August 11, 2016

RE: AB 1326

Chairman Steven M. Glazer
Senate Banking and Financial Institutions Committee
State Capitol, Room 405
Sacramento, CA 95814

Chairman Glazer and members of the Committee:

On behalf of Coin Center, I am writing to you in opposition to AB 1326 as presently drafted.

Coin Center is an independent nonprofit research and advocacy center focused on the public policy issues affecting decentralized digital currencies. Our mission is to build a better understanding of blockchain technologies and to help develop sound public policy for the digital currency space. 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.

Our supporters include the top companies and investors in the digital currency space, including Andreessen Horowitz, BitPay, Blockchain, Blockstream, Coinbase, Gem, Xapo (all California-based companies), as well as developers, academics, hobbyists, and enthusiasts. More information can be found on our website coincenter.org.

Last year, Coin Center wrote to you in support of AB 1326 because the language in the bill at that time would have created a smart licensing regime for virtual currency businesses. The amended bill now before you is a completely re-written bill from that which passed the Assembly last year, and it not only provides no regulatory clarity, it will likely stifle innovation if enacted unchanged.

The purpose of AB 1326 before it was amended was to provide regulatory clarity for businesses who have long been in a sort of regulatory limbo when it comes to money transmission law in California. The Department of Business Oversight (DBO) has refused to grant digital currency businesses money transmission licenses and has also refused to issue an authoritative statement saying that such businesses do not need to license.[1] The new bill is silent on the question of money transmission licensing—preserving that uncertainty—and instead sets up a new and separate enrollment scheme with which businesses will also have to comply. At the very least we would expect the creation of a new "enrollment program" would take the place of money transmission licensing, thus providing clarity. If it does not, then it is difficult to see what is the purpose of this bill.

Looking at the language in the bill, Coin Center is primarily concerned with four definitions that are components of the definition of "digital currency business," the superset of entities that must enroll as part of the enrollment program. We appreciate that the enrollment scheme does not have minimum capital requirements or costly bonding or insurance obligations, and serves primarily as a means for the DBO to develop policy in this space. However, enrollment is still mandated as a condition to engaging in the regulated activities, and serious penalties (as much as $25,000 in fines per offense) could await those in California (or serving California users) who fail to enroll.

Accordingly, we believe that enrollment should only be required of entities who present a true risk to consumers. To tailor that category appropriately, the definition of "storing" should be modified as we suggest below, and the terms "transmitting," "issuing," and "exchanging" should be struck from the definition of "digital currency business." We supported last year's version of AB 1326 in large part because that bill *only* regulated the *storage* of virtual currency (specifically those with "full custody or control"), which is, again, the core activity that generates a consumer protection risk.

Below you will find our proposed definition of "storing" and an in depth explanation of why the other activities—transmitting, issuing, and exchanging—should be struck from the definition of "digital currency business."

"Storing" digital currency

The definition of "storing" is written as a non-exhaustive list of activities. What we mean is that "having custody or control of digital currency" is defined as "including" having access to credentials, having the ability to execute a transaction, or having the ability to prevent a transaction. Because the word "include" is used, this means that there are other activities that may constitute "having custody or control." We believe that to achieve the clarity this bill seeks to provide, the list should be exhaustive, and thus the word "include" should be removed.

[1] *See* Tanaya Macheel, *California Leaks, Retracts Bitcoin-Friendly Statement*, American Banker, May 22, 2015, *available at*
http://www.americanbanker.com/news/bank-technology/california-leaks-retracts-bitcoin-friendly-statement-1074510-1.html

Additionally, there are many companies and individuals that participate in digital currency networks in a manner which may involve having access to *some* “digital currency credentials” but does not give that individual or company the ability to execute or prevent a transaction on the network. These activities do not generate the type of risks to consumers that necessitate consumer protection regulation in the form of licensing.

The real innovations in this technology do not pose consumer risk; to the contrary, they limit a service’s ability to transact or block a consumer from transacting with her own funds. By including these technologies in a licensing or enrollment regime you will be preventing unimpeded experimentation with these tools in California. These non-custodial participants develop and provide fundamental infrastructure to these networks. Without these services and technologies, the network as a whole is *less* secure and *less* capable of providing real improvements in speed and efficiency over traditional payments system. Customers of businesses using these networks will, as a result, be harmed by a licensing process that chills these innovations.

Additionally, some companies and individuals may *temporarily* have the ability to prevent transactions and may, along with the affirmative participation of the customer or a third party, have the ability to transact. These activities also do not give rise to the sort of solvency risks that necessitate licensing or enrollment and these activities are also fundamental to security and scaling of the technology as a whole. Therefore, only those who have *sufficient* access to a customer’s credentials to execute transactions or to *indefinitely* prevent the customer’s digital currency should be subject to licensing or enrollment.

We are heartened that in the exemptions section an effort has been made to exempt companies developing innovative and non-custodial technologies. However, these exemptions reference a definition of “storing” that is too inclusive. In many ways, the definition of “storing” as now written undoes what the exemptions try to accomplish. As a result they fail to offer safe harbor to the great majority of potential non-custodial innovations.

Given all this, we would suggest these changes:

> “Storing,” with reference to digital currency, means to have custody or control of digital currency on behalf of others. For the purposes of this subdivision, custody or control of digital currency means having ***sufficient*** access to a customer's digital currency credentials ***to execute a digital currency transaction on behalf of the customer or to prevent indefinitely the customer from executing a transaction in the customer’s own digital currency;*** ~~, the ability to execute a~~

> ~~digital currency transaction on behalf of a customer, or the ability to prevent a customer from effecting a desired transaction of such digital currency;~~

To the extent that non-custodial entities do present some consumer protection risk (because, *e.g.*, 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, 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.

"Transmitting" digital currency

As drafted, the definition of "transmitting" is confusing. It now reads:

> "Transmitting" digital currency means the transfer of digital currency, by or through a third party, from one person to another person, or from one storage repository of digital currency to another storage repository of digital currency;

Is the third party mentioned in the definition the Digital Currency Business or someone else? If it is the Digital Currency Business, then the definition is self-referential and circular.

This circularity aside, we do not know who is meant to be covered by a definition of transmitting apart from those already covered by the definition of "storing." Several parties in these networks transmit digital currency transaction messages, but only the party who can validly sign a message with credentials that control bitcoins is capable of actually transmitting value (everyone else is only providing communications infrastructure). The definition, however, seems to cover transmission as something distinct from storing credentials, which leads to several questions.

For example, do internet service providers (*e.g.* Comcast or Time Warner) "transmit" by relaying digital currency transaction messages to and from participants on the currency's peer-to-peer network? They do, but are they then digital currency transmitters? Surely not, but a statute with such wording would not clearly foreclose that interpretation, and the result is complexity and uncertainty in both compliance and enforcement.

Do digital currency miners or those running so-called "full-node" software relay and receive these same transaction messages? Yes. Do they therefore "transmit" digital currency even though they can never misdirect or assume control over the funds that are described in those messages? The current language of this bill is unclear on this question as well.

Digital currency networks rely on miners and full-node software-running participants in order to function, and these participants, in turn, do nothing beyond developing and running free and open source software on their internet-connected computers and relaying digital currency transaction messages. Restricting the ability of Californians to participate in these activities without first enrolling in a regulatory program reduces the ability of Californians to learn about these new technologies, experiment with them, and innovate. An enrollment scheme for merely running software and relaying messages would be antithetical to the permissive and inclusive culture of innovation for which California has become globally renowned.

We are heartened that in the exemptions section an effort has been made to exempt those who provide connectivity or computing power to the network, *e.g.* miners or those running full nodes. However, this exemption is confounded by a definition of "transmitting" that appears to have no target other than these exempted parties. We can think of no entity that engages in "transmitting" but does not also engage in "storing" credentials, other than, perhaps, miners, full nodes, and internet service providers. As a result, either the definition covers only parties who are intended to be exempted or it covers no one. A court interpreting this language would likely employ the rule against surplusage, a canon of construction holding that no passage should be interpreted to mean nothing, or add nothing, to a statute.

If we are misinterpreting the intent of the legislation, we'd very much like to understand who is meant to be covered under the proposed definition of transmitting (but is not covered by the definition of storage).

At root, the activity that generates risks for consumers in California is best described as the *storage of sufficient credentials to transact*, not the transmittal or relaying of messages that result in digital currency transactions between users on these networks. We do not see how demanding enrollment from those "transmitting" adds any level of consumer protection beyond the enrollment of those who engage in "storing," and we are wary of large-scale unintended consequences and regulatory confusion that could result from overbroad or uncertain interpretation of this term. Therefore, "transmitting" should be stricken from the definition of "digital currency business."

"Issuing" digital currency

We do not believe that "issuing" should be among the activities that fit under digital currency business and thereby trigger an enrollment 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, hold and secure value on behalf of their customers.

The “storing” activity already requires that issuers presenting a custodial risk be enrolled. Ambiguity over what “issuing” otherwise means beyond storring could endanger academic research or hobbyist activities that may “create” or “issue” units of a cryptocurrency apart from any custodial services offered to users. Therefore, “issuing” should not be included as a trigger for enrollment.

“Exchanging” digital currency

As drafted, the definition of “exchanging” may cover innovation-critical activities that do not present a risk to California consumers. It currently reads:

> “Exchanging” digital currency means converting or exchanging Fiat Currency into Digital Currency, the conversion or exchange of digital currency into fiat currency, or converting or exchanging one form of digital currency into another form of digital currency;

Digital currencies can be “converted” into other digital currencies via two very different systems: (1) through a custodial exchange (*e.g.* Bitstamp, Bitfinex, Coinbase’s GDAX, etc.) or (2) via various automated protocols or techniques (*e.g.* sidechains, cross-chain atomic swaps). In the case of custodial exchanges, consumers place trust in a corporation: they must trust that the exchanger will take possession of the selling user’s digital currency and faithfully send it onward to the buyer or *vice versa*. Given this position of trust, mandating the enrollment of these exchangers is sensible.

A sidechain or a cross-chain atomic swap is not a corporation; it is a *function* that can exist on a digital currency network. Much as the ability to send a bitcoin directly from one user to another is one *function* that the network provides, a digital currency network with sidechains also allows one user to send bitcoins to another user that will be automatically converted by the network into another type of digital currency, say namecoins. This type of transaction and conversion is processed by miners who exert no ability to misdirect or take control over the underlying value of the transaction, just as they do with more typical same-chain transactions. It is automatic and peer-to-peer. Similarly, a cross-chain swap is a means to exchange assets on two different blockchains through a decentralized, peer-to-peer network. Accordingly the user of a sidechain or atomic swap is not putting trust in a custodian or corporation.

There are companies that may help develop the underlying network software that powers sidechains or atomic swaps, but these companies—so long as they do not take custody of the funds being exchanged—do not present a solvency risk to users of the network (anymore than do miners or normal protocol developers) and therefore they should not be subject to the enrollment scheme.

Given the potential confusion surrounding the definition of exchange, we believe it should not be an activity subject to enrollment. Many companies that offer to provide digital currency exchange do, indeed, present potential solvency risks to consumers, but this risk arises from their *storage* of customer digital currency before and/or after the exchange takes place, not the act of exchanging itself. Again, the activity that generates risks for consumers is the "storing" of valuable tokens, not the exchange activity. Accordingly, "exchange" should be stricken from the definition of "digital currency business."

That said, if the Legislature feels that it must, perhaps for anti-money laundering purposes rather than consumer protection purposes, enroll businesses that offer exchange services, then we ask that the language defining exchange be modified to exclude technologies like sidechains and cross-chain swaps as follows:

> "Exchanging," with reference to digital currency, means converting or exchanging fiat currency into digital currency, converting or exchanging digital currency into fiat currency, or converting or exchanging one form of digital currency into another form of digital currency. **Exchanging shall not be interpreted to include purely automatic conversion of digital currencies for other digital currencies by way of software or network protocol.**

I therefore respectfully request that you amend AB 1326 with the foregoing in mind or else oppose the bill. If we can ever help answer any questions about the technology or its implications for public policy and law, or if we can ever help connect you to members of the digital currency ecosystem, please do not hesitate to ask.

Sincerely,

Jerry Brito
Executive Director

cc: Members, Senate Banking and Financial Institutions Committee