COIN CENTER

June 10, 2015

The Honorable Matt Dababneh
State Capitol
P.O. Box 942849
Sacramento, CA 942490045

Dear Chairman Dababneh:

The California Assembly has made laudable progress refining AB 1326, legislation that will protect virtual currency consumers and promote innovation. ” We thank you and your staff for taking a conscientious approach to this lawmaking. As it stands, AB 1326 is far and away the most promising state effort in this field. Only one section of the legislation remains troubling to us, not because it is insensitive to extant bitcoin technologies but, because it may fail to countenance a future development in blockchain technology that would provide extremely useful services without generating consumer risks. We thank you for the opportunity to explain these new technologies, and offer our further recommendations.

This past May, Nasdaq announced a pilot program to trade stock shares on a blockchain. Nasdaq is proposing to use marked bitcoins[1] on the Bitcoin blockchain in order to trade these shares. Accordingly, this innovative yet non-monetary use of virtual currency technology could technically be required to be licensed under the letter of AB 1326, as presently drafted. We do not believe California intends to regulate non-monetary uses of virtual currencies, uses typified by Nasdaq’s proposal. Nonetheless we understand the importance of not creating loopholes within the language of AB 1326 that would leave consumers of virtual currency monetary services unprotected. Accordingly we would like to suggest a further refinement of the bill’s definition of virtual currency business.

First, however, we’d like to quickly explain the Nasdaq program in order to illustrate how it could create a licensing obligation under the current language. We don’t have all of the details about what exactly Nasdaq has in the works, but a critical passage in the program’s announcement reveals the basic mechanism:

> Nasdaq will initially leverage the Open Assets Protocol, a colored coin innovation built upon the blockchain.[2]

“Colored coin” means that the bitcoins sent in a particular bitcoin transaction will be representing something beyond the bitcoin value itself. It’s as if one painted a dime red and passed it around the office saying, “whoever has the dime is allowed to speak at the meeting.” This can be done with a bitcoin by attaching a short message to a bitcoin

[1] *See* Brock Cusick, “What are Colored Coins” *Coin Center* (Nov. 2014) https://coincenter.org/2014/11/colored-coins/.

[2] *See* Nasdaq Press Release, “Nasdaq Launches Enterprise-Wide Blockchain Technology Initiative” *Nasdaq OMX* (May 2015) http://www.nasdaqomx.com/newsroom/pressreleases/pressrelease?messageId=1361706.

transaction when asking that the transaction be written to the blockchain. The message effectively marks (or “colors”) the specific coins in the transaction as something more than just bitcoins.

The implication of this arrangement is that Nasdaq’s platform will trade shares of stock by trading bitcoins. This is not a use of blockchain ledger technology standing alone; this is the Bitcoin network and blockchain being used by Wall Street. It is, in fact, technically impossible to use Bitcoin’s blockchain without transacting in bitcoins.

When a company such as Nasdaq decides to “color” a coin so that it can be traded representing stock shares on the blockchain, it necessarily “converts” or “exchanges” that coin from a normal bitcoin into an item of “other value”—stock certificate—or, in some respects an alternative form of “virtual currency”—a colored bitcoin, or a “Nasdaq coin” on the Bitcoin network. Such activity would require license under 26000(c)(2) either because Nasdaq is:

> **providing conversion or exchange services of . . . the conversion or exchange of virtual currency into . . . other value, or the conversion or exchange of one form of virtual currency into another form of virtual currency.**

Assuming that California does not wish to demand a license from companies that create colored-coin implementations, we suggest that all of 26000(c)(2) be removed from the draft.

We recognize that 26000(c)(2) was included to protect the customers of virtual currency exchanges that fail to maintain solvency and security—e.g. Mt. Gox. We agree that such protections are important. But, as we read the preceding section in the definition—26000(c)(1)—a company like Mt. Gox, and indeed any other exchange company that poses a consumer risk, would be required to be licensed because they necessarily will have full custody of consumer virtual currency balances in order to provide their exchange service. By holding a customer’s bitcoins in order to offer something in an exchange, or vice versa, the company will necessarily have full custody. Additionally, any company that exchanges fiat currency for virtual currency will already need to obtain a money transmission license from the state because it will be holding fiat currency on behalf of a consumer.

Given that 26000(c)(1) will already require licensing from any company that has custody or control of customer funds (regardless of whether the purpose of that custody is to make an exchange or merely to provide a hosted wallet service), we do not believe that removing 26000(c)(2) will create any additional consumer risk. Instead, removing 26000(c)(2) will shield companies, like Nasdaq, from licensure requirements when they convert virtual currency into colored coins for the purposes of stock trading or other such non-monetary use.

We previously advocated for an exemption of such colored coin services by suggesting a non-financial uses exemption that mirrors language adopted by New York’s Department of Financial services. We no longer believe such an exemption to be the appropriate approach. Determination of what is and is not “financial” could prove difficult to operationalize, and could fail to shield financial uses involving colored coin record-keeping activities dealing in securities or other financial records.

Additionally, we are concerned that 26000(c)(2) would unintentionally mandate licensure from innovative companies testing very new technology that could link alternative blockchains together (i.e. allow users to move their bitcoins off of the bitcoin ledger and onto another ledger that is also open-source and decentralized but built on different software, running on a different open community of networked computers). The most development in this field is a technology called sidechains.[3] We'd briefly like to offer an example explaining sidechains.

Say, for example, Nasdaq wanted to utilize an alternative blockchain (public ledger) that is better suited to trading securities than the Bitcoin blockchain because the alternative blockchain's protocol allows for faster trades or smaller divisions of each token (perhaps to allow for stock splits). Nasdaq could issue these securities as "Nasdaq Tokens" on this alternative blockchain-based ledger, "Nasdaq-chain." For these tokens to be reliable markers of a share of some stock, they must be unique and non-duplicatable. However, if this Nasdaq blockchain is young and lacks widespread adoption of the software by an open network of participants, it may be easier for a malicious user to create fraudulent copies of these tokens as compared with the difficulty—it is effectively impossible— of creating such counterfeits on the Bitcoin network. The question presents itself: how can Nasdaq utilize some new blockchain that better suits its needs but still have the security against counterfeiting that comes from the scale and power behind the longer-established bitcoin network. The answer may be sidechains.

Using a sidechain, Nasdaq can allow interested investors to provably "park" their bitcoins in a bitcoin network-controlled lock-box; this action would simultaneously make a corresponding number of Nasdaq-tokens available on the Nasdaq-chain. This conversion can occur without any single individual or business holding custody of the user's funds, and, therefore, without any risk to the consumer that their money will go missing. The exchange is not made by people, it is made using the same deterministic math that underlies the bitcoin network.

The technology behind sidechains is very young but, nonetheless, extremely promising, because it is purpose-built to limit the risk to users seeking access to a blockchain record-keeping service outside of the bitcoin network. We believe that the language of 26000(c)(2) could impose undue costs on the developers of these nascent and promising innovations. We also believe that should any consumer risk emerge from these technologies, it will be foreseeable and in the reasonably distant future, affording the assembly time to react and develop new protective measures beyond AB 1326. Again, we respectfully ask that 26000(c)(2) be removed from the definition of virtual currency business.

Thank you for your time, and please do not hesitate to contact us for further clarification on these points or other questions.

Sincerely,

[3] *See* Adam Back, Matt Corallo, et. al., "Enabling Blockchain Innovations with Pegged Sidechains" (Oct. 2014) https://www.blockstream.com/sidechains.pdf.

Peter Van

Peter Van Valkenburgh
Director of Research