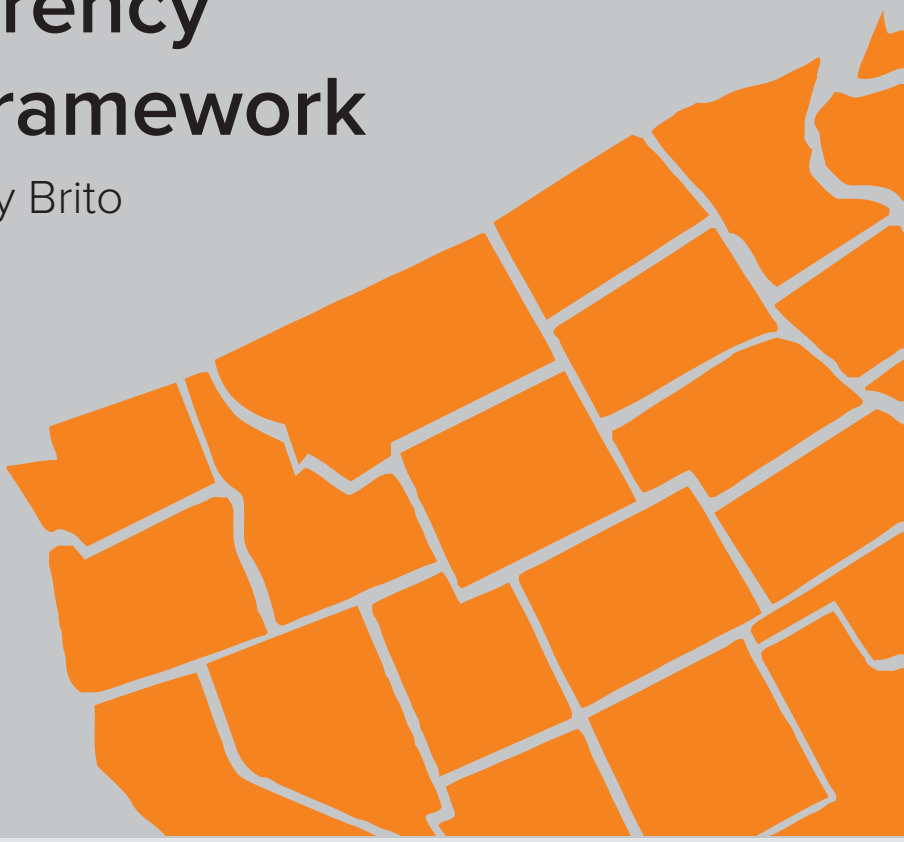
State Digital Currency Principles and Framework

Peter Van Valkenburgh & Jerry Brito

Version 1.3
Oct. 2015



Coin Center Report

COIN CENTER
coincenter.org

Peter Van Valkenburgh and Jerry Brito, *State Digital Currency Principles and Framework v1.3*, Coin Center Report, Oct 2015, available at https://coincenter.org/2015/04/state-principles-and-framework/

Abstract

States have begun to look at how digital currencies, such as Bitcoin, and the businesses that utilize them to provide consumer products, interact with money transmission and consumer protection policy. This report offers model language for a *sui generis* statute or implementing regulation. It is not a draft or model bill in full. Instead, language is offered for the essential components of any digital currency law: *who must be licensed, how are start-ups encouraged, how is solvency guaranteed, etc.*. This report can also be used as an aid in the process of amending existing money transmission statutes, particularly where simple amendments to definitions could prove vague and under- or over-inclusive.

Author

Peter Van Valkenburgh
Director of Research
Coin Center
peter@coincenter.org

Jerry Brito
Executive Director
Coin Center
jerry@coincenter.org

About Coin Center

Coin Center is a non-profit research and advocacy center focused on the public policy issues facing cryptocurrency technologies such as Bitcoin. Our mission is to build a better understanding of these technologies and to promote a regulatory climate that preserves the freedom to innovate using blockchain technologies. We do this by producing and publishing policy research from respected academics and experts, educating policymakers and the media about blockchain technology, and by engaging in advocacy for sound public policy.

Introduction

States have begun to look at how digital currencies, such as Bitcoin, and the businesses that utilize them to provide consumer products and services, interact with money transmission and consumer protection policy. Texas[1] and Kansas,[2] for example, have published guidance explaining that third-party bitcoin exchanges *do* engage in money transmission and therefore must be licensed as money transmitters with state authorities. New York, by contrast, has decided to place digital currency businesses under a separate regulatory regime from traditional money transfer and has crafted a so-called, "BitLicense."[3]

Developing *sui generis* digital currency statutes or regulation is difficult, however. Without carefully chosen language and an understanding of the underlying technology, the regulatory regime could fail to provide much needed certainty to innovative companies, fail to protect consumers, and instead stifle the economic growth, new jobs, financial inclusion, and business transparency that these technologies promise.

This report offers model language for a *sui generis* statute or implementing regulation. It is not a draft or model bill in full. Instead, language is offered for the essential components of any digital currency law: *who must be licensed, how are start-ups encouraged, how is solvency guaranteed, etc.*

This report can also be used as an aid in the process of amending existing money transmission statutes, particularly where simple amendments to definitions could prove vague and under- or over-inclusive. To illustrate, formally re-defining "money" within a statute to include digital or virtual currencies would not be sufficient to guarantee efficient regulation of these new technologies. One must also define what it means to "transmit" a digital currency or be a "digital currency transmitter." Traditional money transmission occurs when an intermediary reassigns credits or debits among its customers or partner institutions. These institutions have free reign to assign and reassign credit to different accounts, subject to applicable legal restrictions, as long as they remain solvent at the end of the day. By contrast, bitcoins, for example, can *only* be transmitted by the holders of unique cryptographic keys. Therefore, only a business that holds these keys could ever have the ability to transmit a bitcoin. A transmittal instrument for a digital currency is not, then, a *promise* to pay; it is the *ability* to pay—*i.e.* cash on hand—as measured by possession or knowledge of cryptographic keys sufficient to execute or prevent a transaction.

---

[1] Texas Department of Banking, Supervisory Memorandum - 1037 Regulatory Treatment of Virtual Currencies Under the Texas Money Services Act (Apr. 2014) *available at* http://www.dob.texas.gov/public/uploads/files/consumer-information/sm1037.pdf.

[2] Kansas Office of the State Bank Commissioner, Regulatory Treatment of Virtual Currencies Under the Kansas Money Transmitter Act (June 2014) *available at* http://www.osbckansas.org/mt/guidance/mt2014_01_virtual_currency.pdf.

[3] *See* New York Department of State Department of Financial Services, New York Codes, Rules and Regulations Title 23. Department of Financial Services Chapter 1. Regulations of the Superintendent of Financial Services Part 200. Virtual Currencies (Jan. 2015) *available at* http://www.dfs.ny.gov/legal/regulations/adoptions/dfsp200t.pdf.

For example, a bill has been introduced in Pennsylvania to amend its money transmission licensing statute in an attempt to cover digital currency transmission.[4] In an early draft, "virtual currency" was added to the definition of "money."[5] The definition of "transmittal instrument" was amended to include "electronic transfer . . . for the payment of money."[6] "Electronic transfer," however, was not defined. Were this draft bill to pass in that form, we might reasonably expect a dispute to arise and a judge to interpret the definition in a reasonable manner; however, it seems inefficient to leave such an important distinction to an *ex post*, judicial or administrative process. Instead, Pennsylvania should be clear when certain business activities *are* digital currency transmissions and when they are not. Pennsylvania should adopt the definition of "digital currency transmission" found in Part 1, below, and revise their definition of "transmittal instrument" to include "digital currency transmission" rather than—or in addition to—"electronic transfer."

For use in either *sui generis* or amending legislation, these model excerpts are explained piece by piece in the following sections. While all sections are important to consider when regulating these new technologies, *the discrete policy points in this framework are generally laid out in order of importance.*

[4] Pennsylvania House Bill 850 (March 26, 2015) *available at* http://www.legis.state.pa.us/CFDOCS/Legis/PN/Public/btCheck.cfm?txtType=PDF&sessYr=2015&sessInd=0&billBody=H&billTyp=B&billNbr=0850&pn=1029

[5] *Id.* at 3-4.

[6] *Id.* at 4.

1. Defining Digital Currency Transmission

In its policy statement on state virtual currency regulation, the Conference of State Bank Supervisors has clearly set out the normative case for consumer protection regulation of digital currencies:

> [M]any virtual currency services are clearly focused on consumer financial services. Such virtual currency service providers are in a position of trust with the consumer, which creates a public interest to ensure activities are performed as advertised with appropriate minimum standards to minimize risk to consumers.
>
> It is CSBS policy that entities performing activities involving third party control of virtual currency should be subject to state licensure and supervision like an entity performing such activities with fiat currencies.[7]

Digital currency presents a challenge to regulators because digital currency can be utilized to perform activities involving third party control—activities that have long been performed with fiat currencies. However, unlike prior electronic financial tools, digital currency can also be used for other unrelated purposes. It can be used by businesses to offer a financial service without having control of the customer's funds; it can be used by intermediaries to offer a non-financial service (such as a notary service); and it can be used by consumers directly and entirely without intermediaries.

Undoubtedly, some consumers will ask an intermediary to store and transmit their digital currency, and these intermediaries thereby assume a position of trust, which generates the basis for licensing and regulation. The key to developing such licensing and regulation, however, is to include those trusted intermediaries within a regulatory scheme while excluding others who do not assume that trust or do not offer financial services.

Intermediaries who do not assume a position of trust, non-financial uses, and individual access are digital currency innovations that should be encouraged. "Trustless" intermediaries can benefit both consumers and businesses through improved financial privacy,[8] financial inclusion,[9] and vibrant technology-based economies. These uses should not be burdened by compliance costs that lack concomitant consumer protection benefits.

Trusted intermediaries, on the other hand, so long as they walk and quack like a money transmitting duck, offer the same case for regulation as traditional financial services. The key

---

[7] Conference of State Bank Supervisors, *State Regulatory Requirements for Vitrutal Currency Activities CSBS Model Regulatory Framework* 10, (Sep. 2015) *available at* https://www.csbs.org/regulatory/ep/Documents/CSBS-Model-Regulatory-Framework(September%2015%202015).pdf

[8] *See* Peter Van Valkenburgh, *Bitcoin: Our Best Tool for Privacy and Identity on the Internet*, Coin Center (Mar. 2015) available at https://coincenter.org/2015/03/bitcoin-our-best-tool-for-privacy-and-identity/

[9] *See* Brock Cusick, *How can Bitcoin be Used for Remittances? A Backgrounder for Policymakers*, Coin Center (Dec. 2014) available at https://coincenter.org/2014/12/remittances/

is narrowly defining that duck. Statutes should limit licensure to those businesses or persons engaging in "Digital Currency Transmission." Digital Currency Transmission should then be defined, *functionally*, as follows:

Digital Currency Transmission

A. *Qualifying activities*. A person or entity shall be found to be engaged in Digital Currency Transmission if and only if it regularly and in the course of business has the ability to unilaterally execute[10] or prevent[11] a Digital Currency transaction on behalf of others,[12] except in cases where the ability to prevent transactions is reasonably time-limited and integral to a service such as escrow or transaction management.[13]

B. *Non-qualifying activities*.[14] In no event shall any of the following activities, in and of themselves, be interpreted as Digital Currency Transmission:
   1. developing, distributing, or servicing software;[15]
   2. contributing software, connectivity, or computing power to a Decentralized Digital Currency;[16]
   3. providing data storage or security services for a Digital Currency Business;[17] or
   4. engaging in otherwise qualifying activities undertaken for non-monetary purposes,[18] or that do not involve more than a nominal amount[19] of Digital Currency.

The sections that follow explain in detail each component of the above model language.

A. "Digital Currency Transmission" vs. "Virtual Currency Business Activity"

The New York Department of Financial Services, in its BitLicense, defined a category of regulated activities with the novel phrase, "Virtual currency business activity."[20] *Tabula rasa*, better terminology would be "Digital Currency Transmission." "*Virtual* currency" could refer to any sort of non-tangible currency, *e.g.*, dollars sent through Paypal or airline miles.

[10] *See infra* Part 1.C "unilaterally execute" at p. 6.
[11] *See infra* Part 1.D "unilaterally prevent" at p. 8.
[12] *See infra* Part 1.E "on behalf of others" at p. 13.
[13] *See infra* Part 1.D "unilaterally prevent" at p. 8.
[14] *See infra* Part 1.G "Non-qualifying activities" at p. 13.
[15] *See infra* Part 1.H "developing, distributing, or servicing software" at p. 14.
[16] *See infra* Part 1.I "contributing software, connectivity, or computing power" and "Decentralized Digital Currency" at p. 14.
[17] *See infra* Part 1.J "providing data storage or security services" at p. 17.
[18] *See infra* Part 1.K "non-monetary purposes" and "nominal amount" at p. 18.
[19] See *Id*.
[20] BitLicense, *supra* note 3, at § 200.2(q)(2).

"Digital," by contrast, makes clear that newer electronically tokenized money is what is at issue. Additionally, the broad phrase "business activity" suggests any and all activities relating to these new technologies. Money transmission, on the other hand, is a term that signifies a limited range of businesses that help consumers move money, not all money-related business. As similar regulations are tailored to new technologies for moving money, the terminology should remain appropriately circumscribed: "digital currency transmission" not "digital currency business" or "business activity."

B. Differentiating by Capability and Risk Rather Than Technology or Method

The determination of which businesses warrant regulation and which do not should be made by reference to what harm the business is capable and incapable of doing, rather than whether they—vaguely and metaphysically—"hold" or "store"[21] units of digital currency.

The only businesses who are truly capable of harming their digital currency consumers are those who can lose (e.g., through hacking), misspend, permanently immobilize, or fail to protect a customer's funds entrusted to them. Therefore, the businesses that should be clearly covered within a definition of Digital Currency Transmitter are those that have the ability, ***on their own and without seeking additional information (a secret key) from the consumer***, to execute or prevent a digital currency transaction. That ability raises the potential for digital currency mismanagement and is what gives rise to a position of trust.

C. "unilaterally execute"

Digital currency allows for programmatic money. Software can manipulate the digital currency so that it exists in a state of divided control. In Bitcoin technologies, for example, this divided control is made possible with so-called multi-signature wallets.[22] Multi-signature wallet software can assign bitcoins to public addresses that are linked to multiple private keys, each separately stored, some majority of which are needed to effectuate any transfer out of the wallet addresses. Think of it like the keys to a hypothetical safe deposit box at a bank: You have one key, your banker has the other, and both are required to open the box. Bitcoin addresses can be mathematically linked so that some number (M) of the total linked

[21] Digital or "virtual" currency is not, by definition, something that is capable of being held in the literal sense. Moreover, while we talk of "storing" digital files, perhaps in a cloud service like Dropbox, we cannot talk of storing Bitcoins. Bitcoins are not files; they are assignments of value made to pseudonymous addresses and listed on a public ledger called the blockchain. ***No one holds or stores bitcoins; one holds or stores the cryptographic keys that grants one permission on the network to sign for transactions involving particular addresses***. To the extent anyone ever *holds* or *stores*, or simply *has* bitcoins, it will be because they have control over these cryptographic keys.

[22] *See* Ben Davenport, *What is Multi-Sig, and What Can It Do? A Backgrounder for Policymakers*, Coin Center (Jan. 2015) available at https://coincenter.org/2015/01/multi-sig/

keys (N) are required to move funds. This is referred to as *M-of-N* transactions[23] or, more simply, "multi-sig."

Given multi-sig, some parties may have only one of several keys necessary to execute a digital currency transaction. For example, if two of three keys are required to transact, and a service provider only ever holds one key, that service provider should not be understood, for the purposes of consumer protection, as being a Transmitter of Digital Currency. Minority key-holders cannot, solely by their own negligence or malice, lose consumer value. This is why our proposed definition includes the word ***unilaterally.*** That caveat is critical. These parties can play highly valuable consumer-protective roles in the digital currency ecosystem as fraud-monitors, or disaster recovery services. They should be supported in their development. Moreover, if they cannot abscond with or otherwise lose a customer's funds they should not be subject to the costly burden of licensure.

A company could, for example, help store only the disaster recovery key of a customer who is afraid of losing one of her keys or is afraid of her digital currency exchange (a separate company) being compromised. Another company could, for example, hold a single key to sign off on transactions initiated using the consumer's key after, and only after, the company verifies that the consumer's phone has not been hacked or her key otherwise compromised.

Both of these hypothetical companies would provide an essential service in securing and safeguarding customer funds. Both hypothetical services are novel and unavailable to the customers of traditional banks and money transmitters because they rely on the use of new cryptographic tools and the blockchain to divide control among multiple businesses without using laws to enforce that division. Neither of these companies, however, should need to be licensed as Digital Currency Transmitters. Without possession of *sufficient* keys to move or immobilize a customer's funds on its own, the company does not pose a consumer protection risk; quite the opposite, they mitigate that risk.

Such companies will be highly valuable innovators in the field of digital currency. The technology that enables divided key control, *i.e.*, multi-sig, is widely understood within the industry as the single best tool for preventing a Mt. Gox-style heist before it even happens.[24] By defining custody and control to only those who can ***unilaterally*** *execute a transaction,* regulation would send a credible and welcome signal to innovators in the digital currency space: *we value your effort to build technology that will complement our consumer protection efforts and do not want to impede your progress unnecessarily*.

---

[23] *See* Gavin Andresen, *BIP 0011*, (Oct. 2011) https://github.com/bitcoin/bips/blob/master/bip-0011.mediawiki. *See also* Ben Davenport, *What is Multi-Sig, and What Can It Do? A Backgrounder for Policymakers*, Coin Center (Jan. 2015) available at https://coincenter.org/2015/01/multi-sig/

[24] *See* Ben Davenport, *No Sleep Till Multi-Sig* (Jan. 12, 2015) https://medium.com/@bendavenport/no-sleep-till-multi-sig-7db367998bc7.

D. “unilaterally prevent”

Given multi-sig, we can imagine many various business models where control of funds is divided between the customer and the business or even between a customer and multiple businesses. At root, any multi-sig service provider can be classified as either: *able to unilaterally execute*, described above, *able to unilaterally prevent*, or *able to prevent if customer/other parties agree*. Additionally, useful systems can be designed by using another technology native to many cryptocurrencies, time-locked transactions (within the bitcoin protocol referred to as n-lock transactions). With time-locked transactions a business may temporarily have the ability to stop a user from transacting with some certain amount of cryptocurrency, but the user will always automatically regain full control of the funds after a specified time. So, in full, our list of possible configurations is as follows:

1. unilaterally able to transact on user’s behalf
2. unilaterally able to block transaction on user’s behalf
3. able to block transaction when customer/third party also agrees
4. temporarily able to block transactions

Of these, only (1) and (2) present similar risks of insolvency or loss to the customer as traditional money transmitters, and only businesses implementing these systems should be regulated via money transmission or digital currency licensing. Configurations (3) and (4) pose no solvency risk to consumers. Moreover, they are highly novel innovations with promising future applications that are only now being envisioned and developed. Some of these applications are described below in order to offer better context for our policy recommendations. ***Refusing to treat these uses of the technology as money transmission is the single most innovation-friendly policy that state legislators and regulators can adopt.***

Additionally, clearly exempting services that employ these configurations does not leave the customers who utilize these services fully outside of consumer protection regulation. Any consumer-facing service will be responsible for upholding the conditions and warranties of its terms of service agreement, and good behavior can be enforced in the state courts under contract law. Further, as is the case with many Internet-based services, the law of Unfair and Deceptive Acts and Practices, as enforced by both the states and the Federal Trade Commission, applies. These service providers would also be subject to Unfair, Deceptive, and Abusive Acts or Practices regulation under Dodd Frank and the federal Consumer Financial Protection Bureau. All told, these safety nets should be sufficient to guard the users of non-custodial services—who already are in a far less vulnerable position than users of custodial services—while also enabling permissionless innovation. The following three subsections describe the various ways that businesses may have the power to prevent transactions and explains why some should and some should not be regulated as digital currency transmitters.

Unilateral Prevention. In rare situations, a business could have sufficient keys to unilaterally block a consumer from transacting with her digital currency, but insufficient keys

to transact without consumer agreement. Sometimes this power is referred to as "negative control" over consumer funds. For example, if funds are moved into an address that requires 2 of 2 keys to sign for outgoing transactions, but a service provider retains one key and its customer retains the other, then the service provider can unilaterally prevent a transaction (the customer can only sign with one key, fewer than is required to transact) even though it cannot unilaterally execute a transaction (the service provider can only sign with one key, not the required two to create a correctly formed transaction).

We can think of this arrangement as similar to a bank safe deposit box: the box requires two keys to be opened, one that the customer retains and the other supplied by a bank employee. In the example of digital currency, however, there is a subtle additional factor to consider: the box doesn't exist on the service-provider's premises (it is an entry on a global shared ledger) and the box simply can't be opened without the keys (as compared with a safe deposit box, which would, in theory, eventually yield to a safe-cracker or a crowbar).

It is unclear why a business would ever set up such an arrangement. However, if it does so it should be regulated as a Digital Currency Transmitter. Should the business ever be hacked, for example, the hackers could take the key and blackmail the consumer into signing with the other key for a transaction that would send some funds to the thieves' address and some to another address held by the customer. The blackmailers will probably succeed in this scam, given that refusal to comply will irrevocably lock all of the funds out of anyone's reach. Because of this vulnerability, businesses unable to execute but able to unilaterally prevent transactions pose similar risks to consumers, and assume a similar level of trust, as traditional money transmitters. They should be regulated accordingly.

Low Trust Escrow and Transaction Management Services. There may be situations in which several entities, acting together, may be capable of preventing a transaction. Given the open and programmatic nature of digital currency, many of these future uses have yet to be put into practice, but their mechanisms and benefits can easily be imagined. Perhaps the simplest example is something we can call *low-trust escrow*.

To understand low trust escrow, imagine the following hypothetical: Alice has a boat she'd like to offer for sale; Bob likes Alice's boat and would like to buy it with Bitcoin. Bob, however, is concerned with the irreversibility of normal Bitcoin transactions. "What if," Bob worries, "the boat turns out to be a lemon. What if it has a delaminating hull, and widespread mold damage in hidden compartments? Shouldn't I be able to know for sure that I can get my money back within some reasonable period, in the event that there are hidden defects." Alice understands Bob's concerns and she is willing to provide some assurance. She's even willing to promise a full refund if he's not happy within the first 30 days. However, if Bob pays with Bitcoin there's always a possibility that, as with cash, Alice disappears and simply reneges on her promises.

To solve this problem without relying on a traditional escrow service or an ex-post contract dispute, Bob and Alice can agree to use a multi-sig transaction with an appointed arbitrator

in the event of a dispute. Bob and Alice ask their mutual friend Chad to be their arbitrator. Together they use freely available software to create a multi-sig bitcoin address with three keys, where two keys are required to sign for transactions. Alice, Bob, and Chad each receive one of the three keys. Bob, to show good faith, signs a transaction using his own personal Bitcoin wallet that moves the purchase price of the boat into this new multi-sig address. Alice now knows that if she and one of the other key-holders were to sign a transaction moving these funds into her own private wallet, then she would have her payment free and clear, so she gives Bob the boat.

At this point the transaction can go one of three ways:

1. Bob likes the boat and doesn't notice any defects. At the end of the month he signs a transaction that would move the funds from the multi-sig address into Alice's private wallet—essentially turning one of two keys necessary to make the transfer. Alice now provides the other signature and broadcasts the transaction to the network, effectuating the permanent transfer to her private wallet.

2. Bob discovers defects. He returns the boat and asks Alice to refund his money. Alice, being the honorable businessperson that she is, signs a transaction that would move the funds back to Bob. She shows the transaction to Bob, and he gives the second signature and broadcasts the transaction to the network, making the transfer of funds back to his private wallet permanent.

3. Bob discovers defects, but Alice refuses to refund the money, claiming that the defects are minor. At this point the money will sit, locked in the multi-sig address because neither Bob or Alice can unilaterally create fully-signed transactions. They call Chad. Chad investigates the boat and ultimately agrees with either Alice or Bob. In the end he signs a transaction that would move the funds to the party he judges to be in the right. The party that benefits (Alice if Chad thought the defects were de minimis, Bob if he didn't) signs as well, effectuating a permanent transfer to that party's private wallet.

In this example, Chad provides a valuable service. Like an escrow agent he can be an important hedge against Bob and Alice's counterparty risk. Unlike a traditional escrow agent, however, Chad can never embezzle from the transactions he's tasked with moderating. He never has custody of the funds because he can't transact unless either Alice or Bob also agree to sign the transaction. In fact, after the initial multi-sig address is created, Chad need not be involved in the transaction at all unless a dispute arises.

There is one situation in which Chad appears to have the ability to prevent a transaction from going forward. He could refuse to sign for either party in a situation where Alice and Bob don't agree. Yet even in that case he cannot **unilaterally** block transactions. For example, if he were to disappear, Alice and Bob could agree to sign a transaction moving the funds to a new multi-sig address with another, more responsible, arbitrator since they still together have two of three keys. In such a scenario, Chad does not create the same degree of consumer

risk as the multi-sig provider described in the previous section (who can lose or destroy one of the two keys necessary to ever transact—effectively destroying the customer's Bitcoin holdings).

Given this substantially lower consumer risk and the value of these novel technological arrangements, only those with the **unilateral** ability to prevent transactions should be regulated as money transmitters. To the extent that non-unilateral negative custodians (*e.g.* Chad in our example) should be regulated, there are better fitting policy approaches to be found in contract law and/or the state and federal laws of unfair and deceptive trade practices.

In order to better describe these services, our model language makes reference to both escrow and "transaction management services." This term comes from guidance that has been given by FinCEN on the subject of activities exempted from Bank Secrecy Act compliance.[25] FinCEN goes further than our framework: even parties with full control over customer funds are exempted from their interpretation of money transmission in cases where that custody is integral to an escrow transaction. The language proposed above is, in fact, more conservative. It only explicitly exempts digital currency escrow providers when the provider has the ability to prevent, not execute, a transaction on behalf of others. Such an escrow provider could never run-off with the funds, she can only prevent a transaction between two parties from proceeding unless or until both parties agree to proceed (she can also allow a transaction to proceed as long as one of the two parties agrees).

Reasonably Time-Limited. Finally, with respect to prevention, it is necessary to discuss how those with the *temporary* ability to unilaterally prevent transactions should be regulated. In the most fundamental sense, the transaction validators—*e.g.* miners in the case of Bitcoin—on a cryptocurrency network will be capable of preventing transactions for the brief period in which they are capable of incorporating or not incorporating requested transactions into the currency's blockchain. Additionally, the Bitcoin protocol—as well as several other cryptocurrencies—allows for transactions that are time-locked—often referred to as "n-lock" transactions. An n-lock transaction can be signed by the party moving funds but in such a way that it cannot be accepted by the network until a specified time in the future.

A primary use for n-lock transactions is in the creation of low-trust microtransaction channels for the metering of goods or services.[26] Say, for example, you were a cellular network provider and you wanted to charge your network users for every kilobyte of data they

[25] See FinCEN Ruling FIN-2014-R005, "Whether a Company that Offers Secured Transaction Services to a Buyer and Seller in a Given Sale of Goods or Services is a Money Transmitter." (April 29, 2014) http://www.fincen.gov/news_room/rp/rulings/pdf/FIN-2014-R005.pdf.

[26] For a more complete backgrounder on microtransaction channels see Chris Smith, What are Micropayments and How does Bitcoin Enable Them? A Backgrounder for Policymakers, Coin Center (June 2015) available at https://coincenter.org/2015/06/what-are-micropayments-and-how-does-bitcoin-enable-them/

used. Rather than establishing a legal relationship with the user—*e.g.* signing them up for a subscription or otherwise making a formal service contract—you'd like to allow anyone to connect to your network, sight unseen, and have their phone automatically pay you for its data usage. Writing a new microtransaction to the blockchain for every kilobyte of data consumed is not an efficient method to create such a system. Even Bitcoin—often celebrated for its low per-transaction fees relative to credit card networks—would require some fees for each transaction, and if an additional transaction was required for every few seconds or minutes of additional use, the cumulative fees would still be cost-prohibitive. Bitcoin, and other cryptocurrencies, however, can use n-lock transactions and microtransaction channels to achieve the same result with extremely low fees.

To set up a microtransaction channel the user's device and the service provider's server generate a new 2-of-2 multi-sig address. The user retains one key and the service provider gets the other. Into this address the user will put the maximum amount of bitcoin she imagines spending on mobile data with this provider over a set period. Let's say $5 for the day. Before moving any of her funds into this multi-sig address, however, the user writes a "refund" transaction that would move $5 from this new multi-sig address back into her own private address and she puts an n-lock on the transaction so that it cannot be spent until the day is over. Because the address is a multi-sig address, she sends a copy of the transaction to the service provider and asks him to sign it as well and send it back to her. Once she checks the signature, she puts her $5 in the address. At this point the user is guaranteed that she'll always get her money back at the end of the day, even if the service provider suddenly disappears or refuses to deal with her. If the service provider disappeared, she'd simply wait for the n-lock period to expire (after a day in our example) and then broadcast the refund transaction to the network.

Assuming the service provider does not disappear, however, the microtransaction channel is now working. As the user consumes the service provider's bandwidth, they continue to exchange transaction messages spending from the $5 in the multi-sig address. After one kilobyte of data is used, a new transaction is created that would move $0.01 to the service provider and $4.99 back to the user—and the user signs this transaction and sends it to service provider. This process repeats as the user consumes more data. Eventually, when the user is done with the service provider (say she has left the service provider's range) the service provider takes the last transaction message it received from the user—say $1.49 to the service provider and $3.51 back to the user—and broadcasts this transaction to the network, thus finalizing it on the blockchain. Many transactions have occurred but only the last one is actually processed by the network; this means there is only one network fee as opposed to many. All throughout the process both parties are protected from counterparty risk because they can always broadcast the most recent transaction in the event the other party becomes unresponsive.

This arrangement would be, for the users, much simpler than it may seem. The entire process would be automated—*i.e.* the user's device would set up the multi-sig address, exchange all of the transaction messages, and check the validity of signatures on those messages. All the

user would do is specify a certain maximum amount of money they'd like to spend on mobile data per day, and the device would do the rest, potentially even negotiating the best price from a range of providers.

The implications of this arrangement on a standard for licensed activities should be clear. By placing the user's funds in a multi-sig address with an n-locked refund transaction that cannot be processed for a day, the service provider is temporarily able to prevent the user from transacting with her money. This temporary ability is necessary to guarantee that the service provider be paid for the goods it is offering, however, it does not generate the sort of consumer protection risk that a multi-sig wallet provider who has the permanent ability to block transactions creates. Moreover, although some microtransaction channels may be excluded under a merchant services or payment processor exemption, it is not clear that all microtransaction channels will be established for the purposes of paying for goods. These channels may be provided by intermediaries with relationships to several merchants or, indeed to other individuals. Regardless, because of n-lock transactions, these microtransaction channels will never engender the sort of solvency or consumer protection risks inherent in traditional money transmission—the provider can never lose or run-off with the funds—and therefore these technologies should be regulated under different regimes such as contract or unfair and deceptive practices law.

In order to avoid potentially metaphysical, unproductive discussions over what "temporary" may mean with reference to the "temporary ability to prevent transactions," our model language strongly advocates the use of the phrase "reasonably time-limited." This allows policymakers to focus on whether the service on offer is appropriately circumscribed to protect the user—i.e. funds for a microtransaction channel will never be locked beyond the user's control for years, but, instead for an amount of time suitable to providing the good that is being metered (*e.g.* broadband) with microtransactions.

E. "on behalf of others"

Individuals should not be regulated as money transmitters when they deal only in their own funds; therefore, licensing regulations should clearly indicate that only transmission "on behalf of others" rises to the level of "Digital Currency Transmission." Bitcoin and other cryptocurrencies enable users to manage their own deposits and transmissions without relying on a trusted intermediary. Such a user would install a *software wallet* on her computer or mobile device. The user would be able to receive and send bitcoins by storing keys to Bitcoin addresses on the device and writing transactions using the software and their keys. The software broadcasts those transactions to the peer-to-peer network, which then adjusts balances in the public ledger—the blockchain— accordingly.

F. "Non-qualifying activities"

The diversity of business models and activities enabled by digital currency technology underscores the importance of not only clearly defining who is, but also who is not, required

to be licensed. Four particular activities should not, in and of themselves, qualify as Digital Currency Transmission.

G. "developing, distributing, or servicing software"

Regulation should not unnecessarily foreclose an individual's ability to access financial services that do not employ a trusted intermediary. Bitcoin and other cryptocurrencies, because they can be accessed with software and an Internet connection alone, enable this access. Accordingly, the mere development, distribution, or servicing of software that enables individuals to manage and transmit their own digital currency should not be regulated at the level of Digital Currency Transmission. At no point does the software provider hold keys to the user's funds. Instead, the software provider provides the user with tools to generate, store, manage, and use, locally, her own keys. Without the element of trust engendered by safekeeping a user's keys on her behalf, these service providers should not require licensure. Additionally, the mere production and distribution of software is protected speech under the First Amendment.[27] Any attempt to mandate licenses from entities acting solely in this capacity would likely constitute a prior restraint on protected speech and be found unconstitutional.

H. "contributing software, connectivity, or computing power" and "Decentralized Digital Currency"

Digital currencies can be divided into two broad categories: centralized and decentralized.

Centralized digital currencies are created and controlled by a singular authority, usually a business. For example, Amazon.com has created Amazon Coin to allow its users to buy digital content on its sites.[28] Such a business can create digital tokens and distribute or sell them to customers. That business can peg the value of the currency by promising to redeem those tokens for a fixed amount of fiat currency or some item of value, or they can allow the value to float according to market supply and demand. As the Financial Action Task Force has explained, "the vast majority of virtual currency payments transactions involve centralised virtual currencies. Examples include E-gold (defunct); Liberty Reserve

[27] *See Bernstein v. United States Dept. of Justice*, 192 F.3d 1308 (9th Cir. 1999) [add in quoted language to support]. *See also* Robert X. Cringely, Accidental Empires: How the Boys of Silicon Valley Make Their Millions, Battle Foreign Competition, and Still Can't Get a Date 28 (1992) ("Programs are written in a code that's referred to as a computer language, and that's just what it is—a language, complete with subjects and verbs and all the other parts of speech we used to be able to name back in junior high school. Programmers learn to speak the language, and good programmers learn to speak it fluently. The very best programmers go beyond fluency to the level of art, where, like Shakespeare, they create works that have value beyond that even recognized or intended by the writer.").

[28] *See* Amazon Inc., *Amazon Coins*, http://www.amazon.com/gp/feature.html?docId=1001166401; *see also* Wikipedia, *Amazon Coin*, http://en.wikipedia.org/wiki/Amazon_Coin.

dollars/euros (defunct); Second Life "Linden dollars"; PerfectMoney; WebMoney 'WM units'; and World of Warcraft gold."[29]

Decentralized digital currencies, by contrast, are created and maintained by an open community of interested participants using open source software. These participants run the software, or a compatible modification of the software, on Internet-connected computers that, together, form an open peer-to-peer network. Decentralized digital currencies are also known as cryptocurrencies because all decentralized currencies, to date, have utilized theories and functions from the science of cryptography in order to guarantee both (A) that network participants cannot spend money they don't own, and (B) that the money supply grows at a predictable rate. Bitcoin, launched in 2009,[30] was the first cryptocurrency, and as of 2015, it remains the largest by market capitalization.[31]

Decentralized Digital Currencies should be defined as follows:

> *Decentralized Digital Currency.* Decentralized Digital Currencies are digital currencies that (1) do not have a single administrative authority, and (2) are issued and transferred using an open network running open source software.

The consumer protection implications of this distinction are not trivial and warrant heightened licensing requirements for centralized currencies over their decentralized counterparts. A business utilizing a centralized digital currency can unilaterally decide to devalue consumer balances by issuing more currency, similar to how a normal financial servicer could choose to take on more debt. A cryptocurrency business is not at such liberty; it cannot unilaterally create more tokens because monetary supply is governed by an open, collaborative protocol of which the business is only a small part.

A centralized digital currency business can rearrange consumer balances, or refuse to honor a consumer credit; and it, ultimately, is the sole fiduciary of the currency's accounting records. A cryptocurrency business, even if it rearranges consumer balances once deposited, can only receive and dispense funds to a consumer by writing to an indelible and public accounting record, the public ledger or blockchain of the cryptocurrency. This ledger, unlike the closed, internal ledger of a centralized digital currency business (or, for that matter, a traditional financial services business) can be publicly audited in real time to guarantee the solvency of the firm.

A centralized digital currency business can operate using closed source software, meaning the underlying scarcity or safety of the currency cannot be easily audited by outside

---

[29] Financial Action Task Force, *Virtual Currencies: Key Definitions and Potential AML/CFT Risks*, (June 2014) *available at* http://www.fatf-gafi.org/media/fatf/documents/reports/virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.

[30] *See* Satoshi Nakomoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, (May 2009) *available at* https://bitcoin.org/bitcoin.pdf.

[31] *See* Market capitalization of top cryptocurrencies *available at* http://coinmarketcap.com/.

technologists. A cryptocurrency is open-source by default and the underlying fundamentals of that technology are scrutinized by a bevy of third-party validators.

Even though software that is fundamental to decentralized digital currencies may be released and updated primarily by an individual or group of individuals, *e.g.*, Bitcoin's "Core Devs,"[32] these individuals cannot unilaterally change how the currency functions. To make any change to the currency, the updated software must be adopted by a majority of the peer-to-peer network. This network, composed as it will be of independent, technologically-sophisticated users, will audit the new code and likely reject any code that attempts to inject risk or fraud into the system.

Transaction validation on decentralized digital currency networks is performed by independent participants, often called "miners." These participants will, for brief (~10 minutes for Bitcoin) and sporadic intervals, have the sole power to validate all network transactions. However, that power is limited by fellow participants on the network. If a miner attempts to mark as valid a fraudulent transaction, the miner's work would be rejected by other network participants.

Therefore, individuals and businesses contributing to a decentralized digital currency are not trusted intermediaries. They can only take actions over which the network as a whole reaches consensus. As such, the user is not trusting a miner, she is trusting the majority of the Bitcoin network. Individual contributors to that network, whether they contribute computing power, software, or network access, should not be regulated or licensed as money transmitters, except in situations where they are able to unilaterally execute or prevent transactions.

New York's former money transmission regulator and architect of the state's BitLicense, Benjamin Lawsky, has repeatedly insisted that he did not intend to require licenses of individuals or companies that only mine a decentralized digital currency, such as Bitcoin, or develop the software that underlies those currencies. As he stated:

> We are regulating financial intermediaries. We are not regulating software development. To clarify, we do not intend to regulate software or software development. . . . Mining per se will not be regulated. To the extent the miner engages in other virtual currency activities, however—for example, hosting wallets or exchanging virtual currency—a license may be required for those activities. For mining itself, there will be no license requirement.[33]

This approach is well-advised, allowing regulators to focus on trusted intermediaries who control consumer funds—and could lose them—rather than individuals who merely build the underlying infrastructure of the currency. To ensure that these individuals and business are

[32] *See* List of Bitcoin Core Developers *available at* https://bitcoin.org/en/development.
[33] Benjamin M. Lawsky, *Excerpts From Superintendent Lawsky's Remarks on Virtual Currency and Bitcoin Regulation in New York City* (Oct 14, 2014) *available at* http://www.dfs.ny.gov/about/speeches_testimony/sp141014.htm.

unintentionally swept into a licensing regime, they should be clearly exempted by including the following language within a passage on non-qualifying activities: "contributing software, connectivity, or computing power to a Decentralized Digital Currency."

I. "providing data storage or security services"

As the Bitcoin ecosystem has matured, a new class of infrastructure service providers has emerged. Interacting with the Bitcoin protocol can be technically complex, particularly when using advanced transactions such as the multi-sig or divided key transactions described in a previous section.[34] Early bitcoin hosted wallet providers and exchanges generally coded these transactions in-house. However, this activity may not be the organization's expertise or comparative advantage. A consumer-facing business may find it more advantageous to focus on marketing, user experience, and regulatory compliance. It may, therefore, choose to contract-out the safekeeping of customer bitcoin keys to business-to-business firms that have developed expertise at utilizing multi-signature transactions and cold storage in order to best secure sensitive data.[35]

This is not novel in the world of Internet technologies. The video-on-demand service Netflix, for example, does not actually build or maintain the technology necessary to store video data. Instead, it relies on Amazon's cloud storage solution, Amazon Web Services.[36] If a Bitcoin bank or exchange decided to contract-out the safekeeping of customer keys, it would raise a novel regulatory question. Do both the consumer-facing bitcoin business, as well as the service provider it uses to secure its data, need to be licensed? Double-licensing would substantially erode any cost-savings thanks to firm specialization, and would likely discourage a competitive market for business-to-business digital currency security. The result would be higher fees for consumers as well as less security.

As a result, only one party should be licensed in such a situation: the consumer-facing business. The consumer-facing business holds itself out as a trusted intermediary to its customers who may not have the time, expertise, or caution necessary to effectively comparison shop or hedge against risks. A business-to-business Bitcoin firm, on the other hand, offers its security services to savvy institutions who have both the motivation and the capacity to aggressively comparison shop. In short, while market failures may prevent competition from effectively protecting individual consumers, a competitive market unfettered by regulatory costs in the business-to-business arena would best enhance

[34] *See infra*.
[35] Cold storage involves placing the majority of an institution's private keys in offline media, either disconnected computer memory like a thumb-drive, paper, or as memorized passphrases—a so-called brain bank. If keys are not stored on Internet-connected servers, then they can only be accessed by compromising either the individual with access to the key or the physical security surrounding the key. The attack surface could thus be minimized by limiting the number of employees with knowledge of or access to offline key storage, and storing the offline drives or slips of paper in safe-deposit boxes or guarded premises.
[36] Amazon, *AWS Case Study: Netflix*, http://aws.amazon.com/solutions/case-studies/netflix/ .

security. Moreover, as long as the consumer-facing business is a regulated entity, the protections of a Digital Currency Transmitter license will remain in effect for consumers.

Such a carve-out has been the longstanding norm for companies that are the legal agent of licensed money transmitters.[37] Similarly, the Financial Crimes Enforcement Network ("FinCEN") exempts merchant processors and banking intermediaries from duties under the Bank Secrecy Act because these entities are merely intermediaries between banks, which are heavily regulated entities.[38] FinCEN also exempts those who only provide "the delivery, communication, or network access services used by a money transmitter to support money transmission services."[39] Digital Currency Transmission regulations should include a similar exemption in order to promote the development of enhanced security tools and services.

J. "non-monetary purposes" and "nominal amount"

The technology underlying decentralized digital currencies has promising applications apart from the provision of money transmission services. Distributed ledgers (or "blockchains") are used within digital currencies in order to keep a shared, write-only, public record of *who* has been sent *how many* units. Such a ledger may also find use in any area where records need to be authoritative, irreversible, and public.

Several non-monetary blockchain projects are already underway. They include distributed systems for Internet domain name registration (*e.g.* Namecoin), identity and authorization services (*e.g.* Onename.io), and notary services (*e.g.* Proof of Existence). Other companies are finding ways to simplify the process of setting up a blockchain for uses specific to a particular client. Much as RedHat helps IBM develop web servers using a particular version of the open-source Linux operating system, a blockchain specialist (*e.g.* Eris) might help an accounting firm develop a specialized accounting system using blockchains.

Although these uses may have nothing to do with the provision of a money transmission service to consumers, they may nonetheless employ microtransactions in order to time-stamp some form of tokenized data. For example, a tiny fraction of a bitcoin (worth far less than one cent) may be sent on behalf of a customer in order to irreversibly note the identity of that customer on a public blockchain. The transaction is not intended to be a means of sending or receiving value; it is merely a representation of information that would be difficult to spoof, a verifiable token.

States may fear that such an exemption would create a dangerous loophole: a business could effectively operate as a money transmitting intermediary without licensure as long as it

---

[37] *See* New York Banking Law § 641 ("[N]or shall any person engage in such business as an agent, except as an agent of a licensee.").

[38] 31 C.F.R. § 1010.100(ff)(5)(ii) ("The term "money transmitter" shall not include a person that only: . . . (B) Acts as a payment processor to facilitate the purchase of, or payment of a bill for, a good or service through a clearance and settlement system by agreement with the creditor or seller; (C) Operates a clearance and settlement system or otherwise acts as an intermediary solely between BSA regulated institutions.").

[39] 31 C.F.R. § 1010.100(ff)(5)(ii)(A).

claims that the transactions are merely representing non-monetary data. As long as these placeholder transactions are small in value, however, there would be no viable way to use such tools to transmit a meaningful amount of funds. As Muneeb Ali and Ryan Shea of Onename.io have explained:

> To illustrate with an example, if someone planned on moving $100 by breaking it up into 2,500 $0.04 transactions, they would have to pay a fee on the order of $0.04 for each and every transaction. Since moving the $100 from location A to location B would require 2,500 transactions to split up the money and 2,500 transactions to rejoin the money, the mover would be left with scattered denominations totaling $50 in the middle of the process and absolutely nothing by the end of the process. Second, if the mover ever wanted to reclaim all of those funds and make any use of them, they'd leave an enormous footprint on the blockchain, with thousands of suspicious addresses and transactions that people would be able to inspect and track. Thus, such transactions should be considered impractical for the movement of any kind of funds. It should be noted that any microtransaction that moves funds that are equal to or less than the minimum accepted network fee (today about $0.04), cannot possibly result in the transmission of any money whatsoever, as demonstrated above. Rather, they would result in the loss of 100% of funds by the time they are rejoined at the end of the process. By extension, orchestrated microtransactions that move funds equal to double the minimum accepted transaction fee would result in the loss of 50% of the total funds by the end of the process, and would still leave an enormous, conspicuous footprint.[40]

Accordingly, non-monetary transactions of *nominal* amounts should be outside the scope of Digital Currency Transmission regulation.

[40] Muneeb Ali & Ryan Shea, Comments to the New York Department of Financial Services on the Proposed Virtual Currency Regulatory Framework, *available at* http://www.dfs.ny.gov/legal/vcrf_0500/20141022%20VC%20Proposed%20Reg%20Comment%20245%20-%20OneName.pdf

2. Exempted Businesses

Digital currency is exciting, in part, because it has brought new life and competition to markets for the provision of financial services. This vibrancy is not the result of careful scientific research or newly patented inventions developed by large technology firms. It is, instead, the result of many small start-up companies working with freely available software and an open network.[41]

A. Why Digital Currency Startups Matter

An ecosystem of many small firms is diverse, presenting consumers with many new options for financial transactions. These firms are also capable of scaling massively should their ideas gain widespread consumer traction. That diversity is contingent on low overhead costs inherent to open digital currency networks, which allow a company to securely accept funds from a customer across the world in a matter of minutes for fractions of a penny on the dollar.[42] That network also enables scalability: transactions of many millions of dollars carry the same fees as transfers of pocket change and can be executed just as easily.[43] As technological limits on diversity and scalability are lifted, it is important that those limits are not merely reinstated by a costly regulatory structure that is insensitive to the small size or rapid growth of new and innovative players.

B. Discretion Alone Cannot Accommodate Innovation

The Bitlicense, for example, rightly contemplates the need to exempt small and innovative digital currency startups from the costly burdens of licensure. However, the BitLicense grants those exemptions, called "conditional licenses," at the "sole discretion" of the NYDFS Superintendent.[44]

Discretion can be an important tool for lessening the unduly harsh effects of a regulation, but it should not be the only tool. Discretion also generates regulatory uncertainty: a person never knows whether conduct she has freely engaged in before will suddenly become punishable simply because a government official changed her mind, or was replaced, or—in the worst case—was influenced by a competitor or someone who wished our hypothetical citizen harm.

---

[41] Angel.co, a valued trade publication within the technology investment community, lists some 619 companies that are now building Bitcoin related businesses. These companies, however, are small. Average valuation is estimated at $3.9 million. Angel.co, *Bitcoin Startups*, https://angel.co/bitcoin (last accessed Feb. 2015).

[42] Popular hosted wallet provider Coinbase, for example, pays the Bitcoin network typically 0.0002 BTC for transactions of any size. They do not charge this fee to the customer choosing to bear these small costs internally. Coinbase, *Does Coinbase pay bitcoin miner fees?* (Dec 2014) *available at* https://support.coinbase.com/customer/portal/articles/815435-does-coinbase-pay-bitcoin-miner-fees-.

[43] *Id.*

[44] BitLicense, *supra* note 3, at § 200.4(c)(3)(i).

A formal, rather than discretionary, carve-out for small startups is essential to preserve the freedom to innovate using these technologies, and it should be accomplished in a way that sets clear ex-ante standards and safe-harbors for budding entrepreneurs.

C. Drafting an On-Ramp for Startups

Small startups can be shielded from the costs of regulation by explicitly exempting them from regulation up until the point at which they pose serious consumer protective risks. Shelter should also be granted to businesses that have passed that point and taken appropriate steps to alert the regulator and initiate the process of licensure. The following illustrates such exemptions:

Exempted Businesses.

A. *Startup On-ramp*. Businesses engaged in Digital Currency Transmission shall be exempted from regulation and licensure under this part if:
    1. the business's average aggregate outstanding obligations[45] to customers remains below $5 Million or the equivalent in Digital Currency,
    2. the business has registered with federal authorities as a Money Services Business if applicable, and
    3. the business discloses its unlicensed status to customers.
B. *Transitional Period.* Businesses that surpass the $5 Million threshold shall be exempted from regulation and licensure under this part, for a period of time beginning when the Commissioner is notified and lasting for a duration determined at the discretion of the Commissioner but no shorter than six months, if:
    1. the business notifies the Commissioner of the increase in volume in a reasonably timely manner, and
    2. the business takes reasonable steps to initiate the process of licensure under this part.

The $5 million per year transaction level is an appropriate threshold among companies that can pose serious, systemic risks to consumers (*e.g.* Mt. Gox[46]), and those where risk-level is

[45] The threshold for consumer risk should be based upon the amount of consumer funds over which the company has custody. These balances are often referred to within the context of traditional money transmission as "outstanding transmission obligations." *See, e.g.*, Texas Administrative Code Title 7 Chapter 33 *available at* http://texreg.sos.state.tx.us/public/readtac$ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=7&pt=2&ch=33&rl=23.

[46] Robert Mcmillan, *The Inside Story of Mt. Gox, Bitcoin's $460 Million Disaster*, WIRED (Mar. 3, 2014) http://www.wired.com/2014/03/bitcoin-exchange/.

tolerable given the benefits that unfettered start-up innovation could bring. However, a regulator could carefully calibrate this threshold as it sees fit. This threshold could change from time to time or be based on some other ex ante specification (*e.g.* a time-delimited safe-harbor for companies younger than two years), affording the regulator some discretion to adjust regulatory policies in response to observed rates of fraud, consumer harm, or other extenuating circumstances. However, those adjustments should be explicit, apply generally across the industry, and be announced in advance so that firms can plan their compliance strategies efficiently.

3. Interaction with State Money Transmission Law

A Digital Currency Transmitter should not need to acquire both a money transmission license and a digital currency license. Both kinds of licenses aim to accomplish the same thing. They are meant to ensure that companies are well-run, well-capitalized, and adequately serve consumers in a compliant manner. Once a business has acquired a Digital Currency Transmission license, therefore, there is no apparent public benefit from going through the expense and trouble of acquiring a second license. Similarly, if a digital currency business has already obtained a money transmission license there is little to be gained from a separate inquiry and licensing process for digital currency. In short, if a digital currency company is adequately capitalized and vetted by the regulator, what can be gained from a second set of examinations, invoked merely because the company holds fiat currency in addition to digital currency?

Statutes should clearly specify this interchangeability to avoid any confusion. Courts are increasingly coming to the conclusion that digital currencies such as Bitcoin qualify as "money" under various statutory definitions.[47] Relatedly, any individual who "knowingly conducts, controls, manages, supervises, directs, or owns all or part" of a money services business operating without a money transmission license can be fined and imprisoned for up to five years under federal law.[48] State legislators surely do not wish a licensed digital currency company to remain technically in violation of federal law (should the requirement to have a *money transmission* license be interpreted strictly). Legislation should therefore clarify that each license satisfies state law requirements to have the other:

Interaction with state money transmission law.

A. A business licensed as a money transmitter under the Money Transmission Act of this State shall be exempted from regulation and licensure under this division.
B. A business licensed or exempt from licensure under this division shall be exempted from regulation and licensure under the Money Transmission Act of this State.

[47] 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).
[48] 18 U.S.C. §1960(a).

4. Capital Requirements

To protect consumers, Digital Currency Transmitters, as with licensed money transmitters, should be required to have sufficient capital reserves on hand to guarantee the solvency of the institution. In money transmission licensing, these reserves can usually be satisfied by holding cash. California, for example, lists cash as an eligible security for the purposes of capital requirements in money transmission licensing.[49] Allowing the transmitter to hold cash avoids a situation where the business must hold illiquid assets alongside and in duplication to any liquid (*i.e.* cash) assets held in order to quickly make good on outstanding payment orders. Digital currency transmitters should face similar standards. If the business holds digital assets in the form and amount deposited by their customer, it should not also have to hold duplicative reserves in some other form.

Capital Requirements.

A. *Permitted Holdings.* In order to satisfy capital requirements set by the commissioner, each licensee shall hold either:
    1. digital currency equal in form and quantity to customer deposits, or
    2. high-quality, investment-grade investments.

Bitcoin and cryptocurrency technologies can, in fact, offer superior proof that intermediaries are solvent, and that consumer funds are protected against loss, mismanagement, or the excessive fees of financial intermediaries. All cryptocurrency transactions take place on a public ledger, called the blockchain. These records could indicate, authoritatively, whether funds remain within the organization's publicly- announced customer addresses on the public ledger and whether any fees are being deducted from those addresses. A company could voluntarily, or if required by a regulator, provide real time records of consumer funds as they travel through the intermediary.

Some digital currency companies are already offering this form of real-time disclosure and proof of solvency. Bitreserve, for example, has developed an automated system of transparency that it hopes could even help stem future financial crises:

> Bitreserve is the first financial service in the world to publish a real-time, verifiable, proof of solvency. Anyone at any time can confirm that the aggregate amount of value in our members' wallets is matched with assets in our full reserve.

[49] *See* Cal. Fin. Code §2082, *available at* http://www.leginfo.ca.gov/cgi-bin/displaycode?section=fin&group=02001-03000&file=2081-2089.

> Built for a post-trust world, Bitreserve's real-time transparency system eliminates the opportunities for fraud and destructive risk-taking that have caused the collapse of banks and other financial institutions throughout history.
>
> We're setting this new standard of transparency, accountability and consumer protection with two features called the Reservechain™ and the Reserveledger™. The Reservechain enables anyone to trace a transaction all the way back to the point where it entered our network. The Reserveledger is a real-time publication of every change in our obligations to our members and every change in assets held in our reserve.[50]

The technology described by Bitreserve is not unique to this one company. Programmatic money that exists on a public ledger, as enabled by cryptocurrency generally, holds great promise in automating regulatory compliance. Companies must be allowed to hold their reserves in these currencies to enable the transparency and regulatory compliance systems that bitcoin makes possible.

[50] Bitreserve HQ Inc., *Transparency*, https://bitreserve.org/en/transparency.

5. Other Important Considerations

New York was the first state to craft a digital currency-specific transmitter license: the BitLicense. Many states may be tempted to follow not just New York's lead, but its regulatory language as well. This report has sought to promote superior language particularly for defining the scope of licensed activities and exemptions for startups. New York's proposed regulations, however, also contain sections that are simply bad policy regardless of artful or inartful drafting. Adopting New York's anti-money laundering requirements and pre-approval requirements for new products would be ill-advised.

A. AML Requirements

The BitLicense's AML requirements impose costs onto digital currency businesses that are not borne by any other money transmission business under state or federal law.

Specifically, the license has a state-level suspicious activity reporting (SARs) requirement[51]—the first of its kind for state money transmission law—and a requirement that duplicates the efforts of FinCEN.[52] Additionally, the BitLicense's state-level SARs requirement has no lower bound of application (*i.e.*, any transaction regardless of the dollar amount must be reported if suspicious; this contrasts with FinCEN, which generally requires reporting of suspicious transactions only when they are over $2,000), potentially resulting in a flood of low-value reports that hemorrhage sensitive user-credentials and damage user privacy because of overly-cautious regulatory compliance. The license has a reporting requirement for all transaction over $10,000[53] that similarly doubles the efforts of FinCEN.[54] In drafting the BitLicense, New York's Department of Financial Services has not explained why FinCEN and Federal regulators are failing at their remit and therefore need a second line of state-level reinforcements. Nowhere in New York's, or for that matter, any state's money transmission licensing scheme, are such AML requirements in evidence.

If not remedied, this aspect of the BitLicense will make New York an unlikely home for young, mobile companies free to choose their base of operations and their regulator. Companies may choose to protect user privacy and avoid costly requirements by settling in, for example, the United Kingdom, which has recently shown a sensitive approach to digital currency regulation.[55] To the extent necessary, these companies may screen the IP addresses of their customers and limit their services when dealing with New Yorkers so as to avoid embroiling themselves in a legal struggle with inherently large downside risks (time in prison) and little upside (a marginal number of additional customers from New York).

---

[51] BitLicense, *supra* note 3, at § 200.15 (e)(3).
[52] 31 C.F.R. § 1022.320.
[53] BitLicense, *supra* note 3, at § 200.15(e)(2).
[54] 31 C.F.R. § 1010.330.
[55] *See* Jerry Brito, "The UK plan for Bitcoin is a step in the right direction," *Coin Center* (March 18, 2015), *at* http://coincenter.org/2015/03/the-uk-plan-for-bitcoin-is-a-step-in-the-right-direction/.

It is entirely unclear what can be gained by duplicating the enforcement efforts of Federal regulators at the state level. However, to the extent that a state wishes to guarantee that licensees have proper AML controls in place, the CSBS takes a reasonable position in its Draft Model Regulatory Framework. It recommends:

> Required implementation and compliance with BSA/AML policies, including documentation of such policies. Required compliance with applicable ***federal BSA/AML laws*** and recognition of state examination and enforcement authority of BSA/AML laws[.]

This is standard practice and is echoed in several state money transmission licensing. For example, New York's regulations state:

> d. Compliance with applicable federal requirements shall constitute compliance with the provisions of this Part [Sec. 416.1 Anti-Money Laundering Programs].[56]

Moreover it is echoed by California's proposed licensing regime for digital currency business, which correctly makes no mention of AML requirements.[57]

If a state is serious about attracting digital currency business, it must not place a greater burden on these firms than it places on traditional money transmitters. It must not place a greater burden on firms than would other, more restrained states or nations. Accordingly, we strongly urge states to either remain silent with regard to AML requirements or, if necessary, to match Federal standards, and specify that "compliance with applicable federal requirements shall constitute compliance with the provisions of this part."

B. Material Change of Business

New York's BitLicense requires that licensees seek pre-approval from the superintendent for any:

> [N]ew product, service, or activity, or to make a material change to an existing product, service, or activity, involving New York or New York Residents.

Such a requirement is ill-advised. The product release and testing cycle for startups is different than for traditional banks or other financial service companies. Startups will often pivot to new services or do trial tests (*i.e.*, beta testing) of new services in order to probe markets for new opportunities. This experimentation is what allows for innovation despite uncertainty.

The innovator does not know, *ex ante*, what will absolutely succeed, providing customers with the exact product they would have wanted all along. Instead, the innovator tries several

[56] http://www.dfs.ny.gov/legal/regulations/adoptions/banking/ar416tx.htm.
[57] An act to add Division 11 (commencing with Section 26000) to the Financial Code, relating to virtual currency, A.B. 1326, California Legislature 2014-2015 Regular Session (February 27, 2015) *available at* http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201520160AB1326.

products, often with a limited number of users or at small scale, in order to see what sticks. Innovators may even try two versions of a service simultaneously; this is referred to as A-B testing. Subtle differences between these two versions can reveal specific consumer preferences that can significantly improve the user experience.

The agility to try several approaches is essential to innovation in the new and rapidly growing financial technology landscape. If New York licensed start-ups are forced to wait for pre-approval every time they seek to test a new service, these start-ups will likely miss opportunities seized by faster, more agile competitors overseas. Other states should not make the same mistake.

C. Registration or Licensure

A recently proposed bill in the New Jersey legislature seeks to create a registration obligation for digital currency businesses in the alternative to traditional licensing. The bill is structured to mandate that any digital currency business servicing New Jersey customers must register with the relevant state regulator within 30 days of beginning operations.

> No person shall, without completing a registration as set forth in this act, engage in any digital currency custodial activity for more than 30 days. Only a person engaging in digital currency custodial activity as its primary business may complete a registration under this act.[58]

This structuring would allow a business to begin servicing customers immediately rather than waiting for approval and a license. Registrants must generally comply with all of the same compliance obligations as a traditional money transmitter but need not ask for permission before offering services. This approach makes sense in the case of Internet-based service providers given that services are usually offered everywhere by default; i.e. the Internet in New Jersey has all of the same websites open to visitors as the Internet in California. This stands in stark comparison to legacy financial services where the choice to service an area involved a costly and difficult process of moving physical infrastructure into the region or, at least, finding and negotiating with local agents. Limiting or blocking one's online service in states where licenses are pending is a difficult technological feat. States that wish to be leaders in the digital currency and financial technology space should consider a registration-based approach to save service providers the difficulty of fragmenting the availability of their service and lagging against competitors while licenses are pending.

Leading states may also wish to consider offering tax-breaks to innovative companies, as are also proposed in the New Jersey bill.

[58] New Jersey State Legislature, *Digital Currency Jobs Creation Act*, (Apr. 2015) Available at http://www.scribd.com/doc/266842667/NJ-Digital-Currency-Jobs-Creation-Act

D. Agent of the Payee Exemption

Several states have formalized exemptions in money transmission law for so-called "agents of the payee."[59] At minimum, a state offering such an exemption to traditional money transmitters should treat digital currency payment processors similarly. Additionally, there are some states where no formal exemption exists in the statute, but state regulators may consistently interpret their laws as not including agents of the payee. States taking this interpretive approach should consider crafting a formal exemption in the case of *sui generis* digital currency legislation. Payee Agent Transactions should be exempted from licensing and defined as follows:

> Payee Agent Transactions. Transactions in which the recipient of digital currency is an agent of the payee pursuant to a preexisting written contract and delivery of the digital currency to the agent satisfies the payor's obligation to the payee.

or else the exemption should mirror existing language in the state's money transmission statute.

[59] California - SEC. 3. Section 2010 of the Financial Code: "This division does not apply to the following: … (l) A transaction in which the recipient of the money or other monetary value is an agent of the payee pursuant to a preexisting written contract and delivery of the money or other monetary value to the agent satisfies the payor's obligation to the payee."
New York - Banking Law 641.1: "1. No person shall engage in the business of selling or issuing checks, or engage in the business of receiving money for transmission or transmitting the same, without a license therefor obtained from the superintendent as provided in this article, nor shall any person engage in such business as an agent, except as an agent of a licensee or as agent of a payee;"

Conclusion

To be a leader in the future of financial technology, a state must carefully forge a path toward consumer protection and avoid the pitfalls of inartful and unnecessarily costly regulation. As described throughout this report, this path has several essential steps, that (1) only those with unilateral control be subject to a license requirement; (2) innovative and small startups be protected with a non-discretionary on-ramp; (3) licensed firms need not seek a duplicative money transmitter license; (4) capital requirements may be satisfied by holding digital currency, (5) AML requirements, if absolutely necessary at all, at least match and not exceed federal standards; and that (6) changes of business require notification rather than pre-approval. Each state will independently travel this craggy and dimly-lit terrain. The state that reaps the benefits of new technologies, new jobs, and enhanced financial inclusion will be the state that first discovers a path worth following.