

TESTIMONY OF MARCO SANTORI**CHAIRMAN, REGULATORY AFFAIRS COMMITTEE, THE BITCOIN FOUNDATION****TO THE NEW YORK DEPARTMENT OF FINANCIAL SERVICES****HEARING ON VIRTUAL CURRENCIES****JANUARY 28, 2014****EXECUTIVE SUMMARY**

Bitcoin is a revolutionary computer protocol originally intended as a decentralized payment system. Its operation relies on a distributed public ledger. Complex cryptographic systems allow many different kinds of transactions to be recorded in the ledger. As such, there are many potential uses of the Bitcoin protocol beyond payments.

Questions around the regulation of Bitcoin's use are many, and answers are relatively few. Among the threshold questions around the "BitLicense" idea is whether it is technology-specific regulation. New York residents have many reasons to value technology-neutral regulation over technology-specific regulation, including the role of neutrality in the blossoming of e-commerce and information technology.

It is difficult to tell at this early stage whether a "BitLicense" would be suitably tailored to achieve its regulatory goals with respect to the many emerging digital currency business models. The landscape of digital currency businesses today is very different from what existed last year, and game-changing developments may soon come. We should work to ensure that regulations do not prevent emerging business models from providing consumers valuable new products.

At this early stage, it is difficult to determine the problems the "BitLicense" idea is meant to solve, or how well it would solve them. Consumer protection, crime prevention and investor protection are important goals, which are already sought by existing regulation. A "BitLicense" could be worthwhile if it truly aids digital currency businesses in achieving these goals, but the fit between means and ends is unclear at this point in the development of the "BitLicense" idea.

If a "BitLicense" is warranted, it is worth exploring how it should be administered. State and local administration has benefits in some respects, and federal regulation is superior in others. Bitcoin businesses would probably prefer that any regulatory framework be developed cooperatively among levels of government and among states, through groups such as the Conference of State Bank Supervisors, rather than on an ad-hoc, state-by-state basis.

INTRODUCTION

I am pleased to submit this testimony on behalf of the Bitcoin Foundation at the request of the New York Department of Financial Services. The Bitcoin Foundation is a member-driven, non-profit organization dedicated to serving the business, technology, government relations, and public affairs needs of the Bitcoin community. The Foundation works to standardize and strengthen the Bitcoin protocol and software, to protect the Bitcoin community, and to broaden

the use of Bitcoin through public education and by fostering a safe and sane legal and regulatory environment. Incorporated in July of 2012, the foundation is organized under section 501(c)(6) of the Internal Revenue Code.

The Bitcoin Foundation's members include many of the top companies, entrepreneurs, and technologists working to make Bitcoin a success. The Foundation draws a portion of its membership from the state of New York, but represents an international membership with well over a thousand corporate and individual members. Our focus is global. The rapid development of Bitcoin is a global phenomenon and the Bitcoin 2014 conference, successor to our hugely successful Bitcoin 2013 conference in San Jose, California, last year, will be held in Holland May 15-17, 2014. The Bitcoin Foundation is actively developing systems to empower local Bitcoin Foundation subsidiaries and chapters in countries around the world with the resources they need to further the foundation's mission of promoting, protecting, and standardizing the Bitcoin protocol and distributed, decentralized digital currency in general.

I am the chairman of the Bitcoin Foundation's Regulatory Affairs Committee. This committee consists of legal and compliance professionals dedicated to addressing the state, federal, and international regulatory challenges faced by participants in the Bitcoin ecosystem. Additionally, I am an attorney practicing in New York City. My practice consists of representing high technology and digital currency companies, including exchanges, institutional miners, wallet services, payment processors, and other financial technology providers. I received my Juris Doctor from the University of Notre Dame Law School and my undergraduate degree from the University of California at Berkeley.

ABOUT BITCOIN

Bitcoin was invented in 2008 as a peer-to-peer payment system for use in online transactions.¹ Bitcoin is revolutionary in that, unlike any prior online payment system, Bitcoin is not administered by any central authority. There is no middleman between the sender/buyer and the receiver/seller as there is with, for example, PayPal, traditional payment cards, bank wires, or other payment systems. Bitcoin is thus referred to as a "decentralized" digital currency.

The Bitcoin software is also open-source and non-proprietary, developed by a community of volunteers in collaboration with our chief scientist, Gavin Andresen. There is no "Bitcoin company" that manages or controls the software or its operation. If the Bitcoin Foundation ceased work on Bitcoin's technical development, the technical development work would continue among the volunteers worldwide who already do much of the heavy lifting. If the Bitcoin Foundation or any other actor tried to take control of the Bitcoin software, the Bitcoin community would reject that attempt and develop the software on its own, independently.

Instead of a central authority, the Bitcoin transaction network consists of computers around the world running the Bitcoin software, which operates the protocol for administering Bitcoin transactions. That software can be downloaded and run by anyone, and any computer running the

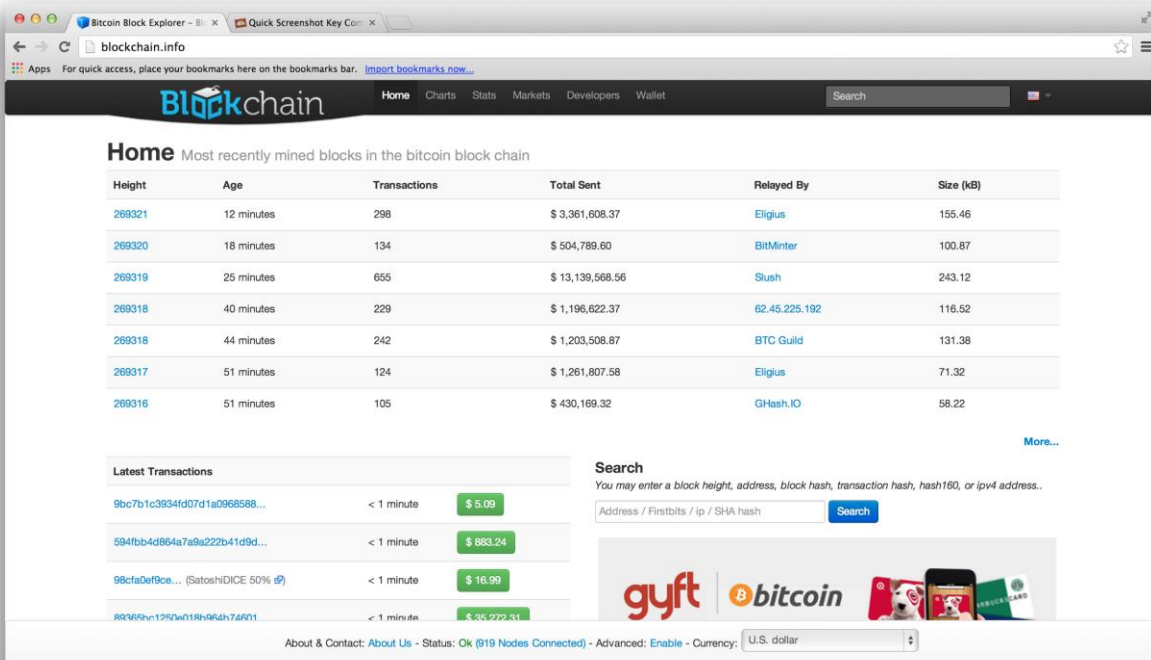
¹ Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," <http://bitcoin.org/bitcoin.pdf>.

software can join the network. Each computer on the network also maintains a copy of the universal public ledger known as the “block chain.”

THE BLOCK CHAIN

The public ledger is crucial to understand. The heart of the Bitcoin technology is this public ledger that records all transactions occurring in the system. The ledger is broken into blocks of transactions, and each new block of transactions is linked to the previous block, forming what is called the “block chain.” The newest block at the end of the chain links back to every block that precedes it. Having access to the most recent block allows one to follow the chain backward to observe every Bitcoin transaction ever made.

New blocks are created by “mining.” Mining is done by solving a very difficult math problem, which creates the next block incorporating recent transactions. Though the problem is difficult to solve, the solution is easy to verify, so a miner discovering the solution can declare it, and nodes across the network will promptly confirm the new block.




Home Most recently mined blocks in the bitcoin block chain

Height	Age	Transactions	Total Sent	Relayed By	Size (kB)
269321	12 minutes	298	\$ 3,361,608.37	Eligius	155.46
269320	18 minutes	134	\$ 504,789.60	BitMinter	100.87
269319	25 minutes	655	\$ 13,139,568.56	Slush	243.12
269318	40 minutes	229	\$ 1,196,622.37	62.45.225.192	116.52
269318	44 minutes	242	\$ 1,203,508.87	BTC Guild	131.38
269317	51 minutes	124	\$ 1,261,807.58	Eligius	71.32
269316	51 minutes	105	\$ 430,169.32	GHash.IO	58.22



[More...](#)

Latest Transactions

9bc7b1c3934d07d1a096858...	< 1 minute	\$ 5.09
594fbb4d864a7a9a22b41d9d...	< 1 minute	\$ 883.24
98cfa0ef9ce... (SatoshiDICE 50% )	< 1 minute	\$ 16.99
883664e1250a018a964d76f01...	< 1 minute	\$ 35,272.31

Search
You may enter a block height, address, block hash, transaction hash, hash160, or ipv4 address.

Address / Firstbits / ip / SHA hash

gyft | **bitcoin**  

About & Contact: [About Us](#) - Status: OK (819 Nodes Connected) - Advanced: [Enable](#) - Currency: U.S. dollar

Source: blockchain.info

The difficulty of the math problem increases with the amount of effort going into mining across the network. This controls the pace at which new bitcoins are added to the system, and it reduces the chance that any one miner or group will take control of the block chain. The amount of Bitcoin created by mining will drop over time until it ceases altogether in 2140 at just fewer than 21 million bitcoins in existence. In the meantime, mining will increasingly be rewarded by transaction fees.

Critically, the universal ledger prevents anyone from double-spending the bitcoins they own. Because a record of every transaction is available to all, attempts to spend the same bitcoin after it has already been transferred are easily detected using the block chain. This permits purely digital transactions without any central administrator, who would otherwise manage the ledger and police against double spending of a digital currency.

HOW A BITCOIN TRANSACTION WORKS

Any Bitcoin user can transact directly with any other Bitcoin user. To utilize the Bitcoin network, a user needs a Bitcoin address, or “wallet.” A Bitcoin wallet takes the form of a cryptographic “public key,” which is a string of numbers and letters roughly 33 digits long. Each public key has a matching “private key,” known only to the user. Control of the private keys is what assures one of control of the bitcoins at any Bitcoin address, so collections of private keys must be protected by passwords or other means of securing them. Wallets can be created and maintained on user’s own computers using the Bitcoin open-source software. In practice, however, many users have accounts with one or more Bitcoin service providers, and they store bitcoins at addresses provided through their accounts, known as “hosted wallets.”

To initiate a transaction, the software or service sends a message to the other computers on the network announcing the transfer of a certain value in bitcoins from the user’s public key to the recipient’s public key. The sending user’s private key is used to “sign” the transaction. The private key is mathematically paired with the public key, and through a standard cryptographic process of the sort used to secure website connections, every computer on the network can verify that the transaction is signed with the correct private key. The private key signature thus serves to confirm that the transaction originated with, and was approved by, the actual owner of the originating public key, and therefore that the transaction is valid. While this process sounds complicated, it is handled automatically and invisibly for users by the Bitcoin software. From the user’s perspective, sending bitcoins to someone else is no more difficult than sending an email.

Administering a payment or money system is not the only use of a universal public ledger. The Bitcoin protocol is expanding to facilitate many advanced services such as deposits, escrows, general contracts and even distributed stock trading. Indeed, the Bitcoin protocol is now finding many uses beyond payments and money, including proving the existence of documents, verifying human identities, Internet naming and numbering, and many more.

At bottom, Bitcoin is a computer protocol. It is like TCP/IP, which enables all the different uses people around the globe invented for the Internet. It is like HTML, which enables all the different uses people invented for the World Wide Web. We envision Bitcoin as a driver of global change that rivals these other protocols in terms of the benefits it delivers to humankind across the globe. How Bitcoin businesses interact with existing regulatory regimes is comparatively straightforward when they replicate an existing financial service, but more complicated when they break down old categories to enable new services.

REGULATION AND “BITLICENSING”: ABUNDANT QUESTIONS, SCARCE ANSWERS

The Department of Financial Services' Notice of Intent,² published on November 14, 2013, posed several questions to the public, including:

- What specific types of virtual currency transactions and activities should require a “BitLicense”?
- Should entities that are issued a “BitLicense” be required to follow specifically tailored anti-money laundering guidelines?
- Should entities that are issued a “BitLicense” be required to follow specifically tailored consumer protection guidelines?
- Should entities that are issued a “BitLicense” be required to follow specifically tailored regulatory examination requirements?

We believe that digital currency companies providing regulated services are subject to all the regulations their conventional counterparts are. The Department's intent to take a “hard look” at digital currency issues through the lens of “BitLicensing” may require that more fundamental issues be addressed first, though, including:

- Is a “BitLicense” technology-specific regulation?
- Could a “BitLicense” be suitably tailored for emerging business models?
- What problems is a “BitLicense” meant to solve and would a “BitLicense” solve these problems?
- If a “BitLicense” is warranted, how should it be administered?

These threshold questions precede still others, especially about the current regulatory burdens on digital currency businesses. Digital financial services firms in the United States now face an uneven and dizzying pattern of state licensing requirements that could cost them millions of dollars in attorneys' fees, ongoing bonding dues, and application costs. Many such firms see these requirements as remnants of an age where money transmitters needed a brick-and-mortar office, located in a specific state, to deal in money. Some digital currency firms rightly see themselves as square pegs being forced into round regulatory holes meant for old business models.

Questions like these deserve consideration, probably before reaching the new idea of having a “BitLicense,” but the “BitLicense” idea raises many interesting questions, too.

IS A “BITLICENSE” TECHNOLOGY-SPECIFIC REGULATION?

A principle of regulation in the modern era is that businesses offering products and services delivered via new technologies should be treated the same as established competitors offering the same products and services. Technology-based competition can shake up established business practices, energize markets, and produce improvements in cost and quality that make life better

² Benjamin M. Lawsky, Superintendent of Financial Services, New York State Department of Financial Services, “Notice of Intent to Hold Hearing on Virtual Currencies, Including Potential NYDFS Issuance of a ‘BitLicense’” (Nov. 14, 2013), <http://www.dfs.ny.gov/about/press2013/virtual-currency-131114.pdf>.

for consumers. Interesting and attractive as new technologies are, regulators have preserved their benefits by according them the same treatment as their “low-tech” predecessors. Fundamentally, regulators generally hold to the principle of technological neutrality.³

An authoritative endorsement of technological neutrality is the Framework for Global Electronic Commerce published by the U.S. government during the Clinton Administration. Widely credited with creating the circumstances for flourishing online commerce, it stated: “rules should be technology neutral (i.e., the rules should neither require nor assume a particular technology) and forward looking (i.e., the rules should not hinder the use or development of technologies in the future).”⁴

Though its application is not always obvious, the goal of technological neutrality is to ensure the same treatment for the same products and services, no matter what technologies deliver them. The protective function of regulation is addressed to outcomes and effects, not to the machines or computers used to produce them.⁵ This generally obliges regulators to examine the markets into which new entrants come – not their methods of service delivery – to determine how existing regulations apply. New technologies and business methods do not necessarily require new or additional regulation to achieve the same protective results, and no particular technological solution should be artificially subsidized or penalized through inconsistent, technology-specific regulation.

The “BitLicense” idea suggests special licensing for services provided digitally. The same services provided without using a technology like Bitcoin would presumably not be similarly licensed. This could, all other things being equal, violate the principle of technological neutrality.

That said, technological neutrality does not preclude all regulation of services provided using new technology. Some technologies may create new services and markets of their own. For example, social media and Internet search are essentially new economic markets that exist thanks to the recent bloom of Internet technologies and content. They have thrived in the absence of particularized regulation, but regulation in these new markets would not necessarily be restricted by the principle of technology neutrality.

It may also be the case that similar services provided using different technologies produce qualitatively different results. Digital publication of music and movies, for example, has different effects than analog publication on the likelihood and amount of copying. This has prompted

³Peter Alexiadis and Miranda Cole, “The Concept of Technology Neutrality,” ECTA Review (European Competitive Telecommunications Association) http://www.gibsondunn.com/fstore/documents/pubs/Alexiadis-ECTA_Review_2004.pdf.

⁴ President William J. Clinton and Vice President Albert Gore, Jr., “A Framework for Global Electronic Commerce,” (July 1, 1997) <http://clinton4.nara.gov/WH/New/Commerce/>.

⁵ Bert-Jaap Koops, “Should ICT Regulation be Technology-Neutral?” published in Bert-Jaap Koops et al., eds., STARTING POINTS FOR ICT REGULATION: DECONSTRUCTING PREVALENT POLICY ONE-LINERS, IT & Law Series, Vol. 9, pp. 77-108, (The Hague: T.M.C. Asser Press, 2006). <http://ssrn.com/abstract=918746>.

changes to copyright law, as well as ongoing debate about both the sufficiency and suitability of copyright to modern technological circumstances.

If digital technologies such as Bitcoin create entirely new services and markets, or if existing services provided with decentralized digital currencies have different effects than their analog or centralized counterparts, new regulation may be appropriate. But an assessment of those services and markets (or those differences) should necessarily precede decisions about what regulatory steps protect the public best. This is especially true in a rapidly-evolving technological and business environment.

COULD A “BITLICENSE” BE SUITABLY TAILORED FOR EMERGING BUSINESS MODELS?

An inventory of the digital currency businesses in New York just one year ago would have included a small group of entrepreneurs and a limited selection of business models. A similar inventory done today would demonstrate literal exponential growth in the number and variety of such businesses. In just one year, the digital currency industry has seen an unprecedented blossoming in the varieties of businesses in operation. Consumers can now select from multiple competing exchanges, payment processors, remittance firms, distributed finance platforms, and hosted wallets—each of whom serve their customers differently. Indeed, even businesses offering largely fungible services now employ starkly different business models and funds flows to do so. Today’s inventory contains many businesses that, from a regulatory perspective, run in meaningfully different ways.

The prospect of tomorrow’s inventory boggles the mind. Emerging uses for digital currency technology like the Bitcoin protocol go well beyond “digital currency.” For example, businesses that will service New York residents are developing so-called “smart contracts” and “distributed chain of title” products. These products use the transmission of what is now known and regulated as digital currency to facilitate, verify, and enforce the negotiation and performance of everyday agreements as well as the transfer of title to property. Most implementations of this technology require the very same entries in Bitcoin’s distributed ledger that a typical digital currency transaction requires. Companies that are not transmitting value in a true sense may make token use of the Bitcoin protocol to effectuate non-financial transactions. Would they be subject to a “BitLicense” intended for financial services providers? The answer is not clear.

In light of the increasing variety of the digital currency businesses serving New York residents, and those to come, drawing up specific regulations today is a particular challenge. In one sense, this is the same challenge faced by all rule-makers. In the case of the digital currency industry, though, it is something like a tailor attempting to fit a child during an unpredictable growth spurt. The tailor can craft a wool suit now, after taking every conceivable measurement and considering the directions he or she thinks the child will grow. Still, what value will the wool suit be when, after the spurt, the child takes up swimming and it becomes apparent that what he needed all along was a swim suit?

People are right to have concerns that overbroad, nonspecific regulation can suppress emerging businesses and deprive consumers of valuable new products. Far worse than non-specificity in regulation, though, is false specificity. Such regulation can strangle a newborn industry in its

crib. The challenge facing the Department is achieving genuine specificity in a highly nonspecific industry like the digital currency space.

WHAT PROBLEMS IS THE “BITLICENSE” MEANT TO SOLVE, AND WOULD A “BITLICENSE” SOLVE THESE PROBLEMS?

Regulation should apply logical means to achieve appropriate ends. That’s easy to say but difficult to do. What are the goals of the “BitLicense” idea, and how well would it achieve them? More importantly, which goals are unique to digital currency businesses? How might a unique license help to achieve them?

The Department issued a Notice of Inquiry in August, 2013, offering three reasons why “putting in place appropriate regulatory safeguards for virtual currencies will be beneficial to the long-term strength of the virtual currency industry.”⁶ The Notice of Inquiry begins with the following justification:

First, safety and soundness requirements help build greater confidence among customers that the funds that they entrust to virtual currency companies will not get stuck in a digital black hole.

If a Bitcoin business takes custody of its customer’s funds, the adequacy of its capital and assets, the quality of its management, its earnings, liquidity, and sensitivity to market risk are all important factors in its ability to do so safely. Licensing is one way to help ensure this. It is not the only way, of course, and a general regulation requiring all businesses of a certain class to adhere to certain standards might be just as effective. Where the stakes are very high—such as when an unsophisticated consumer stores the bulk of his savings with a digital currency company—the prospective protection of licensing is likely warranted.

This consumer protection interest is not unique to digital currencies, though. Any financial services provider should be safe and sound. Any firm that promises prompt transaction processing should provide prompt transaction processing. Consumers should be protected against losing funds in an “analog black hole” as much as a digital one. The first basis articulated for a “BitLicense” by the Department should not apply only to digital currency businesses, but to all businesses.

The second basis suggests that digital currency companies might assist in the commission of serious crimes:

Second, serving as a money changer of choice for terrorists, drug smugglers, illegal weapons dealers, money launderers, and human traffickers could expose the virtual currency industry to extraordinarily serious criminal penalties.

⁶ Benjamin M. Lawsky, Superintendent of Financial Services, New York State Department of Financial Services, “Notice of Inquiry on Virtual Currencies” (Aug. 12, 2013), <http://www.dfs.ny.gov/about/press2013/memo1308121.pdf>.

The public interest at stake here is the interest in having Bitcoin and other digital currency businesses adhere to the criminal laws. The anti-money-laundering laws in some jurisdictions are quite severe. In some cases, they may make financial services providers liable for the misdeeds of their customers despite having no real or constructive knowledge of the wrongdoing.

Since the “BitLicense” idea was conceived, though, the notion that Bitcoin and similar decentralized digital currencies would be havens for money laundering has lost much of its salience. In October last year, federal authorities took down the “Silk Road” Website, which had made itself notorious in part for using Bitcoin as a payment mechanism. The take-down demonstrated that, in fact, Bitcoin is not a powerful tool for escaping criminal prosecution. Most Bitcoin users now realize that the public nature of the block chain makes Bitcoin an unattractive payment system for criminals. Testifying before the U.S. Senate’s Homeland Security and Governmental Affairs Committee in November, the Director of the Financial Crimes Enforcement Network in the U.S. Treasury Department, Jennifer Shasky Calvery said, “Cash is probably still the best medium for money laundering.”⁷

To the extent Bitcoin poses a unique challenge for combating money laundering, financial crime, or terrorist financing, it is in the purview of FinCEN to identify gaps in federal anti-money-laundering policy and enforce rules of the road for money services businesses. The Foundation has made it a priority to work collaboratively with FinCEN and other federal agencies to ensure that we maintain a safe and lawful digital currency environment.

It may be the case that a “BitLicense” could help in some cases. Further detail given to the “BitLicense” idea might reveal what steps are involved and how well those steps would advance digital currency firms’ general adherence to the law.

The third basis provided for the Department’s inquiry is investor protection:

Finally, both virtual currency companies – and the currencies themselves – have received significant interest from investors and venture capital firms. Similar to any other industry, greater transparency and accountability is critical to promoting sustained, long-term investment.

There may be some public interest in the transparency of firms seeking investment, but it seems secondary to the interests of the parties themselves. Digital currency investors are, for the most part, sophisticated parties that can arrange for transparency and accountability that suits their relationships. It is likely that they will seek accountability without the intervention of public authorities spending public dollars. Because the “BitLicense” idea has yet to see much definition, it is difficult to discern how it might improve on private negotiation for solving potential information asymmetries with respect to investment.

⁷ Donna Leinwand Leger, “Bitcoin: What is it? What should government do?”, USA Today (Nov. 18, 2013) <http://www.usatoday.com/story/news/nation/2013/11/18/senate-holds-first-bitcoin-hearing/3628523/>.

The Department's inquiry raises some important questions that are of interest to regulators throughout the country and at different levels of government. This is an issue itself: What levels of government and what governmental bodies or organizations should be involved in generating answers.

IF A “BITLICENSE” IS WARRANTED, HOW SHOULD IT BE ADMINISTERED?

The core of Bitcoin is an open protocol, and it is run on open source software developed by volunteers worldwide. Like any digital currency worth its salt, it is a global protocol, allowing transactions among parties without limitation by their physical locations.

In the past, financial services were inherently local because money was a physical commodity or it was represented by physical notes. Likewise, money services businesses needed a physical location to interact with their customers. That era is ending. Mobile phones are increasingly replacing the transaction counter, and distributed public ledgers will replace clearinghouses. The optimal governmental level at which financial services are regulated may be different than it was when banking and money services began.

There are genuine benefits to localization in governmental systems. Local officials know local circumstances better than their federal or international counterparts. They are also more easily overseen and controlled by their constituents than public officials in larger, more remote jurisdictions. Furthermore, U.S. states and localities have a sharper interest in protecting their residents from fraud and financial mismanagement by third parties.

On the other hand, state and local regulation interacts poorly with national and international markets. Differing standards and licensing regimes from one jurisdiction to another can rapidly raise costs. Costs that are manageable for national and international firms can be prohibitive for firms that have yet to achieve scale. This is particularly salient in an industry whose businesses, wherever located, likely service each of their customers in much the same way, whether those customers live in New York, Nevada, Nigeria, or Norway.

Bitcoin businesses would probably prefer that any new regulatory framework be undertaken at the federal level or with interstate cooperation through a group like the Conference of State Bank Supervisors rather than on an ad-hoc, state-by-state basis.

We view these hearings as the continuation of a much needed conversation among the states and the federal government on how a streamlined, standardized, and fully protective regulatory system can be developed for the United States as a whole, and perhaps internationally. Creating a uniform and standardized framework for digital currency businesses operating in the United States would produce some regulatory parity with the European Union, which has seen greater innovation and competition in the payments industry recently. At the same time, it is important that states retain the power to protect their consumers.

CONCLUSION

We applaud the Department of Financial Services for conducting its activities in the open and for responding to public input and questions in a thoughtful manner. We recognize and appreciate

that this is only the first step in a long and deliberate process of innovation and market restructuring.

The Bitcoin Foundation is pleased to see that the Department recognizes the increasing adoption of digital currencies in general and Bitcoin specifically. As many federal agencies have stated, digital currencies have the potential to improve the lives of New Yorkers, Americans, and the global community at large. A safe and sane regulatory environment is critical to that outcome, and we are glad to see the Department of Financial Services bringing its voice to bear on this important conversation.

Thank you for the opportunity to share my, and the Bitcoin Foundation's, views with you.