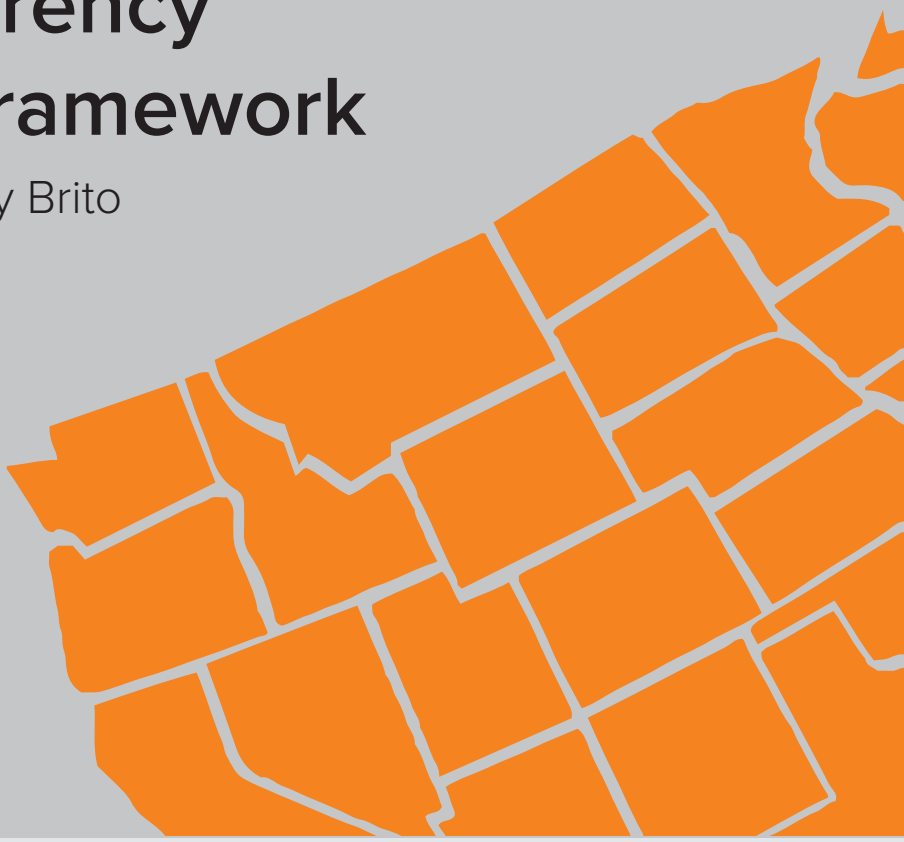
State Digital Currency Principles and Framework

Peter Van Valkenburgh & Jerry Brito

Version 2.0
March 2017



Coin Center Report

COIN CENTER
coincenter.org

Peter Van Valkenburgh and Jerry Brito, *State Virtual Currency Principles and Framework v2.0*, Coin Center Report, Mar. 2017, available at https://coincenter.org/entry/state-digital-currency-principles-and-framework

Abstract

States have begun to look at how virtual currencies, such as Bitcoin, and the businesses that utilize them to provide consumer products, interact with money transmission and consumer protection policy. This report reviews the approaches taken by the several States thus far, and offers model language for a *sui generis* statute or amendment to a money transmission statute. It is not a draft or model bill in full. Instead, language is offered for the essential components of any virtual currency law: Who must be licensed? How do you define "control" of customer virtual currency? How are startups encouraged while still protecting consumers? How is solvency guaranteed?

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 virtual currencies, such as Bitcoin, and the businesses that utilize them to provide consumer products and services, interact with money transmission licensing (MTL) law and consumer protection policy. We begin by characterizing the current regulatory landscape and then offer policy recommendations and some model legislative language.

A. Various Approaches and Disunity Across the States

The fundamental question facing all state banking regulators with respect to virtual currency businesses is: **Do any virtual currency businesses (VCBs) qualify as money transmitters under state law, and, if so, which VCBs qualify specifically (*e.g.* exchanges, wallet providers, software developers, etc.)?**

Apart from how the question is ultimately answered (a matter of substantive policy discussed in later sections of this report) there are seven possible policy approaches to addressing this question (a matter of procedure) that we have observed across the states over the last few years:

1. **Do Nothing** Remain publicly silent on the question of whether VCBs (or which VCBs specifically) must comply with money transmission licensing laws.

2. **Guidance (narrowing)** Explain that only VCBs that also deal in traditional currencies (*e.g.* a virtual-currency-for-dollars exchange) are money transmitters and clarify that businesses dealing strictly in virtual currency are not money transmitters.

3. **Guidance (broadening)** Explain that any VCBs that have control over virtual currency on behalf of their customers[1] will be treated as money transmitters and will need to be licensed (regardless of whether they also deal in traditional currencies).

4. **Rulemaking (*sui generis*)** Promulgate a rule that creates a *sui generis* licensing regime separate from MTL for VCBs that have control over virtual currency on behalf of their customers.

5. **Legislation (narrowing)** Pass new legislation codifying approach 2, above.

6. **Legislation (broadening)** Pass new legislation codifying approach 3, above.

[1] The wording of this standard, mandating licenses from companies who have "control over virtual currency on behalf of their customers" is our own and not the particular language in any guidance or statute. Nonetheless, we believe this descriptive category best explains the activity regulators wish to target for licensure. We feel strongly that "control" be the essential trigger that creates a licensing obligation and the remainder of this report carefully unpacks our preferred legislative language defining control and incorporating that standard into money transmission law or *sui generis* virtual currency licensing law.

7. **Legislation (*sui generis*)** Pass new legislation that creates a *sui generis* licensing regime separate from MTL for VCBs that have control over virtual currency on behalf of their customers.

As of February 2017, no state has taken approach 7, ***Sui Generis* Legislation**, although the **Uniform Law Commission** (ULC) is developing a model law that takes this approach,[2] and a *sui generis* bill in the **California** legislature was proposed but failed to pass.[3]

Connecticut,[4] **New Hampshire**,[5] and **Georgia**[6] have take approach 6, **Broadening Legislation**, and in all three cases the legislature added virtual currency to the definition of *money* but left several substantive policy questions to the regulator.[7] A pending bill in the **Washington** state legislature would also broaden MTL law to include virtual currency businesses.[8]

No state has taken approach 5, **Narrowing Legislation**, although a bill was introduced and failed in **New Hampshire**[9] that would have excluded virtual currency from the definition of money and mandated licensure only from exchanges dealing also in traditional currencies.

Only **New York**[10] has taken approach 4, crafting a ***sui generis* licensing regime for virtual currency through rulemaking**. This may be because only in New York do banking laws grant sufficiently broad authority to the regulator to craft such licensing schemes from whole cloth.

---

[2] *See* ULC *Regulation of Virtual Currency Businesses Act*, *available at* http://www.uniformlaws.org/Committee.aspx?title=Regulation%20of%20Virtual%20Currency%20Businesses%20Act.

[3] *See* California Assembly Bill No. 1326 (2015) *available at* http://www.leginfo.ca.gov/pub/15-16/bill/asm/ab_1301-1350/ab_1326_bill_20160808_amended_sen_v94.htm .

[4] *See* Connecticut Substitute House Bill No. 6800 (2015) *available at* https://www.cga.ct.gov/2015/act/pa/2015PA-00053-R00HB-06800-PA.htm .

[5] *See* New Hampshire House Bill No. 666 (2015) *available at* http://www.nhliberty.org/bills/view/2015/HB666.

[6] *See* Georgia House Bill 811 (2015-16) *available at* http://www.legis.ga.gov/Legislation/20152016/155243.pdf

[7] *See, e.g.*, Peter Van Valkenburgh, "Connecticut and Bitcoin: A legislative question mark" *Coin Center* (June 2015) https://coincenter.org/entry/connecticut-and-bitcoin-a-legislative-question-mark.

[8] *See* Washington House Bill 1045 (2017-18) *available at* http://app.leg.wa.gov/billsummary?BillNumber=1045&Year=2017.

[9] *See* New Hampshire House Bill No. 356 (2015) *available at* https://legiscan.com/NH/text/HB356/id/1073681.

[10] *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* (2015) available at http://www.dfs.ny.gov/legal/regulations/adoptions/dfsp200t.pdf.

North Carolina has taken approach 3, **broadening guidance** explaining that businesses who have control over virtual currency on behalf of customers are money transmitters.[11]

Texas,[12] **Kansas**,[13] and **Tennessee**[14] have taken approach 2, **narrowing guidance**, explaining that only virtual currency businesses who also deal in traditional currencies (*e.g.* a virtual-currency-for-dollars exchange) are money transmitters. **Illinois** is soliciting comments on proposed guidance that would take this approach as well.[15]

The remaining states have taken approach 1, **do nothing**.

B. Which Approach to Choose?

While Coin Center advocates for a light touch regulatory approach to virtual currency technologies, **we do not encourage states to take a do nothing approach**.

Every state except for **Montana** already regulates money transmitters, requiring that such businesses become licensed *before* taking on customers who are residents of the state. The various statutory definitions of money transmission are broad, focused on older payment systems, and difficult to parse with respect to new technologies and business models emerging in the virtual currency space.

Without some clarifying action from lawmakers or regulators, the vague drafting inherent in these state money transmission statutes leaves open the possibility that a virtual currency company with customers in the state will already qualify as a money transmitter under existing laws, and, if operating without a license, will be subject to substantial civil and criminal punishments. This legal uncertainty and looming liability is a real threat to the talented men and women who develop these technologies or start businesses. At the very least, lawmakers and regulators should be clear when it comes to the application (or non-application) of laws that can so easily ruin the lives and livelihoods of our country's most creative and innovative citizens.

---

[11] *See* North Carolina Commissioner of Banks, *Money Transmitter Frequently Asked Questions* (last accessed Feb. 2017) http://www.nccob.gov/Public/financialinstitutions/mt/mtfaq.aspx.
[12] *See* Texas Department of Banking, *Supervisory Memorandum 1037* (2014) *available at* http://www.dob.texas.gov/public/uploads/files/consumer-information/sm1037.pdf.
[13] *See* Kansas Office of the State Bank Commissioner, *Guidance Document MT 2014-01* (2014) *available at* http://www.osbckansas.org/mt/guidance/mt2014_01_virtual_currency.pdf
[14] *See* Tennessee Department of Financial Institutions, *Memo: Regulatory Treatment of Virtual Currencies under the Tennessee Money Transmitter Act* (Dec. 2015) http://tn.gov/assets/entities/tdfi/attachments/2015-12-16_TDFI_Memo_on_Virtual_Currency.pdf.
[15] *See* Illinois Department of Financial and Professional Regulation, *Digital Currency Regulatory Guidance* (2017) *available at* https://www.idfpr.com/news/PDFs/IDFPRRequestforCommentsDigitalCurrencyRegulatoryGuidance2016.pdf.

With *do nothing* off the table, we favor policy approaches that focus on providing **clear, prospective, and public law** that **minimizes regulatory discretion** and **promotes awareness and understanding of the compliance obligations and liabilities that can await innovators** in this space.

To that end we support and encourage states that take either the second, **Narrowing Guidance**, or seventh, ***Sui Generis* Legislation**, approaches.

These technologies bring with them all sorts of new possibilities that were never countenanced in the drafting of money transmission law. Interpreting existing MTL law (via public guidance) to *limit* its application to only those VCBs that also deal in traditional currency ensures that old, ill-fitting regulatory structures are not applied indiscriminately to newer businesses whose technologies may obviate the need for certain compliance obligations and whose customers may not even benefit from legacy regulatory controls. This approach is ideal for states that would prefer a wait-and-see approach. Such an approach is easily justified, especially, given the relatively slow consumer adoption of these technologies (less urgency to intervene), the rapid changes in the technologies themselves (higher likelihood of new rules being rapidly rendered obsolete), and the likelihood that most consumer-facing companies in this space will be exchanges that deal also in traditional currencies and would, therefore, be subject to existing MTL requirements.

For states that *do* want to regulate purely virtual-currency-based businesses (in addition to exchanges) sooner rather than later, we recommend taking the *Sui Generis* Legislation approach. This ensures that the development of new rules will be democratic, open, participatory, and targeted at accommodating the specific risks and benefits inherent in these new technologies (rather than shoehorning their regulation into older structures, or proceeding via arbitrary case-by-case discretion). In the following sections we present legislative language and explanations of the technology that can assist in the careful drafting of such a statute.

For the same reasons, we strongly discourage states from broadening the interpretation of MTL law via guidance (approach 3) or crafting a *sui generis* approach via rulemaking (approach 4, *e.g.* the NY BitLicense).

Approach 6, broadening legislation**,** may be carried out in a manner that does not discourage innovation or erode clarity and the rule of law but only if the specificity with which existing money transmission law is amended is as carefully calibrated to the nuances of the technology as it would hopefully be in the case of developing technology-focused *sui generis* legislation. ***Simply adding virtual currency to the definition of money in the MTL statute is not sufficient, leaves too many questions of application to the discretion of the regulator, and will lead only to confusion and hidden liabilities for honest entrepreneurs.***

The remainder of this report can also be used as an aid in the process of amending existing money transmission statutes, particularly where simple amendments to existing definitions would result in vague and under- or over-inclusive compliance obligations.

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 virtual currency or be a "regulated virtual 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 virtual 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. Just as we would only wish to require licensure from businesses that take it upon themselves to "transmit money" we should only require licensure from VCBs that take it upon themselves to assume ***control*** over keys related to customer bitcoin balances.

For example, a bill was introduced in **Pennsylvania** to amend its money transmission licensing statute in an attempt to cover VCBs.[16] That bill has since failed to pass into law. In an early draft, however, "virtual currency" was added to the definition of "money." The definition of "transmittal instrument" was amended to include "electronic transfer . . . for the payment of money." "Electronic transfer," however, was not defined. Had this draft bill passed in that form, we could 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. All sorts of individuals and businesses transmit and retransmit Bitcoin transaction messages across the virtual currency's computer network, including individuals running software on their home computers, Internet Service Providers (ISPs), and so-called Bitcoin miners. Unlike the consumer facing bitcoin exchanges who presumably should be licensed, none of these non-controlling entities can spend the bitcoins owned by other participants on the Bitcoin network. However, by playing an infrastructure role in these systems do they take part in an otherwise undefined "electronic transfer?" Why leave this question unresolved in vague legislation and simply hope for a good outcome to follow later in administrative rulings or court cases?

Instead, Pennsylvania should have clearly defined the activity that generates consumer risk: the moment when a VCB is actually has "control" over customer virtual currencies. (Such a

[16] *See* Pennsylvania House Bill 850 (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.

definition is proposed in the following section.) Then, the Pennsylvania statute should have proceeded to redefine "money transmission" to include those who maintain *control* of virtual currency on behalf of others.

Developing clear and reasonably calibrated definitions and language for *sui generis* virtual currency legislation or MTL-amending legislation is, however, difficult. Without 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.

The remainder of this report offers model language for a *sui generis* statute or MTL-amending statute. It is not a draft or model bill in full. Instead, language is offered for the essential components of any virtual currency law. For a full model bill we recommend looking at the ULC's Uniform Regulation of Virtual Currency Businesses Act (URVCBA);[17] this framework can also be used to understand the policy reasoning behind several of that bill's substantive and stylistic choices.

Our 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*:

[17] *See* ULC *supra* note 2.

1. Who should be required to obtain a license?

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 virtual currency businesses:

> [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.[18]

Virtual Currency presents a challenge to regulators because virtual currency technology can be utilized to perform activities involving what the CSBS calls "third party control"—activities similar to money transmission, which generate risks to consumers. However, virtual currency technologies can also be used for other unrelated purposes. Virtual currency software or networking technology can be used by businesses to offer a financial service without having control of the customer's funds—the customer uses the software or service in order to maintain control herself. Regulating these parties as money transmitters is akin to regulating safe manufacturers or leather wallet craftsmen as money transmitters; it doesn't make sense.

Virtual currency technologies can also be used by intermediaries to offer a non-financial services (such as a notary service), and these technologies can be used by consumers directly and entirely without custodial intermediaries. In all of these cases, the virtual currency business or service provider is *not* in a position of trust and should not, accordingly, be required to seek a license in order to operate.

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

Intermediaries that do not assume a position of trust, non-financial uses, and individual access are virtual currency innovations that should be encouraged. Non-custodial and non-financial virtual currency businesses can benefit consumers, businesses, and local

[18] 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 *Emphases added.*

economies through improved financial privacy,[19] financial inclusion,[20] and vibrant technology-based economies. These businesses (as well as any academics or hobbyists experimenting with these technologies) should not be burdened by compliance costs that lack concomitant consumer protection benefits. Neither should these low-risk innovators be in perpetual jeopardy of severe criminal liability for failure to license as a money transmitter.[21]

Custodial 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 is narrowly defining that duck. As we will explain in detail, statutes should (1) carefully define "control" of virtual currency as the *de facto* state of holding a customer's virtual currency, (2) use the defined term "control" in a definition of the set of activities that trigger a licensing requirement (*e.g.*, "money transmission" for MTL amendments or "virtual currency safekeeping" for *sui generis* statutes), and then (3) clearly exempt those persons or businesses that do not pose a substantial consumer risk. On the following page is proposed language for these purposes.

[19] *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/
[20] *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/.

[21] 18 U.S.C. §1960(a) ("Whoever knowingly conducts, controls, manages, supervises, directs, or owns all or part of an unlicensed money transmitting business, shall be fined in accordance with this title or imprisoned not more than 5 years, or both").

New or Changed Definitions and Exemptions

Control of Virtual Currency means possession of sufficient virtual currency credentials or authority on a virtual currency network to execute unilaterally[22] or prevent indefinitely[23] virtual currency transactions.

Money Transmission means [*selling or issuing payment instruments, stored value, receiving money or monetary value for transmission* or *other existing definition*], or maintaining control of virtual currency on behalf of a resident of this state.

Or

Virtual Currency Safekeeping means maintaining control of virtual currency on behalf of a resident of this state.[24]

Exemptions
In no event shall any of the following activities, in and of themselves, be interpreted as [*Money Transmission* or *Virtual Currency Safekeeping*]:

1. developing, distributing, or servicing software;[25]
2. contributing software, connectivity, or computing power to a Decentralized Virtual Currency network;[26]
3. providing data storage or security services for a Virtual Currency Business;[27] or
4. engaging in otherwise qualifying activities undertaken for non-monetary purposes,[28] or that do not involve more than a nominal amount[29] of Virtual Currency.

The subsections that follow explain, in detail, each component of our model language.

[22] *See infra* Part 2. B "execute unilaterally" at p. 12.
[23] *See infra* Part 2. C "prevent indefinitely" at p. 13.
[24] Note that the ULC presently has a draft uniform law that regulates *three* activities related to safekeeping: "exchange," "transmission," and "storage." We find this approach acceptable so long as each activity definition in turn utilizes our proposed definition of "control" in order to ensure that only entities posing a risk to consumers are ever categorized as engaging in these regulated activities. Simplifying these activities into a more general category "safekeeping" is also acceptable.
[25] *See infra* Part 2.F "developing, distributing, or servicing software" at p. 17.
[26] *See infra* Part 2.G "contributing software, connectivity, or computing power" and "Decentralized Virtual Currency" at p. 18.
[27] *See infra* Part 2.H "providing data storage or security services" at p. 20.
[28] *See infra* Part 2.I "non-monetary purposes" and "nominal amount" at p. 22.
[29] See *Id*.

A. "Control of Virtual Currency"

The determination of which businesses warrant regulation and which do not should be made by reference to what harm the business is capable or incapable of doing, rather than whether they—vaguely and metaphysically—"hold" or "store"[30] units of virtual currency.

The only businesses that are truly capable of harming their virtual currency customers are those that can lose (*e.g.*, through hacking), misspend, permanently immobilize, or fail to protect the customer funds to which they are entrusted. Therefore, licensure should only be required from those businesses that, on their own, can *execute or prevent a virtual currency transaction* of customer funds. These are the parties who "control" customer virtual currency, and this is the relationship with customers that raises the potential for virtual currency loss.

The CSBS has made it clear in their policy statement that it is only this position of trust that should trigger regulation.[31] Additionally, the Uniform Law Commission (ULC) has developed draft language for a model bill that uses our proposed definition of "control of virtual currency" to more carefully delineate this category of trusted VCBs.[32] That definition, again, is:

> **Control of Virtual Currency** means possession of sufficient virtual currency credentials or authority on a virtual currency network to execute unilaterally or prevent indefinitely virtual currency transactions.

In the ULC draft, all regulated categories of activities reference this "control" definition. Thus, virtual currency "storage" is defined as "maintaining control of virtual currency on behalf of a resident…" and (7) "Exchange" means to assume control of virtual currency from or on behalf of a resident, at least momentarily, in order to sell, trade, or convert:(A) virtual currency for legal tender or for one or more forms of virtual currency; or (B) legal tender for one or more forms of virtual currency."[33]

We believe this is an appropriate approach so long as every regulated activity is defined to limit coverage to those businesses and individuals who have, at least momentarily, control over customer virtual currency. Note, however, that the ULC definitions of transfer and exchange could be interpreted to cover persons who are merely transmitting or exchanging *their own* virtual currency (*e.g.* I send my personally held virtual currency to a resident in a state that follows the ULC approach, or I sell my own virtual currency to a resident of that

---

[30] 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.

[31] *See* CSBS *supra* note 17.

[32] *See* ULC *supra* note 2.

[33] *See* ULC *supra* note 2.

state because I wish to cash out a personal investment). Because of this potentially overbroad application, a state that chooses the ULC approach rather than merely licensing those who engage in safekeeping, must also include a detailed personal use exemption (as also employed by the ULC as well as FinCEN).[34] Alternatively, the various activities could also be consolidated into one "safekeeping" activity, defined as "maintaining control of virtual currency on behalf of a resident of this state."

In the following two subsections the specifics of our proposed definition of control, "execute unilaterally" and "prevent indefinitely," are explained.

B. "Execute Unilaterally"

Virtual Currency allows for programmatic money. Software can manipulate the virtual 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.[35] 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 keys (N) are required to move funds. This is referred to as *M-of-N* transactions[36] or, more simply, "multi-sig."

Given multi-sig, some parties may have only one of several keys necessary to execute a virtual 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 in control of virtual currency. These minority key-holders cannot, solely by their own negligence or malice, lose consumer value. This is why our proposed definition of "control" includes the word ***unilaterally.*** That caveat is critical. Minority key-holders can play highly valuable consumer-protective roles in the virtual currency ecosystem as fraud-monitors or disaster recovery services. They should be encouraged in their development. Moreover, if they cannot abscond with or otherwise lose a

[34] That exemption should be drafted as follows: "(The following are exempt:) a person that mines, manufactures, buys, sells, exchanges, or otherwise obtains or relinquishes control of virtual currency solely for personal purposes if the person does not engage in any virtual currency business activity on another person's behalf. Personal purposes include buying or selling virtual currency as an investment, researching virtual currency or related technologies, and obtaining virtual currency as payment for the purchase or sale of goods or services."

[35] *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/.

[36] *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/

customer's funds, mandating their licensure serves no consumer-protective or prudential-regulatory purpose because no solvency risk exists within their business model.

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 virtual 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 money 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 virtual 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 hacking thefts.[37] Defining control to include only those who can **unilaterally** execute a transaction, ensures that these tools can be developed without subjecting their creators to a licensing regime that adds costs to their business without delivering any benefits to consumers. This definition also sends a credible and welcome signal to innovators in the virtual 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*.

C. "Prevent Indefinitely"

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. 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 for service-providers is as follows:

1. unilaterally able to transact on user's behalf
2. able to block transaction on user's behalf indefinitely

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

3. 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 virtual currency licensing. Configuration (3) poses no solvency risk to consumers.

It should also be noted that clearly exempting services that employ these configurations from money transmission licensing does not leave the customers who utilize these services fully outside of consumer protection law. 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 time-lock services—who already are in a far less vulnerable position than users of truly custodial services—while also enabling permissionless innovation.

Moreover, time-locked transactions are 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. The following two 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 money transmitters or licensed virtual currency businesses.

Indefinite Prevention. In rare situations, a business could have sufficient keys to block a consumer from transacting with her virtual 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, which is 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 virtual 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 any other money 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 indefinitely prevent transactions pose similar risks to consumers and assume a similar level of trust as traditional money transmitters. They should be regulated accordingly.

Temporary Prevention. 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 (typically around 10 minutes or less) in which they are capable of incorporating or not incorporating requested transactions into the currency's blockchain. Additionally, as discussed, the Bitcoin protocol also 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.[38] Say, for example, you were a cellular network provider and you wanted to charge your network users for every kilobyte of data they 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

[38] 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/.

"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 refund transaction to the service provider and asks him to sign it as well and send it back to her. Now she checks the signature and holds onto that refund transaction just in case anything goes wrong in the future. Only then does she put her $5-worth of bitcoin into the multi-sig address. Because she has the signed refund transaction the user is guaranteed that she can 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 ever 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 and more data. Eventually, when the user is done with the service provider (say she has left the service provider's range or simply doesn't want to use any more data) 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 from the description above. 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 for a definition of 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 channel providers may be excluded from licensure 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 channels may be established between two or more individuals for the purposes of paying each other. The reason for creating these channels is the same as in the merchant-customer context: to allow networks like Bitcoin to scale more efficiently by bundling several small transactions together before settling them to the blockchain. 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 providers of such channels can never lose or run-off with the funds—and therefore these technologies should be regulated under different consumer-protective regimes such as contract or unfair and deceptive practices law rather than money transmission licensing.

In order to avoid potentially metaphysical and unproductive discussions over what "temporary" may mean with reference to the "temporary ability to prevent transactions," our model framework strongly advocates for the use of the phrase "indefinitely prevent." Only those who can lock a customer from access to her valuables for an arbitrary and indefinite period of time engender the same solvency risks as money transmitters.

D. "On Behalf of a Resident of this State"

Individuals should not be regulated as money transmitters or licensed virtual currency businesses when they deal only in their own funds; therefore, licensing regulations should clearly indicate that only activities performed "on behalf of a resident of this state" rise to the level of requiring licensing. 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 this 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. In this arrangement, where the user of the network has assumed the risk of safekeeping her own funds, there is no third party to regulate as a money transmitter or virtual currency business.

E. "Non-qualifying Activities"

The diversity of business models and activities enabled by virtual 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 Money Transmission or Virtual Currency Safekeeping.

F. "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 virtual currency should not be an activity that requires a license.

At no point does a mere 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 do not pose a solvency risk and should not be regulated accordingly. Additionally, the mere production and distribution of software is protected speech under the First Amendment.[39] 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.

G. "Contributing Software, Connectivity, or Computing power" and "Decentralized Virtual Currency"

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

Centralized virtual 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 virtual content on its sites.[40] 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 national 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 dollars/euros (defunct); Second Life "Linden dollars"; PerfectMoney; WebMoney 'WM units'; and World of Warcraft gold."[41]

Decentralized virtual currencies, by contrast, are created and maintained by an open community of interested participants using open source software. These participants run the

---

[39] *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.").

[40] *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.

[41] 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.

software, or a compatible modification of the software, on Internet-connected computers that, together, form an open peer-to-peer network. Decentralized virtual 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 control, and (B) that the money supply grows at a predictable rate. Bitcoin, launched in 2009,[42] was the first cryptocurrency, and as of 2017, it remains the largest by market capitalization.[43]

Decentralized Virtual Currencies should be defined as follows:

> *Decentralized Virtual Currency.* Decentralized Virtual Currencies are virtual 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 may warrant heightened licensing requirements for developers of centralized currencies over their decentralized counterparts. A business developing and maintaining a centralized virtual currency can unilaterally decide to devalue consumer balances by issuing more currency, similar to how a normal financial service provider 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 virtual 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 virtual 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 virtual currency business can operate using closed source software, meaning the underlying scarcity or safety of the currency cannot be easily audited by outside 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 virtual currencies may be released and updated primarily by an individual or group of individuals, *e.g.*, Bitcoin's "Core Devs,"[44] 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

[42] *See* Satoshi Nakomoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, (May 2009) *available at* https://bitcoin.org/bitcoin.pdf.
[43] *See* Market capitalization of top cryptocurrencies *available at* http://coinmarketcap.com/.
[44] *See* List of Bitcoin Core Developers *available at* https://bitcoin.org/en/development.

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 virtual 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 will be rejected by other network participants.

Therefore, individuals and businesses contributing to a decentralized virtual 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 also able to unilaterally execute or indefinitely 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 virtual 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.[45]

This approach is well-advised, allowing regulators to focus on trusted intermediaries who control customer 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 not unintentionally swept into a licensing regime, they should be clearly exempted by including the following language within a passage describing exemptions or on non-qualifying activities: "contributing software, connectivity, or computing power to a Decentralized Virtual Currency."

[45] 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.

H. "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.[46] 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.[47]

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.[48] If a Bitcoin hosted wallet provider 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 virtual 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 security. Moreover, as long as the consumer-facing business is a regulated entity, the protections of a Money Transmitter or Virtual Currency Business license will remain in effect for consumers.

---

[46] *See infra*.

[47] 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.

[48] Amazon, *AWS Case Study: Netflix*, http://aws.amazon.com/solutions/case-studies/netflix/ .

Such a carve-out has been the longstanding norm for companies that are the legal agent of licensed money transmitters.[49] 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.[50] FinCEN also exempts those who only provide "the delivery, communication, or network access services used by a money transmitter to support money transmission services."[51] Virtual Currency regulations should include a similar exemption in order to promote the development of enhanced security tools and services.

I. "Non-Monetary Purposes" and "Nominal Amount"

The technology underlying decentralized virtual currencies has promising applications apart from the provision of money transmission services. Distributed ledgers (or "blockchains") are used within virtual 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, identity and authorization services (*e.g.* Blockstack), 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 LTD) 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 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

[49] *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.").
[50] 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.").
[51] 31 C.F.R. § 1010.100(ff)(5)(ii)(A).

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.[52]

Accordingly, non-monetary transactions of *nominal* amounts should be outside the scope of Third Party Control of Virtual Currency regulation.

[52] 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. How can startup businesses be encouraged while keeping consumers safe?

Virtual 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 and individuals working with freely available software and an open network.[53]

A. Why Virtual 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 virtual 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.[54] 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.[55] 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

New York's Bitlicense, for example, rightly contemplates the need to exempt small and innovative virtual 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.[56]

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.

---

[53] 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).

[54] 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-.

[55] *Id.*

[56] BitLicense, *supra note 10*, 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 a De Minimis Exemption and On-Ramp for Startups

Small startups, academics, and hobbyists can be shielded from the costs of regulation and the severe criminal penalties that failure to license can trigger[57] by explicitly exempting them from regulation up until the point at which they pose non-trivial consumer risks; we can refer to this as a *de minimis exemption*. 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; we can call this an *on-ramp* for startups. Language on the following page illustrates such exemptions.

[57] Courts are increasingly coming to the conclusion that virtual currencies such as Bitcoin qualify as "money" under various statutory definitions. 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. 18 U.S.C. §1960(a).

Exemptions.

A. *De Minimis Exemption*. Businesses or individuals shall be exempted from regulation and licensure under this part if:
    1. the business or individual's average aggregate outstanding virtual currency obligations[58] to customers remain below $1 Million in value according to a rolling 30-day average of outstanding balances converted into a dollar amount using each day's prevailing exchange rate,
    2. the business or individual has registered with federal authorities as a Money Services Business if applicable, and
    3. the business or individual discloses its unlicensed status to customers.

B. *On-Ramp*. Businesses or individuals that surpass the $1 Million threshold shall be exempted from regulation and licensure under this part, for a period of time beginning when the Commissioner/Superintendent 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/Superintendent 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.

We believe a $1 million per year transaction level is an appropriate threshold between companies that can pose serious, systemic risks to consumers (*e.g.* Mt. Gox[59]) and those where risk-level is tolerable given the benefits that unfettered start-up innovation can bring. However, a regulator or legislature 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

[58] The threshold for consumer risk should be based upon the amount of consumer funds over which the company has control. 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.

[59] 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/.

explicit, apply generally across the industry, and be announced in advance so that firms can plan their compliance strategies efficiently.

3. How should new virtual currency law interact with state money transmission law?

A virtual currency exchange should not need to acquire both a money transmission license and a virtual 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 virtual currency license, therefore, there is no apparent public benefit from going through the expense and trouble of acquiring a second license. Similarly, if a virtual currency business has already obtained a money transmission license there is little to be gained from a separate inquiry and licensing process for virtual currency. In short, if a virtual 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 traditional currencies in addition to virtual currency?

Additionally, statutes should clearly specify this interchangeability to avoid any confusion. Courts are increasingly coming to the conclusion that virtual currencies such as Bitcoin qualify as "money" under various statutory definitions.[60] 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.[61] State legislators surely do not wish a licensed virtual 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.

[60] 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).
[61] 18 U.S.C. §1960(a).

4. How should capital requirements be structured?

To protect consumers, licensed businesses should be required to have sufficient capital reserves on hand to guarantee the solvency of the institution. In typical 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.[62] 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 which are, of course, also denominated in cash. Virtual currency businesses should face similar standards. If the business holds virtual currency 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/superintendent, each licensee shall hold either:
    1. virtual currency equal in form and quantity to customer deposits, or
    2. high-quality, investment-grade investments.

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

5. What other important considerations remain?

New York was the first state to craft a virtual 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 virtual 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[63]—the first of its kind for state money transmission law—and a requirement that duplicates the efforts of FinCEN.[64] 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[65] that similarly doubles the efforts of FinCEN.[66] 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 virtual currency regulation.[67] 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).

---

[63] BitLicense, *supra note 10*, at § 200.15 (e)(3).
[64] 31 C.F.R. § 1022.320.
[65] BitLicense, *supra note 10*, at § 200.15(e)(2).
[66] 31 C.F.R. § 1010.330.
[67] *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].[68]

Moreover it was echoed in the only other proposed *sui generis* bill to date, **California's** yet-to-be-passed licensing regime for virtual currency businesses, which correctly made no mention of AML requirements.[69] The same goes for the ULC's current draft model law, which simply mandates that licensees must have:

> Procedures and controls to ensure that, to the extent mandated by federal law or guidance published by federal agencies responsible for enforcing federal laws, all reports specified by federal currency reporting, record keeping, and suspicious transaction reporting requirements as set forth in 31 U.S.C. Section 5311, or 31 C.F.R. Part X, and any other federal of state laws pertaining to deterrence or detection of money laundering or terrorist financing are filed on a timely basis.

If a state is serious about attracting virtual 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:

---

[68] http://www.dfs.ny.gov/legal/regulations/adoptions/banking/ar416tx.htm.

[69] 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.

> [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 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 startups are forced to wait for pre-approval every time they seek to test a new service, these startups will likely miss opportunities seized by faster, more agile competitors overseas. Other states should not make the same mistake.

C. Registration or Licensure

A bill in the **New Jersey** legislature seeks to create a registration obligation for virtual currency businesses in the alternative to traditional licensing. The bill is structured to mandate that any virtual 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 virtual currency custodial activity for more than 30 days. Only a person engaging in virtual currency custodial activity as its primary business may complete a registration under this act.[70]

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

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

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 virtual 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.

D. Agent of the Payee Exemption

Several states have formalized exemptions in money transmission law for so-called "agents of the payee."[71] At minimum, a state offering such an exemption to traditional money transmitters should treat virtual 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* virtual currency legislation. Payee Agent Transactions should be exempted from licensing and defined as follows,

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

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

[71] 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 virtual 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.