MERCATUS CENTER
George Mason University
Bridging the gap between academic ideas and real-world problems

PUBLIC INTEREST COMMENT

Comments to the New York Department of Financial Services on the Proposed Virtual Currency Regulatory Framework

Jerry Brito and Eli Dourado

New York Department of Financial Services
Submitted August 14, 2014
Comment period closes September 5, 2014

On July 17, the New York Department of Financial Services (DFS) released its proposed BitLicense regulatory framework for virtual currency firms. We congratulate Superintendent Benjamin M. Lawsky and the entire department for the forward thinking they have demonstrated by making New York the first state to carefully consider the need to accommodate virtual currency firms in its regulatory system. This is a historic occasion in the evolution of money, and it may well be remembered for centuries to come. On July 23, the proposed rules were published in the New York State Register, setting off a 45-day period for public comment.

The Technology Policy Program (TPP) of the Mercatus Center at George Mason University is dedicated to advancing knowledge of the impact of regulation on society. As part of its mission, TPP conducts careful and independent analyses employing contemporary economic scholarship to assess rulemaking proposals from the perspective of the public interest. Therefore, this comment on the DFS's proposed regulatory framework does not represent the views of any particular affected party or special interest group, but is designed to assist the department as it continues to lead the world in supporting the responsible adoption of this important new technology.

INTRODUCTION

As the Treasury Department's Financial Crimes Enforcement Network has found, certain virtual currency businesses are money service businesses.[1] Typically such money service businesses engage in money transmission and as a result must acquire a money transmitter license in each state in which they do business. State financial regulators around the country have been working to apply their existing money transmission licensing statutes and regulations to new virtual currency businesses.[2] In many cases, existing rules do not take into account the unique

1. US Department of the Treasury, Financial Crimes and Enforcement Network, "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies" (Regulatory Guidance, FIN-2013-G001, US Department of the Treasury, Washington, DC, March 18, 2013), http://fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html.
2. Conference of State Bank Supervisors, "CSBS Public Hearing Addresses Challenges and Opportunities Associated with Emerging Payments" (Press Release, May 16, 2014), http://www.csbs.org/news/press-releases/pr2014/Pages/pr-051614.aspx.

For more information, contact
Taylor Barkley, 703-993-8205, tbarkley@mercatus.gmu.edu
Mercatus Center at George Mason University
3434 Washington Boulevard, 4th Floor, Arlington, VA 22201

properties of recent innovations like cryptocurrencies. With this in mind, the department sought to develop rules that were "tailored specifically to the unique characteristics of virtual currencies."[3]

As Superintendent Lawsky has stated, the aim of this project is "to strike an appropriate balance that helps protect consumers and root out illegal activity—without stifling beneficial innovation."[4] This is the right goal and one we applaud. It is a very difficult balance to strike, however, and we believe that the BitLicense regulatory framework as presently proposed misses the mark, for two main reasons.

First, while doing much to take into account the unique properties of virtual currencies and virtual currency businesses, the proposal nevertheless fails to accommodate some of the most important attributes of software-based innovation. To the extent that one of its chief goals is to preserve and encourage innovation, the BitLicense proposal should be modified with these considerations in mind—and this can be done without sacrificing the protections that the rules will afford consumers. Taking into account the "unique characteristics" of virtual currencies is the key consideration that will foster innovation, and it is the reason why the department is creating a new BitLicense. The department should, therefore, make sure that it is indeed taking these features into account.

Second, the purpose of a BitLicense should be to take the place of a money transmission license for virtual currency businesses. That is to say, but for the creation of a new BitLicense, virtual currency businesses would be subject to money transmission licensing. Therefore, to the extent that the goal behind the new BitLicense is to protect consumers while fostering innovation, the obligations faced by BitLicensees should not be any more burdensome than those faced by traditional money transmitters. Otherwise, the new regulatory framework will have the opposite effect of the one intended. If it is more costly and difficult to acquire a BitLicense than a money transmission license, we should expect less innovation. Additional regulatory burdens would put BitLicensees at a relative disadvantage, and in several instances the proposed regulatory framework is more onerous than traditional money transmitter licensing.

As Superintendent Lawsky has rightly stated, New York should avoid virtual currency rules that are "so burdensome or unwieldy that the technology can't develop."[5] The proposed BitLicense framework, while close, does not strike the right balance between consumer protection and innovation. For example, its approach to consumer protection through disclosures rather than prescriptive precautionary regulation is the right approach for giving entrepreneurs flexibility to innovate while ensuring that consumers have the information they need to make informed choices. Yet there is much that can be improved in the framework to reach the goal of balancing innovation and protection. Below we outline where the framework is missing the mark and recommend some modifications that will take into account the unique properties of virtual currencies and virtual currency businesses.

I. TAKING INTO ACCOUNT THE UNIQUE ATTRIBUTES OF VIRTUAL CURRENCIES AND SOFTWARE-BASED INNOVATION

Virtual currencies—especially cryptocurrencies—represent the merging of the financial and software industries. Until now, finance has been dominated by a relatively small, exclusive group of elite bankers who earn enormous returns, often through implicit and even explicit taxpayer support in the form of bailouts. Although the software industry has also produced enormous wealth, its dynamics could not be more different. Software is one of the most inclusive fields on Earth: successful firms are started by college dropouts, by people working in their bedrooms, and by teenagers in the developing world. For the most part, the firms that succeed do so on the merits of their product, not through mastering the political system to secure taxpayer assistance.

---

3. New York State Department of Financial Services, "Notice of Intent to Hold Hearing on Virtual Currencies, Including Potential NYDFS Issuance of a 'BitLicense'" (Notice, Nov. 14, 2013), http://www.dfs.ny.gov/about/press2013/virtual-currency-131114.pdf.
4. New York State Department of Financial Services, "NY DFS Releases Proposed BitLicense Regulatory Framework for Virtual Currency Firms" (Press Release, July 17, 2014), http://www.dfs.ny.gov/about/press2014/pr1407171.html.
5. Jose Pagliery, "New York Unveils Bitcoin License Rules," *CNN Money*, July 18, 2014, http://money.cnn.com/2014/07/18/technology/bitcoin-license.

Bringing software industry dynamics to finance is good for the state of New York and for the world. If cryptocurrencies are allowed to flourish, we will witness an astounding democratization of one of the most insulated industries in America. Just as the personal computer, the World Wide Web, and the smartphone enabled an explosion of new applications on those platforms, cryptocurrencies are poised to facilitate a similar explosion. These new financial applications will help consumers not only by making existing financial services more affordable but also by creating entirely new and unforeseen categories of financial services. These new categories of service represent new benefits for consumers as well as new jobs, new profit opportunities for business, and new sources of economic growth.

To reap these benefits, it is important that the department approach the regulation of cryptocurrency firms with due sensitivity to the dynamics of software firms. Because the software industry is so different from the financial industry, those differences must be explicitly taken into account in the BitLicense framework. In some cases, these accommodations may represent a change in the way that the department has operated, but we maintain that the benefits justify the cost.

As the department has noted, cryptocurrencies are not simply better versions of traditional payment systems; they are different from traditional systems. The department's goal of taking into account cryptocurrencies' unique characteristics is the right approach. One of those unique characteristics is that payments need not be intermediated; they can operate *both* like traditional payment systems *and* like cash. This fact has important implications for approaching the regulation of virtual currencies. Overly burdensome regulation will simply cause users to transact in cryptocurrency in cash-like mode, which deprives users of the benefits in terms of security, reliability, and convenience that come from using an intermediary and deprives regulators of visibility into the mediated transactions.

For this reason, among others, the federal government has opted to impose Know Your Customer and Anti-Money Laundering obligations only on those financial transactions in which virtual currencies are exchanged for fiat currencies. We believe that this is an important principle that should be preserved at the state level. We note throughout this comment some other ways in which the unique characteristics of cryptocurrencies can be more carefully accommodated.

As now written, the proposed definition of Virtual Currency Business Activity is so broad that it potentially captures many activities that should not be subject to regulation. These activities do not require consumer protection, and their inclusion would seriously hamper innovation in the cryptocurrency space. By the same token, the exemptions for certain activities are too narrow. Exempting certain other activities would help make the definition of Virtual Currency Business Activity more practical.

1. Non-financial services

The ability to exchange digital tokens and write to a public ledger can be used for much more than payments, which are only the first application of blockchain technology. As a strictly financial regulator,[6] DFS should carefully define Virtual Currency Business Activity so that it excludes non-financial activities of virtual currency firms. The proposed definition captures virtual currency firms whose business is not primarily financial exchange or safekeeping but who use virtual currencies for purposes beyond the mere purchase and sale of goods and services. Two examples may illustrate the point:

1. Proof of Existence (proofofexistence.com) is a website that functions as a digital notary service. By calculating a cryptographic hash of a document and inserting this hash into Bitcoin's blockchain, the service is able to prove that a given document existed at a given time, even if Proof of Existence itself subsequently goes out of business. It accomplishes the insertion of the hash into the blockchain by performing a small transaction on behalf of consumers that contains the hash as metadata. Since a record of this transaction will be stored for eternity in Bitcoin's blockchain, it can be proved, when the document is later produced, that the document existed at least as early as the time stamped on the transaction.

6. New York Financial Services Law § 30z2.

For this service, Proof of Existence charges an additional fee to consumers. A single use of the service, therefore, consists of two transactions: one in which consumers pay the firm, and a second in which the firm, on behalf of consumers, executes a tiny Bitcoin transaction that inserts the hash into the record. (Recent transactions of this type have been for the equivalent of $0.06, which is paid not to a known recipient but rather to whichever miner discovers the block.) The proposed framework exempts Proof of Existence for the first transaction under section 200(c)(2), but the second transaction appears to constitute non-exempt Virtual Currency Business Activity. This transaction, although executed on behalf of consumers, is *incidental to providing a non-financial service*, the permanent recording of a cryptographic hash in Bitcoin's blockchain.

2. Namecoin is a cryptocurrency that (among other things) functions as an Internet domain name registry for the .bit top-level domain. Holders of Namecoin can execute transactions that register, update, and transfer domain names that can be used, e.g., to browse websites on a suitably configured computer. Suppose a firm operated in the business of managing .bit domain names for consumers. Such a firm would hold balances of Namecoin on behalf of consumers and execute transactions on their behalf to facilitate domain name registrations, updates, renewals, and transfers. However, a Namecoin registrar would engage in such activities only *incidentally to providing a nonfinancial service*, the recording and updating of names and data in the Namecoin blockchain.

To be sure, Namecoin tokens have some value, and there is nothing stopping a person or firm from using Namecoin for financial purposes. However, insofar as virtual currency firms are not materially engaging in financial uses of virtual currency, they should not be considered to be engaging in Virtual Currency Business Activity for purposes of this regulation. Failure to cabin the definition to exclude non-financial purposes would severely hamper innovation in blockchain technology.

2. Mining and mining pools

Current definitions and exemptions make it unclear whether individual cryptocurrency miners would be required to obtain a BitLicense. Miners perform an important function within the cryptocurrency ecosystem. They help secure the blockchain against attempts to fraudulently double-spend coins. To protect consumers, therefore, the law should not encumber the entry of miners into the industry in any way.

We do not believe that the department intends to regulate individual cryptocurrency miners, but the current language of the regulation does not make that perfectly clear. For example, since miners earn coins and then often sell them to others, does mining count as a Virtual Currency Business Activity under section 200.2(n)(3)? This depends on the meaning of "customer business," which is not defined in section 200.2. In addition, since mining helps "secure" the blockchain, are they engaged in Virtual Currency Business Activity under section 200.2(n)(2)? To dispose of these questions, it would make sense to explicitly exclude mining from Virtual Currency Business Activity.

Mining pools are also an important part of the cryptocurrency ecosystem. They help individual miners insure against the stochastic nature of mining revenues, therefore encouraging the entry of miners and making the whole system more secure. The dynamic formation, growth, and shrinking of mining pools also helps regulate the total mining power that any one pool has. This makes it imperative that mining pool formation be unencumbered by law.

Mining pool administrators pay their members several times per day. There is a short period during which they are custodians of coins on behalf of their members, and then they transmit those coins to their members. This would appear to qualify mining pool administration as a Virtual Currency Business Activity.

It would be a mistake to regulate mining pool administrators under this framework. Participants in the mining process are sophisticated actors who do not need protection from the department. And since mining, whether based on proof of work, proof of stake, proof of burn, proof of resource, or yet-to-be-devised proof schemes, is the

lynchpin that holds together all decentralized cryptocurrencies, regulators should proceed with extreme caution in encumbering the mining ecosystem. Consequently, the definition of Virtual Currency Business Activity should be reformulated to include a broad exclusion of mining activity.

3. Software wallet providers

Wallets are systems for holding and managing virtual currencies through the safe storage of the public and private keys associated with virtual currency balances. One cannot be said to have full custody of certain virtual currency units unless one has control of both the public and private keys. Wallets can be hosted by a third party or can be fully managed by the end user. **Web wallets**, such as Coinbase, are hosted services that fully manage both the public and the private keys for the user; the user does not have access to the keys at all. As a result, Coinbase is a custodian of their users' funds. In contrast, **software wallet** providers, such as the Electrum project, distribute software that allows users to manage their own public and private keys themselves. As a result, software wallet providers never have custody of user funds; they merely provide software that allows users to hold and manage their own funds.

Software wallet providers do not have access to virtual currency keys, but it is unclear whether they are nevertheless implicated by section 200.2(n)(2) because they are necessarily involved in providing security features for the software the consumer uses to manage virtual currency balances. Since "securing . . . Virtual Currency on behalf of others" is a Virtual Currency Business Activity, must software wallet providers be required to apply for a BitLicense? We say no. Software wallet providers can never control the virtual currency handled by the software, so there is no need for the capital requirements, bonding, or other consumer protection the framework provides.

There are further ambiguities in this part of the definition. Blockchain.info, a software wallet, uses a model in which an encrypted version of the wallet is hosted on their website but in which decryption happens completely on the user's computer. At no point in the process can Blockchain.info access the virtual currency that it hosts. Should Blockchain.info and services like it be considered custodians and therefore firms engaged in Virtual Currency Business Activities? Because these services never have unencrypted access to the keys necessary to transmit the currency, they should not.

An even more complicated case is raised by **multisignature wallets**. A Bitcoin address can be set up to require any two out of a possible three signatures to conduct a transaction. This ability has many applications, especially for securing funds. For example, an end user could store two keys in separate locations and keep the third in the custody of a firm. This way, the firm would not have access to the funds, but in the event that the end user lost one of his two keys, he could ask the firm to sign a transaction to move the funds to a new wallet. This case is interesting because the firm never has custody of the funds but nevertheless is *involved* in the custody of the funds in a way that improves end-user security.

To address the concerns raised in this section, we suggest editing section 200.2(n)(2) to read:

> (2) ~~securing, storing, holding, or~~ maintaining **full** custody or control of Virtual Currency on behalf of others;

This change would clearly exempt software wallet authors from regulation under this part, as well as firms that offer to facilitate end-user custody of virtual currency without firms having direct access to it.

Exempting software providers is common practice. FinCEN, for example, expressly exempts from its money transmitter rules a person who "provides the delivery, communication, or network access services used by a money transmitter to support money transmission services,"[7] which has generally been interpreted as encompassing providers of software that is used in money transmission. Software providers are exempted from other financial rules as well, where another party has the customer relationship. For example, federal, New York, and many other state laws prohibit deposit taking without a banking license. Yet those who provide deposit-processing software

7. 31 C.F.R. § 1010.100(ff)(5)(ii)(A).

(e.g., support apps that let you take pictures of checks to deposit them) have never been considered "banks" or "deposit takers" under New York or federal banking law.

4. The exemption for consumer and merchant use of Virtual Currencies is too narrow

Section 200.3 (c) of the proposed framework rightly exempts "merchants and consumers that utilize Virtual Currencies solely for the purchase or sale of goods or services." That exemption, however, omits a wide array of possible consumer and merchant uses of Virtual Currencies.

At a basic level, a candidate for public office who wishes to accept Bitcoin donations in accordance with recent Federal Election Commission guidance,[8] or a citizen who wished to make a campaign contribution, would not be strictly utilizing Virtual Currency for the purchase or sale of a good or service. The same would apply to charities that accept Virtual Currency donations and benefactors who wish to donate.[9] Similarly, consumers may wish to use Virtual Currencies to send gifts to friends or family members, or parents may wish to use Virtual Currencies to give their children allowances. In each of these cases the parties would not be covered by the exemption as now written.

At a deeper level, consumers and merchants may wish to use Virtual Currencies for purposes other than simple value transfer. As we have explained above, because blockchains are essentially distributed ledgers, blockchain technologies can be put to myriad uses that are not simply fund transfers.[10] These include many different types of registration services for both financial and non-financial purposes. For example, Virtual Currency tokens may be used to securely control access to websites and computer systems, much as passwords are used today.[11] In the not too distant future, they may be used as the equivalent of a key that allows access to a hotel room or a rental car.[12] And digital tokens may also be used to represent discrete digital assets such as a copyrighted song that one can play or transfer, or even a stock certificate or other bearer instrument. In each of these cases it is possible that consumers and merchants are neither "purchasing" nor "selling" goods or services but instead using the Virtual Currency tokens to facilitate new types of digital transactions.

That the consumer and merchant exemption is narrow might not matter very much, except that the definition of Virtual Currency Business Activities requiring a BitLicense is very broad, as noted above. Because simply "transmitting"[13] Virtual Currency requires one to acquire a BitLicense, a vast array of consumer uses of Virtual Currency will be captured by the proposed framework. The ultimate goal of the proposed framework, however, is to protect consumers from potentially irresponsible actions by the intermediaries with which they do business. With that in mind, we recommend modifying the definition of Virtual Currency Business Activity in section 200.2(n)(1) to read:

> (1) receiving Virtual Currency for transmission or transmitting the same *on behalf of another;*

---

8. *See* Federal Election Commission, Advisory Opinion 2014-02, May 18, 2014, http://www.fec.gov/agenda/2014/documents/mtgdoc_14-24-b.pdf.
9. *See* Fred Wilson, "Bitcoin and Charities Were Made for Each Other, They Just Don't Know It Yet," *A V Club*, June 23, 2014, http://avc.com/2014/06/bitcoin-and-charities-were-made-for-each-other-they-just-dont-know-it-yet; Fred Wilson, *A Fred Talk for Good*, YouTube, July 17, 2014, http://www.youtube.com/watch?v=a9tsLOXNYDM (explaining the advantages Bitcoin promises for charities). *See also* Vitalik Buterin, "Charity Focus: Sean's Outpost," *Bitcoin Magazine*, April 2013, http://bitcoinmagazine.com/sandbox/seansoutpost.pdf (profiling Sean's Outpost, a homeless-outreach organization located in Pensacola, Florida, that has been providing meals and toiletries to Pensacola's neediest solely with bitcoins).
10. Jerry Brito, Houman Shadab, & Andrea Castillo, *Bitcoin Financial Regulation: Securities, Derivatives, Prediction Markets, and Gambling*, forthcoming from the New York Law School Working Paper Series, *available at* http://ssrn.com/abstract=2423461.
11. *See* Jeff Garzik, *Bitcoin core dev: websites do not need passwords*, Reddit, October 2, 2013, http://www.reddit.com/r/Bitcoin/comments/1nkoju/bitcoin_core_dev_websites_do_not_need_passwords; Eric Martindale, "BitAuth, for Decentralized Authentication," *Bitpay*, July 1, 2014, http://blog.bitpay.com/2014/07/01/bitauth-for-decentralized-authentication.html.
12. *See* Stan Higgins, "Authentication Protocol BitID Lets Users 'Connect with Bitcoin,'" *CoinDesk*, May 7, 2014, at http://www.coindesk.com/authentication-protocol-bitid-lets-users-connect-bitcoin; *The Economist*, "Hidden Flipside: How the Crypto-currency Could Become the Internet of Money," March 15, 2014, available at http://www.economist.com/news/finance-and-economics/21599054-how-crypto-currency-could-become-internet-money-hidden-flipside.
13. BitLicense Proposal § 200.2 (n)(1).

Adding "on behalf of another" limits the licensing requirement to only intermediaries providing a service to customers (thus satisfying the consumer protection purpose of the licensing requirement) while exempting simple consumer uses, including giving to charities and campaigns, using Virtual Currency tokens to unlock doors, and many other innovative uses that have yet to be developed. The press release that accompanied the department's release of the proposed BitLicense framework explained that "[t]he new DFS BitLicenses will be required for firms engaged in . . . Receiving or transmitting virtual currency *on behalf of consumers*[.]"[14] Limiting the definition to firms handling consumer funds is no doubt the department's intention, and it should therefore clarify the definition.

5. Requirement to collect physical addresses of all parties is impractical and counterproductive

Section 200.12(a)(1) requires licensees to keep records of all transactions, and for each transaction to note the "physical addresses of the parties to the transaction." Similarly, section 200.15(d)(1) requires that licensees, as part of their anti–money laundering programs, keep records of all transactions, including "the identity and physical address of the parties involved[.]" A requirement that licensees identify and gather the physical address of *all* parties to a transaction, not just that of their customers, would nullify some of the central advantages of cryptocurrencies like Bitcoin.

Bitcoin is an open network that anyone can join as long as one's software client follows the Bitcoin protocol. Open networks based on open protocols are the standard operating procedure of the Internet, and they account for its immense success. For example, anyone can set up an email server and send a message to anyone else with an address at another email server anywhere in the world, without any coordination between the two. As long as your client and server follow the open Simple Mail Transfer Protocol, you can email anyone in the world.

In contrast, early proprietary online services like Compuserve only allowed users to email other users of the same closed system. To send a message to a Compuserve customer, one had to also be a member of Compuserve. The same was true of text and graphical content. To view AOL pages in the early 1990s, consumers had to be a customer of AOL. Then came the rise of the World Wide Web, an interoperable open network built on open protocols. As long as users had Internet access and a web browser that followed the open protocols, they could view content from anywhere in the world without limitations.

The Internet's openness was a boon to consumers not only because it gave them access to other users and content anywhere in the world but also because it allowed innovators to create new services without first having to convince the Compuserves and AOLs of the world to allow them to do so. The open Internet model makes possible what Vint Cerf, the Father of the Internet, calls "permissionless innovation."[15] Tim Berners-Lee was able to launch the World Wide Web without waiting for Internet service providers to support it. Innovative Internet-based voice and video communication services like Skype, FaceTime, and Hangouts work as long as users on both ends use the same software. If Berners-Lee had to explain to a telecom executive what hypertext was in 1990 before he could create the web, it may never have happened. If we had to rely on telecom companies to provide video calling (AT&T experimented with it as far back as the 1960s), it would probably be more expensive and inferior to the video calling services we have today. Permissionless innovation means more innovation.

Requiring a closed, proprietary payments system, such as PayPal, to identify and note the physical address of parties to a transaction is feasible because all parties to a transaction will be customers of PayPal. Similarly, it may be feasible to require a closed network, such as a credit card network, to identify all parties to a transaction because the transacting parties will be customers of the card issuers, who in turn have a relationship with the credit card network operator. In contrast, it is not feasible to ask Virtual Currency businesses to do the same because, by virtue of operating on an open network, they do not have a relationship with all parties. A requirement that they identify all parties to a transaction is tantamount to prohibiting the use of an open network.

---

14. New York State Department of Financial Services, "NY DFS Releases Proposed BitLicense Regulatory Framework for Virtual Currency Firms" (Press Release, July 17, 2014) (emphasis added), http://www.dfs.ny.gov/about/press2014/pr1407171.html.
15. Vinton Cerf, "Keep the Internet Open," *New York Times*, May 24, 2012, http://www.nytimes.com/2012/05/25/opinion/keep-the-internet-open.html.

As one commentator put it, requiring that Virtual Currency businesses identify all parties to a transaction would be much like requiring Gmail or Yahoo! Mail to identify and gather the physical address of the recipients of the emails their customers send.[16] Because it would be impossible to comply with such a requirement on an open network, the result would likely be a reversion back to the days when you could only email others on the same closed network.

We could expect the same to happen to open cryptocurrency networks, such as Bitcoin, if the requirements in sections 200.12(a)(1) and 200.15(d)(1) remain unchanged. To comply with a requirement to identify all parties to a transaction, a Virtual Currency business could limit transactions to only be available between its own customers. That would make such businesses no different than proprietary systems such as PayPal. Alternatively, a Virtual Currency business could enter into agreements with other Virtual Currency businesses and create a closed network of identified customers, but this would simply replicate the existing credit card networks.

The department's rationale behind creating a BitLicense specific to Virtual Currencies is to take into account the "unique characteristics of virtual currencies" that make them such a potentially innovative technology. Sections 200.12(a)(1) and 200.15(d)(1) of the proposed framework, however, ignore the central feature that makes cryptocurrencies unique—their open architecture. A requirement that all parties to a transaction be identified would essentially make operating on an open network like Bitcoin impossible. This would in turn act as an effective mandate for BitLicensees to either operate closed proprietary systems or create closed networks on top of Bitcoin. Not only would this undercut the low-cost global reach of open cryptocurrency networks, which is one of their main advantages, but it would also remove the possibility that these networks will see the same flourishing permissionless innovation that has made the Internet a success. By requiring closed networks, the regulatory framework as written would reintroduce a system in which entrepreneurs looking to offer innovative new cryptocurrency services—whether financial in nature or not—would first have to acquire the permission of the closed networks' gatekeepers.

As written, sections 200.12(a)(1) and 200.15(d)(1) of the proposed framework would deal a heavy blow to innovation while doing little to protect consumers or improve anti-money laundering efforts. Determined criminals will always be able to transact directly with each other by avoiding BitLicensed intermediaries and connecting with each other in a peer-to-peer fashion. The purpose of the recordkeeping requirements, therefore, is to gain visibility into the money flows between different parties. To gain this visibility, however, it is only necessary to require BitLicensees to identify one party to a transaction: their customer.

For example, suppose that the BitLicense only required Virtual Currency firms to identify their own customers. To the extent that a customer of one BitLicensed firm conducts a Bitcoin transaction with the customer of another BitLicensed firm, then while the firms may not know the identities of their customers' counterparties, the department will still have complete visibility into both sides of the transaction because it has access to both firms' records. To the extent that a customer of a BitLicensed firm conducts a transaction with a party on the Bitcoin network not associated with another BitLicensed firm, then the department will still have partial visibility. With access to the identity of one side of the transaction, it can, if necessary, begin an investigation to uncover the other side.

In contrast, the proposed requirement to identify all parties to a transaction might lead to the department having *less* visibility of transactions on the Bitcoin network or any other open cryptocurrency network. This is because, as noted above, the consequence of such a requirement will likely be that Virtual Currency firms will be forced to operate closed systems on top of the Bitcoin network. While the department may have good visibility into the transactions conducted inside these closed networks, it will give up visibility into the broader open network. Again, a determined actor will always be able to avoid BitLicensed intermediaries and connect directly to the network in a peer-to-peer fashion. By segregating the BitLicensed businesses from the wider network, there will be no contact between identified customers and the wider network, and the department will lose visibility into that wider network.

16. Elizabeth Stark & Ryan Singer, "New York to Bitcoin Startups: Get Permission or Get Out," *TechCrunch*, July 21, 2014, http://techcrunch.com/2014/07/21/new-york-to-bitcoin-startups-get-permission-or-get-out.

6. Requirement that changes to business must be approved by the superintendent is onerous

Section 200.10 requires licensees to obtain permission from the superintendent before making a material change to their business. This section should be modified to accommodate the dynamics of the software industry, in which running a successful firm may require frequent and sudden pivots to new business models. Indeed, it is unlikely that Silicon Valley would even exist today if entrepreneurs had to receive written approval from regulators every time they wanted to make a material change to their business model. The industry has thrived on permissionless innovation.

In contrast, the New York State Transmitter of Money License contains no requirement to seek written approval before making a material change. This disparity places Virtual Currency firms at a significant disadvantage compared to traditional money transmitters, which seems like a step backward. Since traditional money transmitters have operated for years with no requirement to seek approval for material changes, the department should reconsider whether it wishes to impose such strict requirements on Virtual Currency firms. For the sake of parity, this section of the framework should be stricken.

If the department insists on proceeding with this line of regulation, it could achieve many of the same objectives of the requirement at significantly less burden to firms if it would replace prior written approval with the simple requirement to notify the department within 45 days of any material change. This change would still impose a significant burden on Virtual Currency firms, but it would at a minimum a) create a stronger presumption that rapid iteration on business ideas is acceptable and b) decrease the risk to firms that a backlog at the department would delay the timeframe for execution. Given the frequency of business model changes in the software industry, the risk of such a backlog is substantial, no matter how efficient the department's paperwork processing operation is.

Another concern with this section is that the definition of "material change" in section 200.10(b) is unclear. In particular, section 200.10(b)(1) appears to define a "material change" as one that would render a product, service, or activity "materially different" from that included on the licensee's application. This does not provide much certainty to licensees as to what is material and what is immaterial. Section 200.10(b)(1) should be stricken and the framework should rely exclusively on subsections (2) and (3) for the definition of "material change," which should be adequate to address the department's concerns.

To reiterate, section 200.10 substantially disadvantages Virtual Currency firms relative to traditional money transmitters, and our primary recommendation is that this section be deleted. In the event that the department declines to remove section 200.10, our other recommendations seek to reduce the compliance burden for Virtual Currency firms in light of the fact that the software industry necessitates rapid iteration of business models to arrive at successful, socially beneficial innovations.

7. Not all transaction obfuscation should be prohibited

Unlike traditional payment systems, cryptocurrencies are inherently public. All transaction data is recorded in a database that is, by necessity, legible to the world. This transparency means that "out of the box," naïve users have very little financial privacy. For example, if a user posts a Bitcoin receiving address online and says that it is his, the whole world is able to see exactly how many bitcoins he has received at that address. Anyone can then follow those coins throughout the network to determine, in many cases, what the user spent them on.

The developers of cryptocurrency protocols have come up with several techniques and best practices to ensure that consumer financial privacy is preserved. These include (1) generating a new receiving address for each payment and (2) collating transactions to and from multiple parties into a single network transaction so that it is not obvious who is paying whom. Both of these steps are necessary to ensure that the general public is not able to de-anonymize the network and breach accepted norms of individual financial privacy. Additional best practices may be developed in the future.

Section 200.15(f) states that BitLicensees are not obligated to disclose transactions to the general public, but it remains unclear under the current text whether they may affirmatively take steps to protect their customers from

public scrutiny. Obfuscation that is aimed at something other than evading BitLicense reporting requirements should remain permissible.

8. Framework should clarify that issuance of new decentralized cryptocurrencies is not covered

The definition of covered Virtual Currency Business Activity in the proposed framework includes "controlling, administering, or issuing a Virtual Currency."[17] This has been interpreted by some commentators to mean that the activity of writing and publishing software that undergirds a decentralized virtual currency would fall under this definition and that such an activity would have to be licensed. It is doubtful that this is what the department intends, but it should nevertheless clarify the definition to avoid confusion.

In defining Virtual Currency, the department rightly makes the distinction between centralized and decentralized virtual currencies.[18] It is only centralized digital currencies that can be said to be "controlled, administered, or issued" by a central authority. Indeed, the key feature of decentralized virtual currencies is that there is no central authority that "controls, administers, or issues" the currency. For example, while Bitcoin has no central administrator that controls the number of bitcoin currency units or issues them, companies like Perfect Money, or the now-defunct Liberty Reserve, do in fact administer, control, and issue their currencies.

As a result, Section 200.2(n)(5) of the proposed framework can only possibly apply to *centralized* virtual currencies that are issued and administered by a central authority. The alternative—that merely writing and publishing code would be subject to licensing—would not stand First Amendment scrutiny,[19] and it cannot be what the department intended. The confusion can be clarified by adding the word "centralized" to the definition in section 200.2(n)(5) so that it would read:

> (5) controlling, administering, or issuing a *centralized* Virtual Currency.

9. Exchanges between two cryptocurrencies should be exempt

Section 200.2(n)(4) includes as Virtual Currency Business Activity performing retail "conversion or exchange of one form of Virtual Currency into another form of Virtual Currency." However, as discussed above, some cryptocurrencies are not primarily used for financial purposes but rather as a way to claim non-financial goods or services on a network. Namecoin, discussed above, is used to facilitate the purchase of .bit domain names, among other resources. Filecoin is a new proposal to offer cloud storage services on a decentralized basis.[20] Exchanging bitcoins for namecoins or filecoins, therefore, is more like a retail transaction than a financial one: the user is buying tokens that entitle them to some amount of naming or file storage. Consequently, such Virtual Currency-to-Virtual Currency exchanges should not be subject to BitLicense requirements.

10. Creating an on-ramp for startups

Whereas traditional financial firms usually begin with a well-conceived business plan, immediate financial backing, and a large team of attorneys and compliance officers, software firms are often started by one person tinkering in his or her bedroom. They often launch with a "minimum viable product" that still requires significant market testing.[21] Software firms frequently "pivot" to new business models when early iterations of the product or service fail.

This dynamic has implications for regulators. While it is important to protect consumers, it is equally important to foster a climate that welcomes entrepreneurs and innovation. Without the ability to rapidly iterate over new business models, it will be impossible for firms to discover what the market opportunities are. The proposed rules

17. BitLicense Proposal § 200.2(n)(5).
18. BitLicense Proposal § 200.2(m).
19. See Bernstein v. US Department of Justice, 176 F.3d 1132 (1999) (finding that software source code is speech protected by the First Amendment and government restrictions on its publication are unconstitutional).
20. See Filecoin: A Cryptocurrency Operated File Storage Network (White Paper, July 15, 2014), http://filecoin.io/filecoin.pdf.
21. "Minimum viable product," *Wikipedia*, https://en.wikipedia.org/wiki/Minimum_viable_product. Accessed August 12, 2014.

do not take this need into account. A balanced approach is needed to ensure that new virtual currency firms do not have the same compliance expenses that the world's largest financial firms have on day one of their existence.

One approach to striking this balance would be to create a regulatory "on-ramp" for startups. The framework could exempt, under section 200.3(c), firms that process less than $5 million annually in virtual currencies or that hold for safekeeping less than $1 million at a time. New applicants could also be offered a safe harbor that would allow them to operate while their license applications are pending as long as they register with federal money laundering authorities, certify that they are well capitalized, and don't attract consumer complaints. The department could also require small firms to clearly disclose their probationary status and post a standard bond pegged to the volume of business they do.

More general antifraud provisions of law would continue to protect the public from deliberate malfeasance by startups even if they are operating under the on-ramp exemption. As a result, this on-ramp would facilitate experimentation with new ideas without posing significant risk to consumers.

II. BITLICENSE MUST BE NO MORE BURDENSOME THAN MONEY TRANSMISSION LICENSING

One of the main reasons for developing a new BitLicense framework is that the existing money transmitter licensing framework, which might otherwise have applied to virtual currency businesses, did not take into account the unique characteristics of virtual currencies. As a result, its application could have hampered new financial innovation and the development of the nascent virtual currency industry. If it is to meet this goal, however, the new BitLicense cannot be more burdensome in its requirements for virtual currency businesses than the existing money transmitter licensing framework would be. We have already noted some serious disparities above. Below we outline several other ways in which BitLicensees potentially face an uneven playing field relative to money transmitters.

1. Businesses should only be required to acquire one license

At the outset, we should note that it is not clear whether a BitLicense is required of virtual currency businesses *instead* of a money transmitter license or *in addition to* such a license. While the department's intention is no doubt the former, it should clarify this question to avoid any confusion.

New York law requires that anyone engaged in "the business of receiving money for transmission or transmitting the same" must have a license issued by the superintendent.[22] Courts are increasingly coming to the conclusion that virtual currencies such as Bitcoin qualify as "money" under various statutory definitions.[23] The department should therefore clarify that a BitLicense satisfies the statutory licensing requirement for money transmission.[24]

2. Requirement to submit fingerprints of all employees is onerous

Pursuant to New York Banking Law Section 22, applicants for money transmitter licenses must submit fingerprints with their application.[25] In contrast, applicants for a BitLicense must submit not just their fingerprints, but also those of "each Principal Officer, Principal Stockholder, and Principal Beneficiary of the applicant, as applicable, and for all individuals to be employed by the applicant," as well as a photograph of each person.[26] This has the potential to be an unnecessary burden on virtual currency businesses.

---

22. New York Banking Law § 641.
23. See Securities and Exchange Commission v. Shavers, No. 4:13-CV-416 (E.D. Tex. Aug. 6, 2013) & United States vs. Ross William Ulbricht, No. 1:14-CR-00068 (S.D.N.Y. July 9, 2014) (each finding that bitcoins qualify as "money" for purposes for the statutes being enforced in each case).
24. To require two licenses would make it essentially impossible for small- to medium-sized entrepreneurs to enter the market.
25. New York Banking Law § 22.
26. BitLicense Proposal § 200.4(a)(5).

Some Virtual Currency firms will be startups with a few dozen employees, many of whom will be graphic designers, web developers, receptionists, and the like and will have no influence over, or relation to, the company's financial soundness. Requiring that all employees submit to identification requirements will be a burden on such small businesses. On the other hand, it is conceivable that some very large companies, such as Facebook or Google, will enter the virtual currency business. As written today, the proposed rules would require that their thousands of employees submit fingerprints and photographs.

The better approach would be to maintain as much parity as possible with the requirements of a money transmitter license. Only applicants should be required to submit fingerprints.

3. Capital requirements create an uneven playing field relative to money transmitters

Section 200.8 of the proposed framework sets forth a minimum capital requirement for BitLicensees. This is in addition to the requirement that licensees have full reserves to cover any Virtual Currency deposits held in custody for customers, and in addition to the requirement that licensees maintain a bond or trust account for the benefit of its customers.[27] Money transmission licensees have no such minimum capital requirement, putting BitLicensees at a relative disadvantage.

In many ways, the proposed BitLicense lumps together into one regime requirements that normally apply individually to banks, money transmitters, broker-dealers, and possibly other institutions. This means that to hold a BitLicense, a company needs to, for example, set aside capital (banks and broker-dealers), collect customer information (banks), post a bond and not lend customer funds (money transmitters), and disclose risk factors to customers (broker-dealers). We are aware of no other financial product regulatory scheme that applies all of these requirements to a single business activity. This is potentially quite onerous and may inhibit entrepreneurship in the virtual currency space. To the extent possible, requirements should share as much parity as possible with money transmission licensing.

BitLicensees would also be permitted to invest their retained profits in only certain approved investments denominated in United States dollars.[28] Not only would this prevent licensees from investing in the very virtual currencies on which their businesses are based, but it also forecloses any number of other safe investment vehicles. For example, a European company that acquires a BitLicense would not be permitted to invest in Euro-denominated German government bonds. Transmitter of money licensees face no such restrictions, putting BitLicensees at a relative disadvantage. Instead, what constitutes a permissible investment for money transmitters is based on the market value or net carrying value of their investments.[29] The requirement is simply that these investments must be equal to at least the aggregate amount of all outstanding payment instruments and traveler's checks[30] and the market value must be at least 80 percent of the net carrying value.[31]

Through full reserve requirements, bonding, and flexible permissible investment requirements, the department can accomplish its goal of protecting consumers from unsound businesses while at the same time fostering a level playing field among regulated entities. It should modify its capital requirement and permissible investment requirements to match the more reasonable ones faced by money transmitters.

4. Some requirements do not seem cabined to financial transactions

The department's authority to regulate Virtual Currency firms stems from New York's Banking Law, which gives the superintendent the authority to supervise and regulate financial products and services.[32] The proposed regulatory framework, however, has certain requirements that seem to stray beyond

27. BitLicense Proposal § 200.9.
28. BitLicense Proposal § 200.8(b).
29. New York Banking Law § 651
30. *Id*.
31. *Id.*
32. New York Financial Services Law § 302.

these bounds. And these proposed requirements for BitLicensees are not similarly applicable to licensed money transmitters.

First, while applicants for transmission of money licenses must submit to the department their written policies and procedures related to money transmission and AML,[33] applicants for a BitLicense are required to submit *all* written policies and procedures for the firm—not just those related to virtual currency operations.[34] This disparate treatment is onerous and there is little discernable justification for it. The requirement for BitLicense applicants should be limited to policies related to their Virtual Currency Business Activity and AML.

Second, a similar disparity exists when it comes to access of books and records. Both licensed money transmitters (under current law) and BitLicense holders (under the proposed framework) must grant to the department access to their books and records. However, in the case of money transmitters the department's access is limited to records relating to money transmission.[35] In contrast, there is no limitation to the type of record to which BitLicensees must grant the department immediate access.[36] This disparity can be remedied by limiting the records to which the department may demand immediate access to records related to Virtual Currency Business Activity and AML. To the extent the department requires access to other records in the course of an investigation or otherwise, it can always obtain that access through a subpoena or warrant.

5. BitLicense anti-money laundering requirements reach much further than money transmitter license

To obtain a license, money transmitters must simply demonstrate that they have an anti-money laundering program that complies with applicable federal anti-money laundering laws.[37] In contrast, BitLicensees have very specific requirements that exceed simply meeting federal requirements. For example, they must report transactions that in the aggregate exceed $10,000 in one day by one person and notify the department within 24 hours,[38] and they must identify all parties to a transaction (as discussed above), which is not required of money service businesses. There is also a new state suspicious activity reporting requirement that goes beyond the federal requirements.[39] These requirements are incredibly onerous on Virtual Currency firms, especially if other states take New York's lead and implement similar requirements. Again, these additional requirements put BitLicensees at a relative disadvantage to money transmitters, as well as other firms, with no discernable justification for the increased regulation.

6. Department should clarify chartered banks exemption

A plain reading of section 200.3(c)(1) suggests that traditional banks licensed to operate in New York may legally engage in Virtual Currency Business Activity if they receive the approval of the superintendent and that such banks are exempt from the provisions of the BitLicense, such as the prohibition on keeping less than 100 percent reserves under section 200.9. Nevertheless, this laudable exemption raises two matters that deserve clarification.

First, under what terms will the superintendent offer approval to persons chartered under the New York Banking Law to engage in Virtual Currency Business Activity? Banks are already subject to such extensive scrutiny that additional review of their Virtual Currency plans seems excessive. The framework should instead reverse the presumption and declare banks eligible to engage in Virtual Currency Business Activity without an additional license unless specifically disallowed by the superintendent.

Second, it is important for the future of the Virtual Currency ecosystem that at least some entities are empowered to hold deposits at fractional reserve. A plain reading of the section suggests that banks, in view of their charter

33. Money Transmitter License Application Instructions, §§ E & K, http://www.dfs.ny.gov/banking/ialfmti.htm.
34. BitLicense Proposal § 200.4(a)(10).
35. 3 New York Codes, Rules, and Regulations § 406.9(c)
36. BitLicense Proposal § 200.12(b).
37. 3 New York Codes, Rules, and Regulations § 416.
38. BitLicense Proposal § 200.15(d)(2).
39. BitLicense Proposal § 200.15(d)(3).

under the Banking Law and not under this framework, are not bound by the custodial limitations set out in section 200.9. If that were not the case, it would raise serious concerns.

CONCLUSION

To ensure that the final regulations do the most they can to protect virtual currency innovation while also protecting consumers, we urge the department to solicit a second round of comments once it incorporates the changes resulting from the current round. Although the New York State Administrative Procedures Act does not require a second round, additional engagement with stakeholders will produce better regulations than one round alone. An additional 45-day window for comments should be sufficient for commenters to suggest final changes to the new draft regulations.

As we have noted, the current draft regulations miss the mark in two ways. First, although they laudably take into account some of the unique characteristics of virtual currency firms, they do not accommodate some other important aspects of new cryptocurrency technology. We have suggested some ways in which the proposed regulations could be improved in this regard. Second, BitLicense compliance should be no more burdensome than that of transmission of money licenses. We have noted several of the differences between these two kinds of licenses, and we ask the department to reconsider those aspects that make the virtual currency regulations more burdensome.

Again, we congratulate Superintendent Lawsky and the Department of Financial Services for their forward thinking, their willingness to engage the virtual currency community, and their hard work on these regulations. With the changes we have outlined, New York is sure to become a major hub for virtual currency innovation. But New York is not the only jurisdiction competing to capture the benefits of such innovation. The United Kingdom is evaluating virtual currencies with an eye toward wooing new firms. "With the right backing from government, I believe we can make London the fintech capital of the world," said U.K. Finance Minister George Osborne.[40] Therefore, we urge the department to carefully consider the right balance between consumer protection and innovation.

40. Matt Clinch & Katrina Bishop, "London Aims to Become a Bitcoin Hub," *CNBC*, August 6, 2014, http://www.cnbc.com/id/101897995.