Jim Harper
Senior Fellow

Attn: Emerging Payments Task Force
Conference of State Bank Supervisors
1129 20th Street NW, 9th Floor
Washington, D.C. 20036

Re: Draft Model Regulatory Framework for Digital Currency Regulatory Regimes

Dear Members of the Task Force:

Thank you for the opportunity to comment on the draft model regulatory framework for state digital currency regulatory regimes. The more methodical approach that you are taking at the Conference of State Bank Supervisors represents an improvement over other, notable U.S.-state-level regulatory proposals.

Regulation in the field of digital currencies must meet high standards. Digital currencies such as Bitcoin have passionate advocates because of the potential benefits Bitcoin holds out not only to American consumers, but to billions of people around the world who are financially marooned and needlessly kept in poverty simply because their countries lack financial integration.

If undue regulation were to hinder the growth of Bitcoin, that would be very costly in terms of jobs and economic growth, which in parts of the United States and many places worldwide means access to food, medicine, housing, and adequate educational opportunities for children. Bitcoin is not only a substantial potential engine for global financial inclusion, but also an opportunity to increase liberty and dignity for many populations, to provide law-abiding people with greater financial privacy, and to offer a more stable money supply in countries with poorly managed currency.

Fundamentally, any regulatory proposal should pass a cost-benefit analysis. The public should be able to ascertain how and how well the regulation serves public interest goals and makes society better off. The CSBS policy statement and draft model regulatory framework present an opportunity to explore what policies and what regulations will help secure Bitcoin's benefits for the public, producing net benefits for consumers in the United States and worldwide.

The CSBS draft, like New York's "BitLicense" proposal, does not come accompanied by analysis that justifies the proposals within it, however. When the New York Department of Financial Services introduced its proposal, it cited "[e]xtensive research and analysis" that it said "made clear the need for a new and comprehensive set of regulations that address the novel aspects and risks of virtual currency." Though New York's financial regulator promised to produce that analysis in response to a request under New York's Freedom of Information Law, the NYDFS has yet to do so despite the passage of more than six months. As of this writing, the NYDFS has published (though not formally issued) a second draft of the "BitLicense," but it still has not released the analysis it promised the public. Here's hoping the CSBS, engaging in this more methodical process, can do better and engage more articulately with the Bitcoin community so that a regulatory framework suitable for the digital currency era can emerge.

Bitcoin is a software protocol, so its community of programmers, businesspeople, and users should not be presumed familiar and conversant with laws, regulations, and practices in the financial services world (just as CSBS should not be presumed deeply versed in the details of the Bitcoin software or anticipated innovative uses of it). The vast difference in cultures requires greater articulation from regulators about the public interest goals being sought, how existing regulations achieve those goals, and how increments to those regulations or new regulations would do so. Such an articulation from CSBS will position the Bitcoin community to help fit means to ends.

I recommend to your attention the Bitcoin study released by the European Banking Authority in July, 2014.[1] The EBA submitted itself to the rigor of risk management, seeking to identify the risks that digital currency poses to consumers, merchants, and a small variety of other interests. This forms the groundwork for a discussion of what steps will prevent or mitigate harms and interdict bad actors.

While the report did not apply risk management as well as it could have, and it came to unduly conservative results in terms of integrating Bitcoin into the European financial services system, the small number of genuine risks it identified can form the basis of discussion about solutions. It is very hard to assess a batch of solutions put forward without an articulation of the problems they are intended to solve, as the draft model regulatory framework unfortunately does.

Many of the proposals in the draft regulatory framework appear to match or parallel existing financial services regulation. Before their extension to Bitcoin and other digital currencies, the public should know what problems they solve and how well. Many may be longstanding practices, but custom alone is not a sound basis for regulation or for extending regulation to a new area. Nobody should want financial services regulations to remain in place or extend to digital currency simply because it has been done that way in the past. But existing practices that do provide genuine consumer protection greater in value than its costs should be welcomed.

The Bitcoin community and the regulatory community can come together over universal interests like consumer protection, security, privacy, and law enforcement if there is a two-way conversation. This opening comment round begins the process. Hopefully, its continuation will get questions answered on

[1] European Banking Authority, "EBA Opinion on 'virtual currencies'" (July 4, 2014) https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf.

both sides, so that the process can reach the appropriate conclusions. Though the basis to comment articulately on each of the many items found in the draft model regulatory framework does not yet exist, please accept the following observations on the policy statement and the framework.

Scope: Digital, Not "Virtual"

Understandably, given the variability of language in this emerging field, the policy statement is unclear as to scope. Tighter adherence to natural meanings of the words "virtual" and "digital" would strengthen the statement.

The policy statement calls Bitcoin a "digital" currency, which is correct because this distinguishes it from analog currencies, which are most recognized as their tangible form-factors, such as rectangular pieces of paper or cylinders of metal. But the statement treats digital currencies as a subset of "virtual currencies," suggesting that it is in the same class as currencies used in games or closed commercial environments.

Though "virtual" has recently come to mean "on a computer or the Internet," its longstanding meaning is: "very close to being something without actually being it" or: "being such in essence or effect though not formally recognized or admitted."[2] Classing Bitcoin as a "virtual" currency suggests that it is not real, even while the Bitcoin network processes tens of thousands of transactions worldwide each day. While people continue to call Bitcoin a "virtual currency," they will tend to think that the system based on pieces of paper and metal is "real" while the fully digital system is not.

The better approach is to treat digital currencies as the superset and virtual currencies as a subset. In their isolated game or business ecosystems, virtual currencies may serve well, but they do not cross over into mainstream commerce and financial services (i.e., they are non-convertible). Because of this, the risks to consumers are far lower than they are in the digital and fiat currency areas. Surely the CSBS does not propose that makers of a videogame that stores chits for trading among players should be licensed and undergo background checks at the behest of their state regulators. This may be appropriate for digital currencies because they have in increasing role in real commerce.

Bitcoin is a digital currency, interesting to the CSBS and the regulators it represents because of its real potential effects, good and bad, on Americans and America's financial services marketplace. Virtual currencies—that is, non-convertible digital currencies—should be outside your scope.

"Market Stability"?

While consumer protection and law enforcement are recognized areas of regulatory interest, the "marketplace stability" role for regulators laid out in the policy statement is not so clear. In a welcome way, the policy statement cites the potential for Bitcoin to improve financial services for the benefit of consumers. If it is meant to defer to innovators' efforts to find ways to serve consumers better, that, too, is welcome.

[2] Merriam-Webster.com definition of "virtual," http://www.merriam-webster.com/dictionary/virtual.

But the claim to responsibility for the "overall health and strength of financial markets" is a little grand. Indeed, guarding "stability" is in tension with "health" and "strength" in markets. The most desirable marketplace (read "healthy" and "strong") has stability in the sense that existing providers deliver products and services reliably while competition drives their prices down and service quality up. But the best marketplace also sees new entrants bringing innovative products using new technologies. This has a *destabilizing* effect on the marketplace because existing providers may lose market share or go out of business.

"Stability" sounds nice, of course, but it should not be put ahead of competition and innovation that produce better services for consumers. The "market stability" role cited in the policy statement may be a surplus idea that if acted upon could actually stand in the way of optimally functioning markets and consumer welfare. If there are other meanings of "market stability" that are more validly a regulatory role, perhaps the policy statement could be amended to reflect them.

Transparency to Law Enforcement

Another note of caution is worth airing regarding the relationship of financial regulation to law enforcement (taken to mean "crime control" interests and not economic regulation). It is not an appropriate role for regulators to see that the provision of financial services is "transparent to law enforcement," as the policy statement says.

The U.S. Constitution's Fourth Amendment, which applies equally to state governments, places a specific disability on law enforcement access to Americans' papers and effects. Information about the financial activities of U.S. companies and U.S. consumers are rightly subject to this constitutional protection. Financial services regulators tasked with consumer protection may be bystanders to these issues, or they may seek balance, but taking the side of law enforcement against the privacy interests of consumers is not appropriate.

Fourth Amendment case law suggesting that Americans do not have a constitutional interest in financial information shared with third parties is controversial at best. The leading Supreme Court case with respect to financial services providers' rights, *California Bankers v. Schultz* (1974), was decided almost entirely on Due Process grounds, with the Court giving Fourth Amendment concerns minimal consideration. Its companion in undercutting Americans' privacy rights, *U.S. v. Miller* (1976), was poorly reasoned and based on misapplication of the "reasonable expectation of privacy" test, which is increasingly falling out of favor with the Court. In her essential concurring opinion in the recent *Jones* case (2012) dealing with GPS tracking, Justice Sonia Sotomayor specifically signaled her desire to reconsider the third-party doctrine, which undercuts Americans' financial privacy.

> This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers. … I would not assume that

> all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.

Justice Sotomayor would likely strike down regulation that makes Americans' private financial transactions "transparent to law enforcement."

If America's regulators intend to protect America's consumers, the vast majority of whom are law-abiding, they should recognize that their role is not alliance with criminal law enforcers or simple obedience to their demands. Information about consumers' use of financial services should be available to law enforcement if they meet appropriate legal standards, such as probable cause evidenced by a warrant.

Activities-Based, Not Technology-Specific Regulation

The policy statement's "activities-based regulation" and "policy implementation" sections lean in the right direction: toward integrating any regulation of digital currencies like Bitcoin into existing regulatory regimes. But the policy statement should be clearer: It does not make sense to have the same financial services, posing the same risks, regulated differently because they serve consumers using a different financial technology. Regulation should indeed be "activities-based" rather than technology-specific, and the CSBS should help guide its membership in that direction.

This section is so short because it appears you're going to get it right. Carry on.

Licensing Requirements

The framework presumes licensing's benefits and thus its appropriateness. The issues deserve more granular analysis. Licensing can serve a number of good purposes, and it carries a number of costs. State-by-state licensing may be an ill fit already for today's national and international commercial environment and particularly weak for the Internet-based digital currency environment.

To the good, licensing creates a barrier to entry that prevents incompetent but law-abiding businesspeople from getting started. Barriers to entry are often regarded as bad, but keeping incompetents from starting Bitcoin businesses would be good.

Also to the good, a low-quality company forced to go through the licensing process will probably have its administrative systems in better order than a company that does not. Licensing may reveal criminal background among participants that disqualifies them, legally or in the eyes of consumers, from providing service. As a tool of prospective enforcement, licensing may give aggrieved parties and government officials easier access to responsible people in the licensed company.

Licensing's role as a barrier to entry is also a public interest liability. By driving up costs, it may exclude worthy competitors from the marketplace and deny consumers the benefits they would offer. This is particularly true in the U.S. financial services marketplace, where separate licensing requirements exist in nearly every jurisdiction of what is a single national market. The public interest benefits of licensing

obviously do not increase arithmetically with each additional license. The highly duplicative U.S. licensing regime is far too costly given the trivial benefits of multiple licensing. The current licensing regime is almost certainly restricting competition in financial services and denying U.S. consumers the benefits of such competition.

Licensing will also decline in consumer protection utility as the digital currency arena expands globally. Licensing is premised on business activity in physical legal jurisdictions, which the Internet essentially does not recognize. In the future, there may well be excellent service providers that do not operate in the United States or that operate in no known jurisdiction. Because they are out of reach of state regulators, the licensing regime will not offer consumers any benefit. Licensing is a means to achieving consumer benefits, not an end in itself. In any given jurisdiction, it will be a weaker proxy for sound business practice with the advance of a global financial services marketplace.

There a few approaches that regulators may consider to address the Internet dynamics of digital currency. The approaches vary in advisability.

The instinct for control may drive regulators toward a heavy-handed approach, in which non-jurisdictional financial services providers are pursued as criminals and their customers as aiders and abettors. There would be some irony in consumer protection agencies seeking punishment for businesses and competent consumers who are trying to get together on the most mutually favorable terms.

A more subtle approach to the Internet dynamics of digital money is to make the licensing process significantly easier, so that legitimate digital currency businesses, which are naturally inclined toward lawfulness, have less reason not to engage with licensing authorities. The CSBS is well positioned to organize an effort by state regulators to streamline their licensing programs, including by forming agreements among licensing jurisdictions to accept each others' licenses. Sharing licensing and enforcement data in real time, as suggested in the document, makes sense in a state-based national licensing regime. Such a regime would make financial services licensing like driver licensing. If you can operate in one state, you should be able to operate in them all.

There are alternatives to requiring licensing from the moment a firm enters into business, too. New firms with a small clientele, such as many digital currency firms today, present a low risk to consumers, to financial services marketplaces, and to the economy even if they are individually less stable than our nation's monster financial services firms. Sensible rules could require that small firms acquire a license once they reach a certain size in terms of customers, value transacted, or other measures. Small, pre-license firms could be required to collect assurances from their customers that they are willing to bear the risk of dealing with an unlicensed firm, or that customers are putting some sufficiently small percentage of their assets with any such firm. There are plenty of ways to conduct a licensing regime that contribute to public protection while minimizing the costs of licensing to competition, innovation, and ultimately consumers.

As noted above, the many other proposals found in the draft model regulatory framework need greater articulation if there is to be a full examination of their appropriate application to digital currencies like Bitcoin. The world of financial services regulation has grown up over many decades, its benefits are non-obvious to newcomers, and it may have vestiges that are not appropriate for our digital currency future. Digital currencies like Bitcoin have popped up very quickly, their functioning is opaque to most people, including regulators, and the innovative ways they will be used are uncertain. For all these reasons, it is worth taking a harder look at all the issues.

Thank you again for taking comments on your work so far. I know the Conference of State Bank Supervisors' staff to be conscientious, hard-working, and keenly interested in the nascent digital currency arena. I would be happy to work with you and them to produce risk-based analyses of what regulations may produce the best of all possible worlds: a burgeoning Bitcoin ecosystem that is safe for consumers, widely adopted, and delivering on its promises of global financial inclusion, liberty and dignity, privacy for the law-abiding, and stable money supplies.

Sincerely,

Jim Harper
Senior Fellow
The Cato Institute