Date: 2/26/2016

From: Peter Van Valkenburgh
Coin Center
718 7th St NW,
Washington, DC 20001
peter@coincenter.org
(703) 338-4456

To: Sarah Jane Hughes, Committee Members, and Observers

Writing on behalf of Coin Center, a Washington, D.C. based non-profit cryptocurrency technology research and advocacy center, I'd like to offer some specific written comments primarily regarding the definitional section of the model law to license virtual currency businesses.

Definitions of Virtual Currency Business Activity (VCBA) and the "Verbs"

In traditional financial services, terms like "exchange," "transfer," and "deposit" have reasonably well-established meanings built from years of industry custom and law. But these terms, when applied to describe activities that virtual currency businesses (or indeed individuals, amateurs, or academic institutions) may perform, do not have clear meanings, because the technology enables services that have imperfect analogies with traditional services, and also allows for new services that have no precedent in the traditional financial services sector.

We agree that performing certain widely understood activities—verbs—on behalf of others should trigger a licensing requirement, specifically "exchange, transfer, and storage" of virtual currency. However, we believe that these verbs need to be defined, and that key to the definition of these verbs is a definition custody (what it means to legally have or control someone else's virtual currency) and a definition of control (what it means to de facto have or control someone else's virtual currency). Both these activities, custody and control, can be then used to define exchange, transfer, and store.

For the definition of custody (the *de jure* state of having someone else's virtual currency) we propose modifying the definitions related to custody of securities found in Article 8 of the UCC. The language we propose is:

- **Custody of Virtual Currency** means maintaining an account to which virtual currency is or may be credited in accordance with an agreement under which the person maintaining the account undertakes to treat the person for whom the account is maintained as entitled to the use and benefits of that virtual currency.

A business has custody of virtual currency when it

(1) indicates by book entry that an amount of virtual currency has been credited to a user's virtual currency account;

(2) receives control of virtual currency from the user or acquires control of virtual currency on behalf of the user and, in either case, accepts this control for credit to the person's virtual currency account; or

(3) becomes obligated under other law, regulation, or rule to credit virtual currency to the person's virtual currency account.

As you will note, the second condition that triggers a custodial arrangement includes "receives control of virtual currency from the user." In the Article 8 context the language is "receives a financial asset from the person or acquires a financial asset for the person." The act of "receiving" virtual currency is not intuitive and it is not easy to define.

When does a person *actually* receive it? The key to understanding when I "receive" virtual currency is that at some point after a sender of virtual currency has chosen to send me some funds, because of the actions of others (people sending transactional messages to and from the network) I will have possession of *credentials sufficient to transact*, myself, using that virtual currency. Note, however, that the sender does not actually *send* me these credentials. I have credentials that I use on the network and they have credentials that they use on the network.

When someone sends virtual currency, they sign a message signed with their credentials, the network acknowledges that message, checks the signature, and (if it is valid) the network will reassign the specified amount of virtual currency from a state of control by the sender's credentials to a state of control by the recipients credentials. Therefore the only way to define receipt of virtual currency is to define the moment when someone obtains "control" over that currency according to the decentralized network (or centralized administration in the case of centralized virtual currencies). "Control" then fundamentally means having sufficient credentials to have the *ability* to unilaterally execute or prevent transactions on the virtual currency network. The definition we therefore propose is:

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

Note that we have added in this language "or authority on a virtual currency network" this language is intended to cover centralized virtual currency administrators who will always (by virtue of being the only--hence centralized--parties maintaining records on that network), *always* have the ability to make transactions on that network.

Especially important to this definitions is the word "unilaterally." Control over an amount of virtual currency can be divided between multiple persons. In situations where a business or individual has *some* virtual currency credentials but insufficient credentials to actually transact, we do not believe these non-custodial credential holders should need to get a license. Parties performing this function, often called mult-sig key recovery services, ***do not carry solvency risks*** because they are unable to hypothecate, move, or utilize the virtual currency to which they hold some credentials. These parties also present ***substantially less consumer protection risk*** because should they be negligent in the storage of these credentials (either because of poor cybersecurity or other internal mismanagement) ***the customer will not lose her virtual currency***. She still retains sufficient credentials to transact apart from the back-up key that has been lost by the business. To the extent that these entities do present *some* consumer protection risk (because if both the business, as well as the customer, lose their credentials simultaneously then funds may be unrecoverable) ***these risks are best addressed through other legal and regulatory regimes than licensing (which principally deals with solvency risk), such as State and Federal Unfair, Deceptive, or Abusive Acts and Practices Law (UDAAP), and Contract law.*** Further, should these legal tools prove insufficient, then new laws may at some point be necessary. However, ***it is premature*** to craft those laws *now* in the context of what will hopefully be a state law regulating actual businesses that currently *do* hold true control or custody over customer virtual currency.

With a clear definition of custody (the *de jure* state of holding other people's virtual currency) and control (the *de facto* state of holding other people's virtual currency) we can then define the various actions we want to regulate:

- **Virtual Currency Transfer** means assuming custody or control of virtual currency from or on behalf of a user and either crediting that virtual currency to the account of another user or relinquishing control to another user or person.

- **Virtual Currency Storage** means maintaining custody or control of virtual currency on behalf of a user or person.

- **Virtual Currency Exchange** means the exchange of virtual currency for money or for other virtual currency when the exchanger has, at least momentarily, custody or control of the virtual currency being exchanged.

And then, finally, these verbs can be used to make a definition of Virtual Currency Business Activity, which would be the action that falls within the scope of this model law.

- **Virtual Currency Business Activity** means engaging as a business in virtual currency transfer, storage, or exchange on behalf of another.

That covers the verbs, hooray (or w00t! as we say). Now, what isn't covered?

Exclusions from the Definition

We agree that within the definition of VCBA there should be a list of excluded activities as found above. We've agreed in meetings that (i), (iv), (v), (vi) below are necessary to exclude. I would like to draw your attention to (ii) and (iii) below, which are exclusions we believe are essential to the future viability of the technology:

- The term Virtual Currency Business Activity does not include (i) contributing connectivity, software, or computing power to a decentralized virtual currency *network*; **(ii) possessing insufficient virtual currency credentials to unilaterally execute or prevent virtual currency transfers; (iii) possessing, for a reasonably time-limited period, virtual currency credentials sufficient to prevent virtual currency transactions in order to provide a service such as escrow or transaction management;** (iv) obtaining virtual currency solely to purchase goods or services for personal, family, or household purposes or to purchase inventory or equipment for their own purposes; (v) receiving virtual currency from the purchase or sale of goods or services; (vi) obtaining virtual currency for investment purposes.

The first of these, (ii), clearly specifies that those failing to meet the unilateral condition described above are not covered. Again, businesses or individuals that limit themselves to these activities do not exhibit solvency risks, and exhibit substantially reduced consumer protection risks that would not be well-addressed by a new state-level licensing framework, and would be better controlled through other, extant law, or new laws that are premature to draft at this point.

The second, (iii), deals with an innovation that is still on the horizon. In order to scale, some virtual currency networks may require so-called, micro-transaction channels (e.g. the Lightning Network). These networks are in some ways similar to the networks of miners that help validate transactions on decentralized virtual currency networks (whom state regulators and Federal AML regulators have repeatedly said they do not wish to regulate under money transmission frameworks). They play an intermediary role on the network, but not a custodial role that generates a risk of loss.

Rather than describe the technical specifics of these networks, I'd like to share with you the risk profile of individuals or computers participating in these channels with respect to the amounts of other people's virtual currency traveling through them.

A participant in these channels (and they may simply be running software without realizing that it takes part in these channels) may at any given time have the ability to prevent another individual on the network from transacting with a small amount of virtual currency, effectively they are in a position similar to an escrow provider except they cannot run-off with the value they are holding (they can only "prevent" transactions not "execute" them). This ability to prevent transactions will, however, be time-limited such that full control of the value is automatically returned to the user of the microtransaction channel after a set period of time (*even if the participant disappears or tries to stop the refund from happening)*. The

exact length of this time will vary but should be calibrated to achieve the needs of the microtransaction service user without locking the user away from her funds for an unacceptable amount of time.

Additionally, these microtransaction networks are organized as webs like the Internet. If one path through the web is temporarily blocked, the network will route around that blockage by finding other pathways that connect to the destination. At no point will the user be blocked from transacting by a party on this network, and at no point will her funds be locked out of her control for longer than an *ex ante* specified short period of time.

Given this risk profile we believe participants in this network or similar arrangements should not need to get a license so long as the ability to prevent transactions is reasonably time-limited. Moreover, should these still-developing services at some point require regulation beyond what would already apply under contract, and state and federal UDAP or UDAAP laws, those laws should be drafted in a separate proceeding. ***It is premature to regulate these activities in this model bill.***

Other Concerns

The material above is, we believe, imperative to drafting a model law that covers risky virtual currency businesses but still allows the technology to grow and develop. Failure to make these clear definitions and exemptions can only result in the functional outlawing of many innovative technologies at the state level, and an inevitable migration of these innovative businesses or technologists to more favorable jurisdictions overseas.

The material below is less critical. However, because the discussions at these meetings have raised some of these points, we choose to address them.

Exempting Vendors

Because our proposed definitions of virtual currency exchange, transfer, and storage include both legal (established by agreement with user) and de facto (established by technological capability) triggers, we must necessarily ask ourselves the following question:

If a customer-facing service says it is performing these services but, in fact, uses a vendor to perform them, who should be required to get a license?

The language we have just proposed thus far *would require licenses from BOTH.* This is because the customer-facing service will have "custody" as defined, by virtue of having an agreement with the customer, and the vendor will have "control," by virtue of having sufficient credentials to unilaterally execute or prevent transactions.

We believe that this double licensing is inefficient and that the ultimate responsibility for safety and soundness should fall on the customer-facing entity. Only the customer-facing entity should be required to be licensed, because they and they alone hold themselves out as

a provider of these services. They assume the risk. Accordingly, we should define another set of activities and exempt them them from the licensing requirement:

- **Virtual Currency Control Services Vendor** means a person who has control of virtual currency pursuant only to an agreement or agreements with a person or persons who assumes virtual currency custody on behalf of another.

The exemption section of the model bill would then exempt Virtual Currency Control Services Vendors as it does Banks and some other parties.

Issuance or Administration

We do not believe that "issuance" or "administration" should be among the verbs that trigger a licensing requirement. Issuing units of these new scarce tokens or assets is trivially easy, as simple as building a database or writing network software, but no customers are endangered until the issuer does, in fact, *sell* or *exchange* these assets with consumers or business for real money or other, already established virtual currency. In short, the "exchange" activity already requires that these sorts of risky issuers be licensed. Ambiguity over what "issuing" otherwise means beyond exchange could endanger academic research that may "create" or "issue" units of a cryptocurrency apart from any sales to users, and therefore issuing should not be included as a trigger for licensure.

If, however, the commission *does* believe that issuing should be included, we propose a definition of that activity that would be sufficiently specific as to avoid unintentionally limiting low-risk academic activities. This definition is based on language from the FATF Report: Virtual Currencies – Key Definitions And Potential AML/CFT Risks.[1]

- **Virtual Currency Administration** means issuing a virtual currency *and* having authority to redeem the currency (withdraw it from circulation).

Thanks and Further Questions

Thank you for your time and attention. It's been a pleasure working with all of you on this model bill. If you have *any* questions regarding this comment please do not hesitate to email me at peter@coincenter.org, or call me at (703) 338-4456. I look forward to seeing you all in Chicago.

Best regards,

[1] *See* FATF REPORT, *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