AMERICAN BANKER

Don't Let Bitcoin Morph into Govcoin

By: Jon Matonis, *Executive Director of the Bitcoin Foundation* – July 30, 2013

Almost since Bitcoin arrived on the financial scene in 2009, traders and exchange operators began contemplating the prospects for a self-regulatory organization that would be organized by bitcoin participants for the purposes of outlining and recommending best practices.

Now, more than four years on, an SRO in the spirit of the National Futures Association and National Association of Realtors could be emerging for the disruptive Bitcoin cryptocurrency and other digital assets. The Committee for the Establishment of the Digital Asset Transfer Authority is set to announce its launch Tuesday in conjunction with several leading industry participants and the well-connected Promontory Group as an advisor.

As a longtime cryptocurrency advocate and the recently appointed executive director of the Bitcoin Foundation, I welcome the emergence of SROs. (Unlike the foundation, the D.A.T.A. will cover a broad range of virtual currencies, including Ven and Ripple). A non-governmental body formed to promote good industry behavior has a distinctly free market heritage. Groups born out of mutually-beneficial community trade can also define a set of common principles that they want to abide by referred to as *lex mercatoria*. This is Latin for "merchant law," the body of commercial law used by merchants throughout Europe during the medieval period emphasizing contractual freedom andalienability of property. Merchants relied on this legal system they developed and administered while shunning legal technicalities and deciding cases *ex aequo et bono* – "from equity and conscience."

Although SROs can be extremely beneficial in advancing an industry, clear political lines must be drawn to mitigate the risk that an SRO would be co-opted by government and this is where it gets tricky. To avoid more direct and onerous regulations, the government may ask the SRO for certain guidelines or rules to be incorporated among its membership. If such modifications are objectionable to the majority of industry participants, the SRO faces the dilemma of challenging the authorities and risking its relevance or being complicit in harmful and over-reaching backdoor legislation.

The path of complicity ultimately leads to an SRO that has strayed from its core constituency and could be absorbed by the government as a direct regulatory body. The SRO should periodically conduct a reality check by remembering Voltaire's words: "To learn who rules over you, simply find out who you are not allowed to criticize."

From a purist perspective, challenging the authorities on points of principle may not necessarily result in irrelevance but it would shift the group's mandate to one of advocacy and most likely even criminal defense. This does not have to be viewed as a negative outcome, but it does have to be anticipated.

As self-regulatory organizations are excellent non-governmental solutions for industry best practices, they need to be vigilant about maintaining the integrity of the original mission. In the

case of bitcoin as a negotiable digital asset class, the protection of core fundamental attributes includes perfect fungibility, payment irreversibility, and user-defined privacy. Also considered sacrosanct for the Satoshi Nakamoto Bitcoin protocol would be the 21 million limitation on coin supply and the roughly 10-minute interval for new "blocks" of transactions added to the public ledger known as the block chain. That interval is a function of the self-adjusting difficulty for bitcoin mining. (The more distributed computing power dedicated to securing and verifying transactions on the network, the harder it becomes for any miner to solve a mathematical problem in order to "find" the next block for the public ledger and earn newly-created bitcoins.)

Anything different simply wouldn't be Bitcoin – it would be an alt-coin. A toaster does one thing and it does it amazingly well. It makes toast. If you modify it and ask it to do something else, then it's no longer a toaster.

Recently, *Govcoin* has become a metaphor for alterations to the core bitcoin protocol that reduce its fungibility, irreversibility or privacy to conform to certain government specifications for an "appropriate" digital currency.

In the Juan Llanos' article with the sensationalist title, "The Hidden Rule that Could Kill Bitcoin's Irrevocability," the author makes the point that bitcoin's privacy and irreversibility could be under attack via ignorant legislation that cannot comprehend what it is attempting to regulate. Llanos states, "It is no surprise that regulation and compliance often set the boundaries of product design. In the case of crypto-currencies, however, don't these rules cut through the fundamental features of digital [peer-to-peer] payments that make them so disruptive?"

The Consumer Financial Protection Bureau has not yet confirmed to what extent the implementation of Regulation E by money transmitters will be applicable to licensed virtual currency providers. Also known as the Remittance Transfer Rule, this amendment to Regulation E mostly overlaps with measures in place at the state level and compliance will be required by Oct. 28. It requires, among other items, prepayment disclosure, transaction receipts, and transaction cancellation within prescribed time limits.

Although it is technically possible to delay a bitcoin transaction, a full reversal of a transaction would require unacceptable developer complicity at the core protocol level and probably the introduction of an intermediary of some sort. This would undermine Nakamoto's vision of a financial system that did not require trusted third parties.

Examples of what would be considered acceptable variables to modify within the core Bitcoin protocol are the block size limit and the proof-of-work algorithm. A block size change would be anticipating transaction throughput and increases in storage and network bandwidth. Changes to the SHA-256 algorithm for proof-of-work would be considered technically feasible and prudent given certain advances in cryptography. However, each of these modifications would require majority consensus of the bitcoin miners to prevent a critical "fork" of the bitcoin block chain.

Think about physical paper cash which everyone has the right to use today. The supreme features of physical paper cash, other than security and divisibility, are fungibility, irreversibility, and privacy.

Digital cryptocurrency assets such as bitcoin do not add anything new to that primary feature set. An SRO in the digital asset industry should not remove any.

Fungibility refers to a commodity possessing the trait of mutual substitution among its individual units. A crumpled $20 bill found between the sofa cushions is as good as a crisp one handed out by a bank teller. In the context of digital currency, this means the blocking or banning of "tainted coins" is not permitted. Just because someone once used a bitcoin to buy drugs, it shouldn't prevent a subsequent owner to use it to buy socks or baklava or MP3s.

Irreversibility means that payments in the unit are final and irrevocable – no chargebacks. User-defined *privacy* refers to a sliding scale, based on individual preference, as to how many details of a particular transaction are associated with the user.

"Privacy on the network begets transparency," writes my colleague Patrick Murck, general counsel at the Bitcoin Foundation, in an article on the Cato Institute's *Cato Unbound* blog. "You can't expect participants to allow full financial transparency at the institutional level if the participants can't choose to guarantee the privacy of their individual transactions."

Rather than a failed patchwork of individual state money transmitter rules, Murck says, "the preferred outcome would be home-rule and reciprocity amongst the states allowing states to compete for industry by creating efficiency and clarity in the regulatory process." Furthermore, multi-state regulation has failed because each state is not required to respect the judgment of another where a company is domiciled.

Over-regulation tends to drive innovation to more lightly-regulated jurisdictions or underground where it thrives. And, this is even truer with the cryptographic bitcoin. Although not government's intention, a throttled and neutered bitcoin in the "official" economy would ultimately enhance its overall effectiveness via increased anonymizing measures and more robust decentralization.