Testimony of

Jerry Brito
Executive Director
Coin Center

Before the

Subcommittee on Commerce, Manufacturing & Trade
Committee on Energy & Commerce
U.S. House of Representatives

Hearing on

Digital Currency and Blockchain Technology

March 16, 2016

Mr. Chairman and members of the committee:

My name is Jerry Brito and I am the Executive Director of Coin Center, a non-profit research and advocacy center focused on the public policy issues facing cryptocurrencies like Bitcoin. I applaud you for taking the time to learn more about this technology and its social, economic, and policy implications. In what follows, I will provide some background on the technology and touch on its potential benefits and the challenges it poses.

Bitcoin is frequently described as a “digital currency.” While that description is accurate, it can be misleading because it is at once too broad and too narrow. It is too broad because Bitcoin is a very particular kind of digital currency—a cryptography based currency (indeed, it is the first of its kind). It is too narrow because although currency is one aspect of the Bitcoin system; Bitcoin is more broadly an Internet protocol with many applications beyond payments or money transfer. Think of it like email or the Web—an open network to which anyone can connect without requiring permission from a central authority, anyone can send a message to anyone else, and on top of which you can freely build many different kinds of applications.

That said, online virtual currencies are nothing new. They have existed for decades. From Microsoft Points to Facebook Credits. Neither are online payments systems new. PayPal, Visa, and Western Union Pay are all examples. So what is it about Bitcoin, and similar cryptography based currencies, that make them unique?

Bitcoin is the world's first completely decentralized digital currency, and it is the “decentralized” part that makes it unique. Prior to Bitcoin's invention in 2009, online currencies or payments systems had to be managed by a central authority. For example, Facebook issuing Facebook Points, or PayPal ensuring that transactions between its customers are reconciled. However, by solving a longstanding conundrum in computer science known as the “double spending” problem, Bitcoin for the first time makes possible transactions online that are person to person, without the need for an intermediary between them, just like cash.

Before the invention of Bitcoin, for two parties to transact electronically always required that they employ a third-party intermediary like PayPal or Visa. Without such intermediaries, there was no way to ensure that money could not be spent twice. To understand why, it is useful to consider cash transactions.

A physical cash transaction requires no intermediary. If I hand you $100 bill, you now have it and I do not. I cannot spend the same $100 bill again because you now have it, and we can verify that you are the sole possessor of the bill simply by looking at our hands. Replicating such a cash-like transaction electronically, however, had been difficult.

If instead of a $100 bill we use a $100 digital file, I can send it to you by attaching it to a message. But as anyone who has ever sent an email attachment knows, when you send a Word document or a photo to a friend, the file is not deleted from your computer; you retain a perfect digital copy. So, if I send you a $100 file, you have no way of verifying that you are now the sole possessor of that file. The same file remains on my computer, and I could send it to a second person. I could spend the same $100 a second and a third time.

The way we solved this conundrum, which computer scientists called the “double-spending problem,”[1] was by employing trusted third-party intermediaries. For example, you and I might have accounts with PayPal, which keeps a ledger of all accountholder balances. To send you $100, I instruct PayPal to make the transfer, and it deducts the amount from my balance and adds it to yours. That transaction reconciles to zero, and at the end of the day all transactions across all accountholders also reconcile to zero. We each trust PayPal to verify balances and transactions using a centralized ledger that it controls.

[1] David Chaum, “Achieving Electronic Privacy,” *Scientific American* (August 1992): 96–101.

Bitcoin's innovation–and it is a profound one–is that for the first time it solved the double-spending problem without relying on a trusted third-party. Bitcoin accomplishes this feat by distributing the necessary ledger among all users of the system via a peer-to-peer network. Every transaction in the Bitcoin economy is registered in a public ledger called the *blockchain*. Complete copies of the blockchain reside on the computers of everyone who uses Bitcoin. New transactions are checked against the blockchain to ensure that the same Bitcoins have not been previously allocated, thus eliminating the double-spending problem.

Transactions are checked and added to the blockchain by users called "miners," who lend their computers' processing power for that purpose. Miners essentially solve the difficult cryptographic math problems that allow them to securely add transactions to the ledger, and they are awarded newly created Bitcoins for their trouble.[2] This is how new bitcoins are injected into the money supply. As more users become miners and the processing power that is dedicated to mining increases, the Bitcoin protocol also increases the difficulty of the cryptographic problem miners must solve, thus ensuring that new bitcoins are always mined at a predictable and limited rate.

This inflation will not continue forever. Bitcoin was designed to mimic the extraction of gold or other precious metals from the earth–only a limited, known number of the coins can ever be dug up. The arbitrary number chosen to be the cap is 21 million bitcoins. Miners also have a second stream of income: voluntary fees that one can attach to a transaction to ensure that it is promptly processed. Once all bitcoins have been issued, these fees will incentivize miners to continue to process payments. These fees will be set at a market rate based on supply and demand.

This certainty and predictability appeals to many because it makes artificial currency inflation impossible. In most countries, a central bank controls the money supply, and sometimes (such as an economic crisis) it may decide to inject more money into an economy. A central bank does this essentially by printing more money. More cash in the system, however, means that the cash you already hold will be worth less. By contrast, because Bitcoin has no central authority, no one can decide to increase the money supply. The rate of new Bitcoins introduced to the system is based on a public algorithm and is therefore perfectly predictable.

Yet as interesting as Bitcoin's deflationary nature is, it is the decentralized design that makes the innovation truly revolutionary. It means that you and I can transact online without PayPal or any other central authority between us, just as we would if we met in person and exchanged dollar bills. Real digital cash is now possible.

Benefits

[2] Peter Van Valkenburgh, What is Bitcoin Mining, and Why is it Necessary? A Backgrounder for Policymakers, Coin Center, Dec. 15, 2014, *available at* https://coincenter.org/2014/12/bitcoin-mining/

You may be thinking to yourself at this point, this is all very interesting, but why would I use Bitcoin when my credit cards work just fine and there is an extensive payments infrastructure in place?

The first answer is that most people in the world do not have access to credit cards or electronic payments, yet they soon will have access to the Internet via smartphones and other inexpensive devices. Bitcoin allows anyone with access to the Internet to engage in mobile commerce even if PayPal or Visa do not serve their country. This is a boon not just to the billions of unbanked persons in the developing world, but also to merchants in the developed world who can now trade with previously untapped markets.

One online technology retailer that accepts bitcoin payments reported that it now sells to nearly 40 countries, many of which are "high-risk markets" to which they previously would not have had access.[3] Customers from India and Pakistan, for example, now have a way of placing an order from a U.S. merchant, and because Bitcoin payments are not reversible, the merchant can be sure he has the money before he ships the goods.

There are many other potential benefits of the technology. For example, micropayments of a few pennies or less are not economically feasible using our existing payments networks. Cryptocurrency technology has the potential to make such tiny payments possible and allow users for the first time to pay directly for the content they consume on websites rather than view ads. Instead of all-you-can-eat plans, digital metering could become a new option for consumers—for minutes of music listened to or video watched or every kilobyte of Wi-Fi used. Additionally, cryptocurrencies make standardized machine-to-machine payments truly feasible for the first time, which will be a key component of the growing "Internet of Things." Imagine being in a hurry and the self-driving Uber car you are riding can pay other autonomous vehicles on the road to let it pass.

Other more prosaic use cases involve settlement of different kinds. For example, international wire transfers today can take days. If the banks at the endpoints of a transfer do not have accounts with each other, they will use one or more intermediary correspondent banks at which they each do have accounts, adding to the cost and time of a transfer. A global ledger used by all banks could make correspondent banking much more efficient. The same principle can be applied to securities and commodities trading by using the ledger to track particular assets rather than simply money.[4]

To date, bitcoins have represented money at a floating exchange rate, and the Bitcoin network has been employed as a fast and inexpensive payments or money transfer system. But there is no reason why particular bitcoins could not represent something besides money. If we conceive of bitcoins simply as tokens, then other applications

[3] Dylan Love, "A Guy Who Owns a Bitcoin-Only Electronics Store Is Revealing Everything on Reddit," *Business Insider*, March 18, 2014, http:// www.businessinsider.com/e-commerce-with-bitcoin-2014-3

[4] Brock Cusick, What are Colored Coins? A Backgrounder for Policymakers, Coin Center, Nov. 30, 2014, *available at* https://coincenter.org/2014/11/colored-coins/

become apparent. For example, we could agree that a particular bitcoin (or, indeed, an infinitesimally small fraction of a bitcoin so as to allow for many tokens) represents a house, a car, a share of stock, a futures contract, or an ounce of gold. Conceived of in this way, the Bitcoin blockchain then becomes more than just a payment system. It can be a completely decentralized and perfectly reconciled property registry.

Remittances also help illustrate the potential cost advantages of cryptocurrencies like Bitcoin. In 2012, immigrants to developed countries sent about $400 billion in remittances back to relatives living in developing countries, and that figure is projected to increase to over $500 billion by 2015.[5] According to the World Bank, the global average fee for sending remittances in 2013 was nine percent.[6] With Bitcoin it could be as low as one percent. Remittances can also take days to clear. Bitcoin transactions, on the other hand, are instantaneous, and can take less than an hour to completely confirm.

Finally, Bitcoin is censorship-resistant. For example, after WikiLeaks began releasing its trove of State Department cables, individuals who sought to make a donation to the organization found that many payment processors, including Visa, MasterCard, and PayPal, would not remit money to WikiLeaks due to U.S. government pressure. PayPal even froze the group's account so that it could not access funds it had already collected. Today, WikiLeaks accepts bitcoins for donations, and because Bitcoin is decentralized, there is no intermediary that can be pressured or censored. While this makes prior restraint of financial transactions impossible, it does not preclude a person from being punished after the fact for engaging in illegal transactions.

Unlike cash, Bitcoin is not anonymous, since a public record is made of every transaction.[7] But it is more private than traditional electronic payments, such as credit card transactions, because users' identities need not be tied to the transactions. That said, security researchers have begun to develop techniques to unmask the identities of the persons behind transactions by analyzing the patterns of activity in the block chain, and law enforcement has begun to adopt such techniques.[8]

Challenges

This last benefit of Bitcoin is also the key challenge that it poses to regulators. One person's censorship-resistance is another's money laundering. To date the U.S.

[5] World Bank*, Developing Countries to Receive Over $410 Billion in Remittances in 2013, Says World Bank*, Oct. 2, 2013, *available at* http://www.worldbank.org/en/news/press-release/2013/10/02/developing-countries-remittances-2013-world-bank

[6] *Id*.

[7] Adam Ludwin, How Anonymous is Bitcoin? A Backgrounder for Policymakers, Coin Center, Jan. 20, 2015, *available at* https://coincenter.org/2015/01/anonymous-bitcoin/

[8] Jason Weinstein, How Can Law Enforcement Leverage the Blockchain in Investigations? A Backgrounder for Policymakers, Coin Center, May 12, 2015, *available at* https://coincenter.org/2015/05/how-can-law-enforcement-leverage-the-blockchain-in-investigations/

government has reacted to Bitcoin even-handedly, seeking to address its potential misuse while preserving its potential benefits for society and the economy.

The Treasury Department's Financial Crimes Enforcement Network (FinCEN) has found that companies in the business of transmitting value over the Bitcoin network, or exchanging dollars for Bitcoins, must register as money transmitters and comply with Bank Secrecy Act regulations, including requirements to identify customers and file suspicious activity reports.[9] Federal law enforcement has also targeted illegal transactions that employ Bitcoin. The FBI shut down Silk Road, an encrypted website that has facilitated the sale of drugs and other illicit goods, and has targeted other such marketplaces. The SEC has shuttered ponzi schemes in which victims are asked to invest using bitcoins, and the FTC has taken on fraud in the bitcoin mining hardware industry.

While Bitcoin no doubt presents some new challenges to law enforcement, the message from the government has been that it is well positioned to adapt. As Edward Lowery, a special agent with the Secret Service noted at the first Senate hearing on virtual currencies that, "High level international cybercriminals have not by-and-large gravitated to the peer-to-peer cryptocurrency, such as bitcoin."[10] At the same hearing, FinCEN director Jennifer Shasky Calvery said that "Cash is probably still the best medium for laundering money."[11] This was reiterated by David S. Cohen, Treasury's undersecretary for terrorism and financial intelligence, in a speech when he said, "Terrorists generally need 'real' currency, not virtual currency, to pay their expenses -– such as salaries, bribes, weapons, travel, and safe houses. The same is true for those seeking to evade sanctions."[12]

Like email or the web, Bitcoin is an open Internet protocol. This means that anyone can plug into the network and easily transact with anyone else in the world. This creates new opportunities for people who previously did not have access to financial markets, and it also opens up a new world of beneficial permissionless innovation. It also means, however, that criminals can use the open network for illicit purposes–just as criminals use email today. We obviously do not criminalize email, however, because we recognize that its benefits outweigh its risks, and the same is true for cryptocurrencies like Bitcoin.

[9] US Department of the Treasury, Financial Crimes and Enforcement Network, "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies" (Guidance FIN-2013-G001, March 18, 2013), *available at* http://fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html.

[10] Katherine Mangu-Ward, Are Bitcoins Making Money Laundering Easier? Bitcoins are sexy, but cash is still king, *Slate*, Feb. 5, 2014, at http://www.slate.com/articles/technology/future_tense/2014/02/bitcoin_money_laundering_allegations_cash_is_still_king.html

[11] *Id.*

[12] US Department of Treasury, Remarks From Under Secretary of Terrorism and Financial Intelligence David S. Cohen on "Addressing the Illicit Finance Risks of Virtual Currency," March 18, 2014, *available at* https://www.treasury.gov/press-center/press-releases/Pages/jl236.aspx

Consumer protection is another area where regulators are currently focusing their attention. States have begun to look at how digital currencies, such as Bitcoin, and the businesses that utilize them to provide consumer products and services, interact with money transmission and consumer protection policy. Texas and Kansas, for example, have published guidance explaining that third-party bitcoin exchanges *do* engage in money transmission and therefore must be licensed as money transmitters with state authorities. New York, by contrast, has decided to place digital currency businesses under a separate regulatory regime from traditional money transfer and has crafted a so-called, "BitLicense."

In its policy statement on state virtual currency regulation, the Conference of State Bank Supervisors has clearly set out the normative case for consumer protection regulation of digital currencies:

> [M]any virtual currency services are clearly focused on consumer financial services. Such virtual currency service providers are in a position of trust with the consumer, which creates a public interest to ensure activities are performed as advertised with appropriate minimum standards to minimize risk to consumers.
>
> It is CSBS policy that entities performing activities involving third party control of virtual currency should be subject to state licensure and supervision like an entity performing such activities with fiat currencies.[13]

Cryptocurrency presents a challenge to regulators because it can be utilized to perform activities involving third party control—activities that have long been performed with fiat currencies—yet unlike prior electronic financial tools, cryptocurrency can also be used for other unrelated purposes. It can be used by businesses to offer a financial service without having control of the customer's funds; it can be used by intermediaries to offer a non-financial service (such as a notary service); and it can be used by consumers directly and entirely without intermediaries.

Undoubtedly, some consumers will ask an intermediary to store and transmit their digital currency, and these intermediaries thereby assume a position of trust, which generates the basis for licensing and regulation. The key to developing such licensing and regulation, however, is to include those trusted intermediaries within a regulatory scheme while excluding others who do not assume that trust or do not offer financial services.

Intermediaries who do not assume a position of trust, non-financial uses, and individual access are digital currency innovations that should be encouraged. "Trustless" intermediaries can benefit both consumers and businesses through improved financial privacy, financial inclusion, and vibrant technology-based economies. These uses should not be burdened by compliance costs that lack concomitant consumer protection benefits.

[13] Conference of State Bank Supervisors, *State Regulatory Requirements for Vitrutal Currency Activities CSBS Model Regulatory Framework* 10, (Sep. 2015) *available at* https://www.csbs.org/regulatory/ep/Documents/CSBS-Model-Regulatory-Framework(September%2015%202015).pdf

Finally, some wonder whether cryptocurrencies like Bitcoin could have an impact on monetary policy. That seems unlikely, at least in the foreseeable future.

For Bitcoin to have any monetary effect it would have to become the widely used unit of account. This means that prices of goods, contracts, and loans would have to be denominated in Bitcoins rather than dollars. But as economist William Luther has shown, short of monetary catastrophe or government support, it's virtually impossible for a cryptocurrency to overcome the dollar's network effects, especially given the vast switching costs inherent in such a transition.[14]

Where Bitcoin may have monetary consequences is in countries like Argentina or Venezuela where capital controls have been a key part of the monetary policy. Many in those countries would like to escape the local currency to U.S. dollars, Swiss Francs, or gold, yet it is difficult to do so. Escaping to Bitcoin may be easier because of its censorship-resistance.

Conclusion

Bitcoin is only seven years old and it is still an experiment, but one that if successful will fundamentally change how we transact electronically. Like the Internet itself, Bitcoin has the potential to be a platform for the kind permissionless innovation that has driven so much of the growth of our economy. In fact, Bitcoin looks today very much like the Internet did in 1995. Some dismissed the Internet then as a curiosity, but many could see that such an open platform for innovation would allow for world-changing applications to be built on top of it. Few in 1995 could have foreseen Facebook or Skype or Netflix, but they could see that all the building blocks were there for some amazing innovations. Bitcoin is like that today. We cannot yet conceive what will be the killer applications of cryptocurrency, but it is plain that they will come.

Bitcoin faces some challenges, however, and chief among them is regulatory uncertainty. If we think back again to the early Internet, it was not until the government made it clear that it would pursue a light-touch regulatory approach that Internet innovation really took off. Bitcoin today is in need of a similar commitment from government.

If Coin Center could offer two guiding principles for you to use when considering policy related to Bitcoin they would be *clarity* and *innovation*. Clarity in terms of how existing regulations would apply to this new technology—rules of the road for innovators seeking to operate this space. And to always measure new policies against their impact on continued innovation. Like all emerging technologies, cryptocurrency also presents risks. The challenge governments face is to address those risks while doing no harm to the innovative potential of the technology.

[14] William J. Luther, "Cryptocurrencies, Network Effects, and Switching Costs," *Contemporary Economic Policy*, Oct. 16, 2015, *available at* http://onlinelibrary.wiley.com/doi/10.1111/coep.12151/abstract

If you need any further assistance as you consider cryptocurrencies, please do not hesitate to contact us at Coin Center. Our mission is to build a better understanding of these technologies and to promote a regulatory climate that preserves the freedom to innovate using blockchain technologies. We do this by producing and publishing policy research from respected academics and experts, by educating policymakers and the media about blockchain technology, and where appropriate advocacy for policies at the state and federal level consistent with our mission.

For your reference, included below is a list of some of Coin Center's plain-language backgrounders that you may wish to reference. More information is available on our website at CoinCenter.org. Also, attached to this letter is a copy of "Bitcoin: A Primer for Policymakers" that I hope will help you learn more about this technology.

Is Bitcoin Regulated? by Jerry Brito, Jan 13, 2015.
Coin Center Executive Director Jerry Brito debunks the common misconception about Bitcoin that it is not regulated. http://coincenter.org/2015/01/bitcoin-regulated/

How Anonymous is Bitcoin? by Adam Ludwin, Jan 20, 2015.
Adam Ludwin, Co-Founder of Chain.com, differentiates between anonymity and privacy in financial tools. http://coincenter.org/2015/01/anonymous-bitcoin/

How Are Payments with Bitcoin Different than Credit Cards? by Richard Gendal Brown, Jan 1, 2015.
Richard Gendal Brown compares paying with Bitcoin and paying with a credit card. http://coincenter.org/2015/01/payment-security/

What is Multi-Sig, and What Can It Do? by Ben Davenport, Jan 1, 2015.
Ben Davenport, co-founder at BitGo, simplifies the technical details of multi-signature transactions. http://coincenter.org/2015/01/multi-sig/

What is Bitcoin Mining, and Why is it Necessary? by Peter Van Valkenburgh, Dec 15, 2014.
Peter Van Valkenburgh, Coin Center's Director of Research, offers a plain English explanation of Bitcoin mining. http://coincenter.org/2014/12/bitcoin-mining/

What are Smart Contracts, and What Can We do with Them? by Houman Shadab, Dec 15, 2014.
New York Law School Professor and Coin Center Fellow Houman Shadab shares how block chains can make contracts "smart." http://coincenter.org/2014/12/smart-contracts/

How can Bitcoin be Used for Remittances? by Brock Cusick, Dec 2, 2014.
Attorney Brock Cusick describes the promise Bitcoin holds for sending money to one's home country. http://coincenter.org/2014/12/remittances/

Is Bitcoin's Price Volatility a Problem for the Technology? by Gil Luria, Dec 2, 2014.
Wedbush's Gil Luria shows why Bitcoin's notorious price volatility is not a surprise, nor a dilemma. http://coincenter.org/2014/12/volatility/

Are Consumer Bitcoin Balances Especially Vulnerable to Hacking? by Mike Belshe, Dec 1, 2014.
Mike Belshe, co-founder at BitGo, explains the risks facing consumers who hold Bitcoin. http://coincenter.org/2014/12/consumer-safety/

What are Colored Coins? by Brock Cusick, Nov 30, 2014.
Attorney Brock Cusick explains why a Bitcoin could be "colored" and potential applications of such coins. http://coincenter.org/2014/11/colored-coins/