

**Testimony of Patrick Murck  
General Counsel, the Bitcoin Foundation  
to the Senate Committee on Homeland Security and  
Governmental Affairs  
“Beyond Silk Road: Potential Risks, Threats, and  
Promises of Virtual Currencies”  
November 18, 2013**

### **Executive Summary**

Bitcoin is a decentralized store of value and open-ledger payment network that operates securely, efficiently, and at low cost without the need for any third-party intermediaries. The Bitcoin protocol allows individuals or service providers access to a global financial system that will see rapid innovation.

Bitcoin and digital currency alone will not alleviate issues of poverty and financial exclusion that effect vulnerable populations around the world. However, Bitcoin can provide a safe store of wealth and a global transaction network that cannot be corrupted or abused by those who would seek to exploit or harm vulnerable populations. It can help advance liberty and dignity for people worldwide, restore financial privacy for law-abiding people, and provide a stable money supply in countries where the currency may be mismanaged.

The United States has an acute interest in maintaining its place as a global leader in developing this cutting edge technology, fostering financial services innovation, and spreading individual freedom and liberty around the globe. Applying consistent rules and regulations that encourage technological experimentation is critical to a vibrant entrepreneurial community, and this committee’s work may help to chart a safe and sane regulatory course for the digital economy in general and Bitcoin specifically.

Though challenges exist, Bitcoin does not pose a unique or unsolvable challenge to law enforcement or existing regulatory structures. Bitcoin service providers enter a highly regulated marketplace with deeply entrenched competitors.

The Bitcoin Foundation looks forward to continuing a dialog with this committee and others, federal and state regulators, law enforcement agencies, financial services firms and banks, and academics. Together, we can help ensure that the substantial benefits of the digital economy are attained while the risks are mitigated.

## Introduction

Good afternoon, Chairman Carper, Ranking Member Coburn, and Distinguished Members of the Committee. I am pleased to have the opportunity to speak with you today. My name is Patrick Murck, and I am general counsel of the Bitcoin Foundation.

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 Bitcoin Foundation represents an international membership and our focus is global. Currently, about 60% of the foundation's membership is international. 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, earlier this year, will be held in Holland May 15-17, 2014. The Bitcoin Foundation is actively developing systems to empower local 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 a founding member of the Bitcoin Foundation and have served as General Counsel since its inception. Additionally, I have been an executive in legal and business development for a number of digital currency companies. In private practice, I have represented digital currency clients, and worked as a telecom, media, and technology attorney with a Washington, D.C.-based law firm. I am a native of Washington, D.C., and received my undergraduate degree from American University and my J.D. with honors from Catholic University, Columbus School of Law.

## About Bitcoin

Bitcoin was invented in 2008 as a peer-to-peer payment system for use in online transactions.<sup>1</sup> 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.

---

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

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 so 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 and develop the software on its own, independent of such an interloper.

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 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**

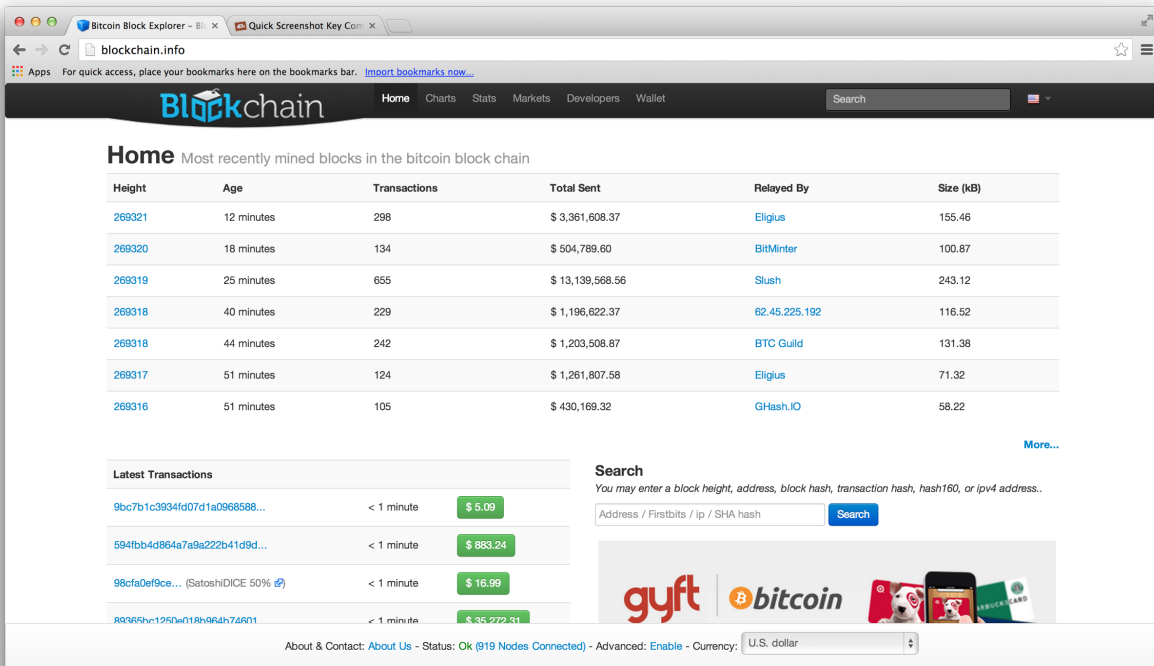
The public ledger is crucial to understand. The heart of the Bitcoin technology is this ledger that records all transactions occurring in the system. The ledger is broken into blocks of transactions, and each new block of transactions is linked to the previous block, forming what is called the “block 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. This is costly in terms of computer processing (hardware, electricity, and time). But though the problem is difficult to solve, the solution is easy to verify, so a miner discovering the solution can declare it (Eureka!), and nodes across the network will promptly confirm the new block.

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 spending the bitcoins they own twice. 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 allows there

to be purely digital transactions without any central administrator, who would otherwise manage the ledger and police against double spending of a digital currency.



The screenshot shows the blockchain.info website interface. At the top, there is a navigation bar with links for Home, Charts, Stats, Markets, Developers, and Wallet. Below this is a search bar. The main content area is titled "Home" and displays "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

Below the table, there is a "Latest Transactions" section showing several transactions with their hashes, ages, and values. A search bar is also present, allowing users to search for blocks, addresses, or transaction hashes. At the bottom, there is a footer with "About & Contact" links, status information ("Status: Ok (919 Nodes Connected)", "Advanced: Enable", "Currency: U.S. dollar"), and a small advertisement for gyft and bitcoin.

Source: *blockchain.info*

## 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. While wallets can be created and maintained using the Bitcoin open-source software, in practice many users have accounts with one or more Bitcoin service providers and store bitcoins at addresses provided through their accounts. 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 funds using PayPal or traditional payment systems, or sending an email. Administering a payment or money system is not the only use of a universal public ledger. The Bitcoin protocol may expand over time to facilitate many advanced services such as deposits, escrows, and potentially even distributed stock trading. And the Bitcoin protocol may find many uses beyond payments and money, including proving the existence of documents, establishing and verifying human identities, Internet naming and numbering, and many more.

Bitcoin is a protocol. It is like TCP/IP, which enables all the different uses people around the globe invented for the Internet. And it is like HTML, which enables all the different uses people invented for the World Wide Web without having to ask anyone's permission. 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.

## **Bitcoin's Promise**

There may be as many reasons to support Bitcoin as there are Bitcoin supporters. But we believe Bitcoin holds out a number of powerfully beneficial social and economic outcomes, including global financial inclusion, enhanced personal liberty and dignity, improved financial privacy, and a stable money supply for people in countries where monetary instability may threaten prosperity and even peace.

## **Global Financial Inclusion**

In April 2012, a World Bank report found that half of adults worldwide are unbanked due to barriers such as high cost, physical distance, and lack of proper documentation.<sup>2</sup> It is hard to believe amid the relative wealth of the United States, but half the world's population lacks access to financial services that are everyday matters to us. These are rungs on the ladder from poverty to prosperity that many people cannot access at all.

A 2001 study confirms in striking terms what common sense suggests: Informal saving methods such as keeping physical money in the home are subject to losses as high as 26% of the

---

<sup>2</sup> Asli Demirguc-Kunt and Leora Klapper, "Measuring Financial Inclusion: The Global Findex Database," Policy Research Working Paper No. 6025, The World Bank, Development Research Group, Finance and Private Sector Development Team (April 2012) [http://www-wds.worldbank.org/servlet/WDSContentServer/WDSP/IB/2012/04/19/000158349\\_20120419083611/Rendered/PDF/WPS6025.pdf](http://www-wds.worldbank.org/servlet/WDSContentServer/WDSP/IB/2012/04/19/000158349_20120419083611/Rendered/PDF/WPS6025.pdf).

amounts saved per year.<sup>3</sup> Around the world, multitudes of hard-working, capable people simply lose wealth that they could use for food, shelter, medical care, and the education of their children because of underdeveloped financial infrastructure.

Bitcoin is an extremely lightweight financial infrastructure because it can exist wherever there is Internet or cell phone access and the requisite computing device, smartphone, or SMS-capable phone. Whether it brings people into existing financial services systems, or if it secures people's wealth better outside of formal systems, we believe Bitcoin has tremendous potential to improve the capacity of people around the world to build and store wealth. That greater access to wealth may produce improved outcomes in the area of food and nutrition, health and longevity, education and child development, family structure, protection of civil and political rights, and even political stability and global security.

It would be a mistake, of course, to think that Bitcoin can simply be sprinkled on longstanding social, economic, and political problems to easily solve them. And it will take time and effort to propagate the infrastructure that is needed to access and use Bitcoin in the far corners of the globe. But the Bitcoin Foundation will be fostering businesses and business environments that allow local merchants everywhere to accept bitcoins and that allow convertibility of Bitcoin to local currencies.

We believe Bitcoin can improve the lot of the world's poor. If these efforts and the underlying genius of the Bitcoin protocol improve the financial situation and wherewithal of millions, hundreds of millions, or perhaps billions of people by even a small fraction, the total quantum of good done by Bitcoin will be quite large.

## **Liberty and Dignity**

Along similar lines, we see potential for Bitcoin to improve people's enjoyment of autonomy, liberty, and dignity everywhere in the world.

Deep running principles—in Western thought, at least—emphasize individuals' ownership of themselves and the things they produce. In varying degrees around the world, though, governments and powerful private actors often encroach on people's rights and their ability to use and dispose of their property as they see fit. This makes people objects of control, denying them the dignity of being autonomous, independent, and responsible moral actors whose well-being and self-worth rise or fall based on their own decisions.

---

<sup>3</sup> Graham A.N. Wright and Leonard Mutesasira, "The Relative Risks to the Savings of Poor People," MicroSave (January 2001) [http://www.microfinancegateway.org/gm/document-1.9.28889/26216\\_file\\_The\\_Relative\\_Risks\\_.pdf](http://www.microfinancegateway.org/gm/document-1.9.28889/26216_file_The_Relative_Risks_.pdf).

Bitcoin can facilitate private and anonymous transactions, which are resistant to oversight and control. Because it can aid people in deploying their property less subject to external impediments, Bitcoin may expand the realm of autonomy, liberty, and dignity for people around the world. This means traveling from market to village without being robbed, it means avoiding official corruption and confiscatory tax regimes, and many more things. It also means that people using Bitcoin can fund controversial speech or causes that governments and powerful private actors may seek to suppress using their control of conventional financial services. Bitcoin is a communications protocol, and it has the Internet virtue of being censorship-resistant, which expands freedom of speech and freedom of action.

This by no means implies that using Bitcoin can or should provide anyone immunity from the law. Though it has sometimes been portrayed as such in careless media stories, Bitcoin is not a magic cloaking device that allows criminal actors free reign. It does offer enhanced privacy protections, however, which is the just desert of hundreds of millions of law-abiding Americans and billions of law-abiding people worldwide.

## **Financial Privacy**

The American people have been reminded this year of reasons to be concerned for their privacy, as have people around the world. We believe that peaceful, law-abiding people are entitled to protections for their privacy.

In the United States, constitutional protections such as the Fourth Amendment should allow people to be secure against unreasonable searches and seizures of their persons, houses, papers, and effects, even when their papers and effects are in digital form. We also believe the International Covenant on Civil and Political Rights bars arbitrary or unlawful interference with one's privacy, family, home, or correspondence, regardless of format.

Privacy is many things to many people. Among other things, it is the individual's bulwark against objectification by governments, corporations, and other individuals. People who have their privacy have more personal power and a richer, more independent life. Privacy is also a means to various ends, including personal security and freedom of speech and action.

Many at the Bitcoin Foundation and in the Bitcoin community are acutely aware that financial transactions in nearly every format are subject to some degree of surveillance. For good and bad, centralized payment systems always include gatekeepers and overseers. Bitcoin can facilitate fully private transactions, which, when legal in the jurisdictions where they occur, are nobody's business but the parties to the transactions.

Privacy can mask wrongful behavior, of course, and governments have a valid interest in information about activities they have made illegal. And there are certainly circumstances when

Bitcoin-based services will require and benefit from collection of personal information about users. So “more privacy” is not the essence of Bitcoin. But the use of Bitcoin should strengthen the hand of individual users to protect their privacy.

Today, privacy in financial services is typically dictated by governments and corporations. The bitcoin ecosystem should be more amenable to what we refer to as “user-defined privacy.” Bitcoin may once again allow law-abiding people to have privacy on the terms they want it.

## **Stable Money Supply**

A significant benefit of Bitcoin in the eyes of many in the Bitcoin community is its assurance of a stable base money supply. As I noted earlier, the bitcoin protocol provides for mining of a limited number of bitcoins, and that limit cannot be changed without the consensus of the community. The production of bitcoins will slow according to a schedule until around 2140, when the last new fraction of a bitcoin, known as a satoshi, will be mined just shy of 21 million bitcoins.

The rate of new bitcoin mining is similar to the mining rate of precious metals such as gold or silver. A low rate of new creation relative to the existing base means that added supply does not significantly debase the value of the existing stock. Like these precious metals and unlike fiat currencies, the stock of Bitcoin cannot increase rapidly, causing them to drop in value relative to other goods.

This means that Bitcoin is largely inflation-proof. Time and experience may prove it to be a more stable store of value than many fiat currencies, while it enjoys advantages over precious metals in other respects, such as transferability, divisibility, security in storage, and so on. This makes Bitcoin a potential key to financial well-being for savers and investors worldwide, but particularly in those jurisdictions where fiat currencies may be mismanaged.

Some Bitcoin enthusiasts may crow about the idea of Bitcoin replacing national fiat currencies, and it may be possible in a small country sometime in the future. The way to contemplate Bitcoin in the near term is as a means of making a small central bank or currency bloc accountable if they poorly manage their portfolio, while at the same time ameliorating the economic effects of the central bank’s mismanagement. We believe all the world’s currency systems are safer if there is a more diverse web of monetary systems with which to work. We believe that Bitcoin can add to monetary stability both directly, by acting as stable money itself, and indirectly, by husbanding the behavior of central bankers.

We are very motivated at the Bitcoin Foundation by the social and economic benefits that we believe Bitcoin has to offer. We are mindful, of course, that Bitcoin is subject to misuse. It would be regrettable if the many benefits Bitcoin offers were denied the world’s people, or even delayed, by overreaction to the challenges that come with this emerging new technology. We



share your opinion, Chairman Carper, stated very well in a recent press release, that “we need to develop thoughtful, nimble and sensible federal policies that protect the public without stifling innovation and economic growth.”

## **Beyond Silk Road**

As you are likely aware, federal law enforcement recently seized the "Silk Road" website and arrested its alleged controller, Ross Ulbricht. With Silk Road shuttered, it is clear that Bitcoin thrives irrespective of sensationalist stories about a “dark web” of illicit transactions. Silk Road drew attention to Bitcoin, and the attention may have helped Bitcoin go mainstream, but now that it is mainstream, Bitcoin is beyond Silk Road.

Bitcoin and tools like Tor, which the U.S. Navy invented to secure the communications of ships, and which protects journalists and dissidents around the world, can be used for illicit purposes. But, as the Silk Road case makes evident, Bitcoin is not a magic cloak for illicit transactions. Bitcoin is a new and advanced technology, and law enforcement will likely have to develop new methodologies for interdicting and investigating criminal activity. This does not make it harder for law enforcement to do its important job. It simply means that law enforcement will have to learn this protocol and adjust its methods somewhat, something that has been successfully accomplished in many different contexts before.

In any event, the choice for policymakers is not whether Bitcoin will exist, and it is not whether Bitcoin will be used in the United States. The question is whether Bitcoin businesses will be integrated with the U.S. financial services system and become producers of U.S. jobs and economic growth that respond to legitimate U.S. law enforcement inquiries, or whether Bitcoin businesses will move offshore, taking jobs and innovation with them, and making it harder for U.S. law enforcement to gather information for legitimate investigations.

## **True: Bitcoin Can be Used for Illicit Purposes, Like All Other Forms of Payment**

Bitcoin is no different than any other payment system, form of money, or technical infrastructure. It can be used by criminals. Bitcoin was used on the Silk Road website, which was primarily a market for illegal drugs. The less this colors public and policymaker assessments of Bitcoin, the better. Criminals do turn the beneficial instruments of society to their ends. But overreacting to this simple and obvious fact because Bitcoin is exotic and new could delay Americans enjoyment of Bitcoin’s benefits, which are vastly greater than its potential costs.

An analysis by digital currency research and data site *The Genesis Block* puts the relationship between Silk Road and Bitcoin in perspective. In a thoroughly researched October 2013 piece entitled, “Analysis of Silk Road’s Historical Impact on Bitcoin,” writer Jonathan Stacke finds that

“a significant portion of bitcoin’s early traction and price gains can be traced directly to Silk Road, with that impact waning over time, most dramatically in the past six months.”<sup>4</sup>

In late December 2010 and early 2011, Stacke finds, people acquiring bitcoin for use on Silk Road may have produced a spike in Bitcoin’s price against the U.S. dollar from \$0.30 to a trading range of \$0.65 to \$0.80. Mainstream press attention from *The New York Times*, *Time*, and Gawker.com then began a far more significant price spike that reached \$30 per Bitcoin before prices settled to a new higher equilibrium of around \$5. Succeeding price changes, Stacke finds, correlate to events and news reporting unrelated to Silk Road. But denial-of-service attacks on Silk Road in April and May of 2012 show effects falling to between 25% and 35% of Bitcoin’s price. When Silk Road was finally taken down last month, the price of Bitcoin suffered a one-day drop of about 20%, but then began climbing relentlessly, more than doubling since then.

The Bitcoin market is infinitesimal compared to its potential size, so it is subject to relatively high volatility. That volatility will drop over time, as the worldwide use of the Bitcoin protocol grows. Psychology around this new asset probably also drives wider price swings than will occur in the future. But judging by their behavior in the markets, the Bitcoin community seems relieved and optimistic about the falling relevance of Silk Road and illicit markets.

As with every other payment system, criminals will surely and regrettably use bitcoins. That said, law enforcement appears well-equipped to deal with copycat sites to Silk Road. In fact, copycats “Atlantis” and “Project Black Flag” have recently shuttered themselves spontaneously and absconded with their users’ bitcoins. Criminals are not reliable business partners, and they will turn on each other when the circumstances are right. Anonymity is also a two-way street. A top dealer on Silk Road was actively working with federal law enforcement, the anonymity of Silk Road making it easier for them to make undercover drug deals and subsequent arrests. A user of “Black Market Reloaded,” another Silk Road copycat, was recently arrested.

The document charging Ross Ulbricht noted Bitcoin’s legitimate uses, and it shows that solid law enforcement work is effective with respect to Bitcoin and Tor just like other payment and communications systems. Silk Road is gone. The lawful uses of Bitcoin will continue to grow in number and quantity, easily swamping illicit uses and helping to bring the association between Bitcoin and crime into accurate perspective.

---

<sup>4</sup> Jonathan Stacke, “Analysis of Silk Road’s Historical Impact on Bitcoin,” The Genesis Block, <http://thegenesisblock.com/analysis-silk-roads-historical-impact-bitcoin/>.

## **New, Not Necessarily Harder**

As I said earlier, Bitcoin is not a magic cloak for illicit transactions. At the same time, it certainly may provide new challenges to law enforcement, who will have to learn about Bitcoin and the block chain to pursue investigations. But we expect the law enforcement challenge to be different, not necessarily harder, in the Bitcoin environment. Law enforcement has and will be able to successfully investigate and prosecute criminals who use bitcoins.

We see the law enforcement paradigm in the Bitcoin ecosystem differing from the status quo in the following way: Law enforcement investigations using payment systems today typically are "parties known/transactions unknown." Having some insight into suspected criminal behavior, law enforcers use warrants, subpoenas, and other legitimate investigative tools to learn from financial services providers what transactions their suspects have engaged in.

If Bitcoin businesses thrive in the United States, investigations may still follow this model, gathering the Bitcoin transactions of existing suspects from U.S.-based providers. But investigations may also follow a "transaction known/parties unknown" model. The block chain—that worldwide public ledger of all transactions—may permit law enforcement to observe transaction flows that they know to be illicit or to use the products of illicit activity. Tracing illicit transactions to transactions that identify the parties will reveal the identities of suspects.

The block chain may be so revealing that the problem with Bitcoin is the difficulty law-abiding people have maintaining privacy. Bitcoin mixing services, which are intended to obscure the source of their users' bitcoins, may become popular if the sense of the Bitcoin community is that the flow of bitcoins is being used for excessive or illegitimate surveillance of private financial activity. Incautious behavior on the part of governments and law enforcement could make the Bitcoin environment harder to work with.

The issues here are complex, and the capacity of mixing services to truly obscure transaction flow will be the subject of much study over time. But a cautious law enforcement approach to Bitcoin is much smarter than trying to convert the Bitcoin block chain and the data held by Bitcoin service providers into a mass surveillance system.

Nimble and sensible interaction with the Bitcoin community will permit law enforcement to protect the public without stifling innovation and economic growth. U.S. law enforcement will have better access to data sought under legitimate legal processes if the U.S. Bitcoin industry is strong. Simply put, U.S. companies will be easier to work with than overseas firms. But some circumstances are already driving Bitcoin businesses offshore.

## **Bitcoin and the U.S. Financial Services System**

While we have been pleased by the solicitous tone of official policy statements coming from U.S. federal government agencies, some factors appear to be driving Bitcoin start-ups away from U.S. shores. To the extent this happens, it comes at the cost of innovation, jobs, and economic growth that Bitcoin promises the United States. Conditions are improving, but initial hostility to Bitcoin in some states may have unnerved U.S. financial services providers, forestalling their adoption of Bitcoin and their provision of service to Bitcoin businesses. We would like to see conditions improve.

### **Official Policy Recognizes Bitcoin**

We have been pleased by federal regulators' recognition of Bitcoin as an exciting and innovative entrant into the field of digital currency and financial services generally. Directly or indirectly a number of federal agencies have recognized Bitcoin and even touted its genius.

In March, for example, the Financial Crimes Enforcement Network (FinCEN) in the U.S. Treasury Department issued guidance on the application of money transmitter rules to Bitcoin businesses. Some interpreted this as official recognition that Bitcoin is valid and legitimate. We believe it signaled that existing regulation covers most of the business activity taking place in the Bitcoin ecosystem.

There are details on which we might quibble, and to the extent FinCEN promulgated new legislative rules, we believe they should have been issued after a notice-and-comment rulemaking. But, the Bitcoin Foundation's successful meeting with financial regulators, which FinCEN hosted in August, shows that the Treasury Department and others recognize the value of dialogue and the capacity of the Bitcoin Foundation to inform their work.

Also in August, at the urging of the Securities and Exchange Commission, a federal judge ruled that Bitcoin is a form of money also fitting the definition of a security under the Securities Exchange Act. A defendant charged with pursuing a Ponzi scheme argued that the SEC did not have jurisdiction over Bitcoin transactions. The judge struck this argument down on the basis that, just like with any other form of payment, it is illegal to use Bitcoin for fraud. This is undeniably sensible and helps to protect the Bitcoin community from similar frauds and scams that may arise in the future.

These are legal questions on which more work will have to be done. Bitcoin's differing characteristics potentially make it a different asset class than what existing regulation recognizes. But it fits well within the legal and regulatory regimes that bar frauds like the Ponzi scheme at issue in that case.

The official reception for Bitcoin among U.S. federal regulators has been essentially welcoming. Even agencies that one might assume to be antagonistic to Bitcoin acknowledge its legitimacy. The Department of Justice, for example, in its charging document for the alleged founder of the Silk Road, Ross Ulbricht, took pains to note that bitcoins are legal “in and of themselves” and “have known legitimate uses.” The Federal Reserve Bank of Chicago issued a Bitcoin “primer” two weeks ago in which senior economist François R. Velde called Bitcoin a “remarkable conceptual and technical achievement, which may well be used by existing financial institutions.”

We look forward to continuing our dialogue with policymakers and regulators at both the federal and state levels. In addition to the Bitcoin Foundation, there are several industry-led efforts underway to create standards of care and best practices for digital currency exchanges (for example, the committee to explore D.A.T.A.), transaction processing (“mining” in some cases), and digital currency investors. We are equally pleased to support these industry efforts.

We appreciate this committee’s inquiries of federal agencies regarding their approaches to Bitcoin. Our belief, supported by the agency activities noted above, is that Bitcoin and Bitcoin businesses largely fit into existing regulatory structures. Where they may not, the framework for analysis we recommend is identifying the few “gaps” in public protection that Bitcoin’s unique characteristics may produce and determining how best to fill them. We look forward to ongoing dialogue that your sensibly structured hearing and thoughtful public comments presage.

## **Improving the Environment for Bitcoin**

While official federal policy as developed in the agencies seems clearly to recognize Bitcoin as an innovative source of economic growth and jobs, the early treatment of Bitcoin in some states and in the banking industry has clouded the picture of the United States as a center of innovation and business development. We are optimistic that the environment for Bitcoin in the United States will improve.

As illustration of early antipathy to Bitcoin, some states have issued subpoenas and cease-and-desist letters to Bitcoin businesses and others involved in the Bitcoin community. While most states and federal regulators seem to intuitively understand this, these harsh actions are not conducive to an open and productive dialog. One state regulator issued subpoenas to 22 Bitcoin-related businesses and went on television making unfounded statements relating Bitcoin to “narcoterrorism.” Irresponsible public statements like these make it more likely that legitimate Bitcoin businesses will relocate to more welcoming countries.

The Bitcoin Foundation is well prepared to respond to legal inquiries and our membership does not rely on cable television for its information, but startups and small businesses are harder-pressed to respond. They may spend much of their seed capital on lawyers responding to

carelessly founded government inquests. And investors, recognizing the risks of heavy-handed government actions like this, may pull out or never materialize to invest in Bitcoin companies.

We do believe that conditions are right for improvement, and we are open to dialogue with all states, as with the federal government and its agencies, seeking to apply their laws to Bitcoin use and Bitcoin businesses. In fact, we have recently perceived a marked improvement in the tone and tenor taken by both state officials and bank executives. We are optimistic that we can generate greater understanding of the opportunity and potential for this part of the digital economy.

There are certainly risks to serving innovative small businesses, but these are matched by potential profit, and we hope that U.S. financial services providers will integrate with Bitcoin. So far, U.S. banks and other financial services providers have yet to harness Bitcoin's transformative power. As a result, most Bitcoin businesses have been started by technology experts with less experience in the intricacies of federal and state anti-money-laundering laws or know-your-customer rules. Established banks could provide expert counsel and cultivate customer relationships with these companies, and we think they should.

Indeed, banks could brand and offer Bitcoin exchange services themselves, quickly becoming the de facto leaders because of their regulatory status and supreme customer identity procedures. As it stands, a majority of people still prefer banks over trusting Apple, Google, or PayPal with sensitive data. Security at banks and financial institutions usually represents the strongest in the world among private businesses. For those individuals desiring a third-party safe-keeper for their Bitcoin balances, banks would provide several obvious advantages.

Bitcoin is a global protocol that will thrive with or without U.S. government support and with or without U.S. banks, but thoughtful policymakers and businesspeople in the U.S. should work to integrate Bitcoin and banking in the United States. Doing so will bring the benefits of Bitcoin to the United States as quickly as they reach the rest of the world. Innovation, economic growth, and jobs related to Bitcoin should be welcomed by policymakers at every governmental level in the United States.

## **Conclusion**

The horizon is bright for Bitcoin under any circumstance. We at the Bitcoin Foundation believe that this innovative protocol can deliver financial services and improve the lot of people the world over. We see coordinate gains in liberty and human dignity, also spanning the globe. Bitcoin-based financial services can improve the privacy of law-abiding Americans and people around the world. And Bitcoin may provide a stable base money supply in countries where currency is mismanaged.

The Bitcoin story goes far beyond Silk Road. Nearly every technology has potential bad uses, but the vast majority of people are law-abiding and hard-working. In their hands, Bitcoin will produce benefits that vastly outstrip the costs of the illegal and wrongful uses.

We are pleased to report that federal agencies across the spectrum are acknowledging Bitcoin and incorporating it into their regulatory regimes. For the most part, Bitcoin fits into existing regulatory structures, and we see little need for new or changed laws, though careful assessment of regulatory “gaps” may reveal where the law requires tweaks to account for Bitcoin.

We see encouraging signs that early skepticism about Bitcoin in some quarters is giving way to interest and support. This bodes well for the United States because the question is not whether Bitcoin will be used here. It is how long Bitcoin’s adoption will take and whether the United States will be leaders in the digital economy.

Thank you for the opportunity to share my views with you.