such potential risks could be mitigated by appropriate regulations.¹⁶⁵

The government response to these concerns was twofold. First, it stated that the evidence available indicates that digital currencies have been used by illicit actors, but the information does not suggest that digital currencies have, at present, been widely adopted as a payment vehicle in the wider criminal community. The government notes that the degree of anonymity and the ease of making payment are key drivers of potential criminal use, and that anonymous use of digital currencies is closely linked to the absence of an effective “know your customer” regime being in place.¹⁶⁶

Second the government recognized the “broad support” for proportionate, but robust, anti-money laundering regulation in order to limit the abuse of digital currencies by criminals or terrorists, and to support development and innovation in the sector.¹⁶⁷

Among its conclusions, the HM Treasury Report stressed that it was committed to measures that are intended to create the right environment for legitimate actors to flourish, and to create a hostile environment for illicit users of digital currencies.¹⁶⁸ It also highlighted the following:

¹⁵⁹ Id.
¹⁶⁰ Id.
¹⁶¹ Id.
¹⁶² Id.
¹⁶³ Id.
¹⁶⁴ Id.
¹⁶⁵ Id.
¹⁶⁶ Id.
¹⁶⁷ Id.
¹⁶⁸ Id. at 9.
The distinctive features of digital currencies can be attractive to illegal users, as well as people and businesses who like to use digital currencies for legitimate purposes. In response, the government intends to apply anti-money laundering regulation to digital currency exchanges, to support innovation and prevent criminal use. The government committed to, and has undertaken since then, a full consultation on the proposed regulatory approach to seek views and evidence on key questions, including how anti-money laundering regulation should be applied to the digital currencies sector, the scope of the regulatory perimeter, and the identity of the regulator.  

As part of the consultation on the proposed regulatory approach, the government will look at how to ensure that law enforcement bodies have effective skills, tools, and legislation to identify and prosecute criminal activity relating to digital currencies, including the ability to seize and confiscate digital currency funds where transactions are for criminal purposes.

Given the nascent state of the technology and the surrounding industry, it recognizes that users of digital currencies are potentially exposed to a number of risks. In response, the government considers that a framework for best practice standards for consumer protection is the right step to take at this stage, in order to address the risks identified, but “without imposing a disproportionate regulatory burden on the industry,” and intends to work with the digital currency industry to develop pioneering voluntary standards for consumer protection.

Since the HM Treasury Report was issued, the UK has begun various regulatory initiatives related to digital currency, while at the same time stressing the desire for the UK to be a global center for FinTech.

C. The Basel Committee on Banking Supervision

As a working committee of the Basel Committee and the Bank for International Settlements Committee on Banking Supervision, the Committee on Payments and Market Infrastructures (“CPMI”), among other things, aims at “strengthening regulation, policy and practices” in the payment system, clearing settlements and related arrangements.

In November 2015, The CPMI issued a report on digital currencies (“CPMI Report”), in considering the possible implications of interests to central banks worldwide arising from innovations in digital currencies.

The CPMI Report concluded that regulatory issues for digital currencies based on distributed ledgers cover three main fields: consumer protection, prudential and organizational rules for the different stakeholders, and specific operating rules as payment mechanisms.

Further, the CPMI Report concluded that given the nature of digital currencies, which are typically online and therefore not limited to national jurisdictions, a coordinated approach at a global level may be important for

---

168 Id.
169 Id.
170 Id.
171 Id.
172 See, e.g. Peter Campbell, Osborne wants London to be “global centre for FinTech,” Financial Times (November 11, 2015). (Chancellor of the Exchequer indicates that UK regulators will provide “space where innovation can happen”).
regulation to be fully effective. Nonetheless, the CPMI Report stressed that this does not preclude certain actions at the national level, for which it identifies at least five general categories of action:

- **Information/moral suasion**: rather than interfering directly with the development of digital currencies, authorities could decide to use moral suasion towards users and investors in order to highlight the relevant risks and to influence the market.

- **Regulation of specific entities**: via such an institutional approach, authorities could establish a limited set of regulations for specific types of entities (e.g., those that enable interaction between digital currencies and traditional payment instruments and/or the real economy). Firms that might be subject to specific regulation include intermediaries providing digital currency-related services, such as exchanges, merchant acceptance facilities, and “digital wallet” applications enabling users to store and transact in their units of the digital currency.

- **Interpretation of existing regulations**: some authorities may be able to assess whether existing regulatory arrangements might be applied to digital currencies and digital currency intermediaries. One example is the area of taxation law, where authorities have made determinations of how tax legislation might apply to digital currency arrangements.

- **Broader regulation**: although jurisdictional issues are likely to be a challenge, authorities might seek to take a broader approach to regulation, potentially reflecting a functional approach, such that regulatory obligations that apply to traditional payment methods and intermediaries also apply to digital currency schemes and digital currency intermediaries. As an example, authorities might seek to ensure that AML/KYC requirements apply to digital currency transactions and counterparties, or that the same consumer protection arrangements apply to transactions conducted with digital currencies as to other payment methods used by consumers.

- **Prohibition**: authorities could seek to ban the use of digital currencies in their respective jurisdictions. Practically, this could imply a ban on any digital currency based financial activities, as well as digital currency exchanges or digital currency acceptance by retailers.176

Finally, the CPMI Report concluded that these categories can provide a "general framework for the analysis and classification of actions undertaken by national authorities."177

D. China

In December 2013, The Chinese central bank announced that all Chinese financial institution and payments systems were barred from handling virtual currency.178 The notice from the People’s Bank of China ("PBOC") stated that the ban was imposed because bitcoins were not backed by any nation or central authority. It added that it was planning to step up its efforts to curb the use of bitcoins to launder cash.179

Individuals were advised that they are still free to trade in bitcoins, but should be aware of the risks bitcoins involve, adding that the PBOC planned to formalize the regulation of exchanges that dealt in digital currency.180

---

176 Id. At 12.
177 Id.
178 See Joe McDonald, Associated Press, China Bans its Banks from Handling Bitcoin, Business Insider, (December 5, 2013); China Bans Banks form handling Bitcoin trade, BBC Online News (December 5, 2013).
179 Id.
180 Id.
Further, Alibaba, China’s top internet retailer, announced an January 9, 2014 that it was prohibiting the use of Bitcoin on its online shopping platforms, thereby rendering the practical use of Bitcoin even more difficult in China, despite massive investor interest in virtual currencies in that country.  

Notwithstanding the foregoing, the PBOC Governor Zhou Xiaochuan subsequently publicly stated that China would not seek to ban bitcoins and other virtual currencies entirely, apparently stating that “it is out of the question of banning bitcoin as it is not started by” a central bank.  He further observed that he viewed bitcoin as “more a kind of tradable and collectible asset, such as stamps rather than a payment currency.”  

E. Japan

Japan has taken a proactive role in regulating virtual currency business activities, through its 1) Fund Settlement Law, 2) Banking Act, and 3) Anti-money Laundering Laws, discussed below.

1. Funds Settlement Law

The Funds Settlement Law, aimed at protecting users of settlement services and enhancing the safety and efficiency of such systems, was recently amended to directly regulate virtual currency exchange operators (“VCEOs,” which includes domestic virtual currency exchange operators (“DVCEOs”) and foreign virtual currency exchange operators (“FVCEOs”). Amendments are scheduled to come into effect no later than June 3, 2017 (the “New Funds Settlement Law”).

VCEO Business, a term of art as defined by the New Funds Settlement Law, is a business that engages in any of the following:

1. Trading virtual currencies or exchanging virtual currencies with other virtual currencies.
2. Acting as a broker, intermediary, or agent for a.
3. Managing customer’s monies or virtual currencies as part of a. and b.

Under this Law, an entity, domestic or foreign, seeking to offer VCEO services in Japan is required to register with the Prime Minister. The statute assumes that any such business operating with respect to Japan from wheresoever is to be regulated. How one’s activities in Japan are evaluated for their regulatory applicability is not entirely clear, and even if Japanese presence is limited to online availability, there is a possibility that a VCEO business will nevertheless be caught within the Law’s regulatory scope, since exchange services are inherently continuous in nature and are aimed at a broad audience.

---

181 Charters Piley, Alibaba bans Bitcoin amid China crackdown, CNN Money Online (January 9, 2014).
182 Pete Rizzo, China’s Central Bank Governor: PBOC Won’t Ban Bitcoin, CoinDesk (April 11, 2014).
183 Id.
184 資金決済に関する法律; shikin kessai ni kansuru hōritsu, Law No. 59 of June 24, 2009 (the “Funds Settlement Law”).
185 Article 1 of the Supplementary Provision of 情報通信技術の進展等の環境変化に対応するための銀行法等の一部を改正する法律; jōhō tsushin gijutsu no shintenjō no kankyō henka ni taiō suru tame no ginkōhōtō no ichibu wo kaisei suru hōritsu, passed on May 25, 2016, Effective on June 3, 2016 (the “Act to Amend Laws in Response to Advancing IT Technology”); 平成 28 年 6 月 3 日付官報号外第 123 号 56 頁 (法律第 62 号).
186 Article 2, Paragraph 7 of the New Funds Settlement Law.
187 Article 63-2 of the New Funds Settlement Law.
188 江頭憲治朗=中村直人「論点体系会社法」6 97 頁。For this analysis, we have referred to literature regarding how the Companies Act would judge whether a foreign company would be required to register in Japan. If further confirmation on this point is desired, we may be able to seek the FSA’s opinion on a no-names basis.
In order for a FVCEO\textsuperscript{189} to be granted registration, it is necessary to have a local business office, as well as a locally residing representative.\textsuperscript{190} A FVCEO, unless registered under this Law, is explicitly prohibited from conducting marketing aimed at those in Japan.\textsuperscript{191} VCEOs who engage in digital currency exchange services without registration, whether foreign or domestic, are subject to criminal punishment of up to three years of imprisonment or three million yen in fines, or both.\textsuperscript{192}

Other registration requirements include having a sound financial standing (minimum capital requirements, net assets), as will be prescribed by the Cabinet Order,\textsuperscript{193} the structure for sound operational management, and other structures that ensure compliance with the Law.\textsuperscript{194}

Once registered, VCEOs (including FVCEOs), will be required to adhere to the following, among others\textsuperscript{195}:

1. Mandatory Customer Session. Upon entering into a contract, users must be given explanations on fees and other contractual terms (Article 63-10 of the New Funds Settlement Law).

2. Segregation of Funds and Auditing Requirements. VCEOs are required to segregate their own funds from the clients’, and to have a CPA\textsuperscript{196} periodically review such funds’ statuses (Article 63-11 of the New Funds Settlement Law).

3. Grievance Resolution. As a general rule, a VCEO will be required to contract with a designated VCEO ADR institution in order to resolve complaints (Article 63-12 of the New Funds Settlement Law).

4. Reporting Requirements. Registered VCEOs are required to record and preserve books and submit business reports to the Prime Minister (Article 63-13, Article 63-14 of the New Funds Settlement Law).

5. Supervision. Authorities will have the right to enter into the VCEOs facilities, issue Business Suspension Orders, and revoke registration, among other things (Article 63-15, Article 63-17 of the New Funds Settlement Law).

2. Banking Act:\textsuperscript{197} Fund-transmitting Transaction Business

Fund-transmitting transactions (\textit{kawase torihiki}) are licensed activities that are allowed to be carried out by banks and registered funds transfer service providers.\textsuperscript{198}

\textsuperscript{189} A FVCEO is defined as a digital currency exchange operator that operates in and is registered (or similarly regulated) under laws similar to the New Funds Settlement Law in a foreign country (Article 2, Paragraph 9 of the New Funds Settlement Law).

\textsuperscript{190} Article 63-5, Paragraph 1, No. 1 and No. 2 of the New Funds Settlement Law do not allow a FVCEO without a local office and a locally residing representative to be registered.

\textsuperscript{191} Article 63-22 of the New Funds Settlement Law.

\textsuperscript{192} Article 107 of the New Funds Settlement Law.

\textsuperscript{193} Relevant ordinances have not yet been promulgated.

\textsuperscript{194} The specific content is undefined.

\textsuperscript{195} DVCEOs under the New Funds Settlements Law is defined as any entity registered as such under Article 63-2. The Law assumes the FVCEOs will also be registered under Article 63-2 (see Article 63-5, Paragraph 1, No. 1 and 2). As such, a VCEO referenced under this Law would include FVCEOs which are also locally registered. Hence, FVCEOs would be subject to provisions applicable for DVCEOs.

\textsuperscript{196} Alternatively, a corporate auditor.

\textsuperscript{197} Article 4, Paragraph 1 and Article 2, Paragraph 2 No.2 of the Banking Act; Article 37 of the Funds Settlement Law; Money transmitters are only allowed to conduct such services for values of less than one million yen (Article 2 Paragraph 2, Article 3 and Article 37 of the Funds Settlement Law and Article 2 of the Funds Settlement Law Ordinance).

\textsuperscript{198} 最高裁決 13.3.12 刑集 55 巻 2 号 97 [___] (___) 称：「為替取引を行うこと」とは顧客から、隔地者間で直接現金を輸送せずに資金を移動する仕組みを利用して資金[___]移動することを内容とする依頼を受けて、これを引き受けること、又はこれを受け引けて遂行することをいう。
Fund-transmitting transactions are defined as “transactions achieved by agreeing to transmit funds at the request of a client by not directly transporting the money but by using a mechanism to transmit funds, or agreeing to do such and carrying it out.”

Because virtual currencies can potentially be used as a convenient and cost-efficient way to transfer funds, they may be viewed as fund-transmitting transaction services for users who intend such purposes. Virtual currencies are not regarded at this point as “funds,” and sending virtual currency, by itself, would not be seen as a fund-transmitting transaction. However, if a user deposits funds at a local bank account which are converted to virtual currency, and this virtual currency is transferred to a receiver’s digital account, which are then converted to fiat currency, taken as a whole, it may be argued that the sender is essentially transmitting funds to the receiver.

3. Anti-money Laundering Regulation: Act on the Prevention of Transfer of Criminal Proceeds (the "AMLA")

In line with the above revisions to the Funds Settlement Law, the AMLA was simultaneously amended to include VCEOs on the list of designated businesses required to implement measures to detect and report potential money laundering activities.

Like the New Funds Settlement Law, amendments to the AMLA ("Amended AMLA") will come into effect no later than June 3, 2017. Further detail is expected to be clarified by a cabinet order.

Specifically, designated businesses are required to conduct sufficient know-your-customer (KYC) procedures at the time of the account opening, collect and preserve KYC and transaction records, report suspicious transactions to the authorities, and have in place an institutional mechanism to effectively implement the above procedures.

V. Conclusion

As virtual currency business activities and related fintech companies emerge and develop, they will continue to present new and growing legal and regulatory challenges. The artistry for governments and regulatory authorities will continue to be to balance fostering responsible developments of innovative virtual currency technologies that will potentially bring significant benefits, with the need for an effective legal and regulatory framework that protects consumers, business, and the financial system.

---

199. 片岡前掲注15) 87頁。Anyone who offers fund-transmitting transaction services without a license or registration granted under the Banking Act or the Funds Settlement Law will be subject to criminal punishment of up to three years of imprisonment or three million yen in fines, or both (Article 61, paragraph 1, No 1; Article 64, Paragraph 1, No 4).

200. 片岡前掲注15) 87頁。

201. 片岡義弘 FinTech の現状と法的課題 (総論的試論) 」 NBL1073号(2016) 9頁。

202. 犯による収益の移転防止に関する法律; hanzai ni yoru shūeki no iten bōshi ni kansuru hōritsu, Law No. 22 of March 31, 2007 (the "AMLA").

203. There is no direct criminal punishment for non-compliance; however, if an entity continues to disregard its KYC and reporting obligations despite receiving a Business Improvement Order from the authorities, it may be subject to criminal punishment of up to two years of imprisonment or three million yen in fines (Article 17 and Article 24 of the AMLA).
This article is not intended to provide legal advice, and no legal or business decision should be based on its contents. If you have any questions about the contents of this article, please call your regular Fried Frank contact or the attorney listed below:

**Contact:**

**Washington D.C.**

V Gerard Comizio  
+1. 202.639.7450  
V.Gerard.Comizio@friedfrank.com