2018

Does Bitcoin Need Regulation?: An Analysis of Bitcoin's Decentralized Nature as a Security and Regulatory Concern for Governments

Hadeka Rasul

Seton Hall University, hadekarasul@gmail.com

Follow this and additional works at: https://scholarship.shu.edu/pa

Part of the Political Science Commons

Does Bitcoin Need Regulation?: An Analysis of Bitcoin's Decentralized Nature as a Security and Regulatory Concern for Governments

Hadeka Rasul

Hadeka Rasul is a recent graduate of Seton Hall University, where she studied Political Science and Economics. She is currently a Business Analyst at Birchbox. As a part of Pi Sigma Alpha, she serves on the executive board of the chapter and is an executive editor for the Political Science journal. She expects to attend graduate school to attain an MBA in the future.

INTRODUCTION

Envision a global currency, accepted in every country on the face of the Earth, a currency accepted not only in the physical world, but also in the virtual world. That currency is Bitcoin. Bitcoin is the first decentralized digital currency,[1] meaning that it is not tied to any state authority and can be used for virtually any transaction anywhere. If a currency is centralized, it has a common place of deposit, such as the U.S. Federal Reserve, and a common administrator, like that of the currency of most countries. If it is decentralized, it does not have one central location of repository and it does not have a single party to administer it.[2] In addition, it is a virtual currency, so it exists only on the Internet – in the cloud, on hard drives, and in "virtual wallets." This allows one to perform transactions anywhere and at any time with no intermediary. Instead, "it depends on a basic system of trust between users."[3]

With the growth of Internet, the world has progressed massively into the virtual world. One can essentially live an entire virtual life and the addition of a virtual currency aides this phenomenon. It allows us to create more possibilities through computing mechanisms – something that would not have been possible when the Internet first came to be. Through these developments over time, we have been able to change the way we live – information has become more accessible, communication has changed drastically, but the way the Internet has influenced financial transactions has been significantly less disruptive – until Bitcoin's emergence.

This paper aims to look at Bitcoin's application of block-chain technology and the security and regulatory issues that stem from its decentralized nature. Many scholars are of the opinion that Bitcoin is inherently anti-regulation and many of its advantages are due to this attribute. Others believe that Bitcoin's decentralization presents risk within the use of the currency itself, as well as concerns regarding untraceable criminal activity. As Bitcoin gains more traction, it is essential that it is better understood. As a crypto-currency, it can be easily misinterpreted due to its mystifying nature. However, Bitcoin and other digital currencies may very well become prevalent in our day-to-day lives in the near future, and it is important that we take notice of their disruptive nature, as well as the societal and political effects of their applications.

---

[1] Daniela Sonderegger, "A Regulatory and Economic Perplexity: Bitcoin Needs Just a Bit of Regulation," *Washington University Journal Of Law & Policy* 47, (2015): 176, accessed November 28, 2017, LexisNexis Academic: Law Reviews.

[2] Mitchell Franklin, "A PROFILE OF BITCOIN CURRENCY: AN EXPLORATORY STUDY," *International Journal Of Business & Economics Perspectives* 11, no. 1 (2016): 80, accessed November 28, 2017, Complementary Index (1931907X).

[3] Ibid.

BACKGROUND
What is blockchain?

Blockchain is the transformative technology that underlies Bitcoin, so it is important to understand what it is and how it works. Blockchain is essentially a method of sharing and recording data, transactions, or any other digital assets in a distributed, peer-to-peer setting.[4] Blockchain uses cryptography and mathematics to create a database that is open and decentralized. Any transaction of any value can be recorded on this database. The blockchain decentralizes and distributes information by storing information across the internet network on a number of personal computers. There is no central power that owns the system, has the ability to change it or to take it down.

Any individual can participate in a blockchain and perform transactions without requiring any sort of review by an intermediary or central authority. The data is kept in a ledger that is maintained by each of the participants involved in the blockchain network. In order for any entry to be considered valid, it must be represented identically across all ledgers on the distributed network. Multiple parties must review and agree upon any transaction in order for it to be recorded in the blockchain. Once there is a consensus, the transaction is added to the ledger and it cannot be reversed. The technology uses cryptography in order to make sure that records cannot be changed or counterfeited. Therefore, security and validity of a blockchain ledger is guaranteed.

Blockchain allows transactions or contracts to be transparent, yet encrypted. Instead of allowing an intermediary to be in charge of important transactions or documents, it ensures that all transactions are essentially free of human failure. With blockchain, there is no need for a chain of intermediaries to send money across borders and pay fees for those services, and the risk of human error throughout these steps is removed. There is no need for a third party to log transactions between people – there is visibility on the blockchain which shows all parties that the transaction has occurred and allows them to verify its validity. The simplest way to describe blockchain technology is "a shift from trusting people to trusting math."[5] Although Bitcoin is one application of blockchain, cryptocurrency is not all that blockchain technology is utilized for. As Lou Carlozo writes, "Everything from property deeds, to birth records, to money such as bitcoin and various alt-coins resides on a blockchain backbone."[6] Blockchain can be used for storing important records of many different types. The underlying concept of blockchain ensures the integrity of any transactions on the ledger and uses a peer-to-peer model in order to establish this. A peer-to-peer system is one where computers are connected to each other through the Internet, and files can be shared directly between the computers on the network without the need of a central server.[7] Such a system is peer-to-peer, computer-to-computer, rather than through a central server or intermediary. In addition to the use of a peer-to-peer system, each block that the blockchain is extended by contains a time-stamp, the hash value of the previous block, and a nonce, which is an identifier or "number only used once," added to each block.[8] This enables verification of the entire chain of blocks. Since no block can be mutated once added to the chain, each hash value should correspond to its previous block. One can verify

---

[4] Molly Suda, Ben Tejblum, and Andrew Francisco, "Chain Reactions: Legislative and Regulatory Initiatives Related to Blockchain in the United States: An overview and critique of existing approaches," *Computer Law Review International* 18, no. 4 (2017): 97, accessed November 28, 2017, Complementary Index (16107608).

[5] Andreas M. Antonopoulos, "Bitcoin security model: Trust by computation," *Medium*, February 2014, accessed November 28, 2017. https://medium.com/@aantonop/bitcoin-security-model-trust-by-computation-d5b93a37da6e.

[6] Lou Carlozo, "What is blockchain?," *Journal Of Accountancy* 224, no. 1 (2017): 2, accessed November 28, 2017, Business Source Elite (0021-8448).

[7] "P2P," *TechTerms*, https://techterms.com/definition/p2p.

[8] Michael Nofer, et al., "Blockchain," *Business & Information Systems Engineering* 59, no. 3 (2017): 184, accessed November 28, 2017, Complementary Index (18670202).

the chain entirely to its first block through this way. It ensures integrity, which is central to blockchain's transformative capabilities, especially in the financial industry.

What is Bitcoin?

Bitcoin is an electronic currency, introduced in 2008 by someone using the pseudonym "Satoshi Nakamoto." Nakamoto released a paper, titled, "Bitcoin: A Peer-to-Peer Electronic Cash System," detailing a peer-to-peer electronic payment system that would allow payments to be sent directly from one party to another without going through any financial institution.[9] In this paper, Nakamoto insisted that an electronic payment system based on cryptographic proof instead of trust was necessary. This system would allow any willing parties to transact directly with each other without the need for a trusted third party. In addition, the currency would not be backed by any asset and without specie, such as coin or precious metal.[10] It is backed by the transparency and mathematical certainty of its transactions, rather than by any asset or the credit of any nation's government.[11] This means that the system is based on an algorithm which is self-regulating, transparent, and participants are able to view the ledger of transactions and verify them. These characteristics make it decentralized and remove the necessity of regulation by any central authority, such as a bank or government.

In many ways, this cryptocurrency and Satoshi Nakamoto's paper were a response to the financial crisis of 2008. Placing trust into the hands of intermediaries, such as bankers, would be unnecessary in the case of Bitcoin. As the financial crisis had revealed corruption in the financial system, Bitcoin provided a new hope. At its fullest potential, digital currencies have the power to make financial institutions relatively obsolete.

With blockchain and Bitcoin, people no longer have to place trust in the hands of other people, but rather in the blockchain itself and mathematics that underlie it. Bitcoin's unofficial slogan, "In cryptography we trust," is a statement about this transition of trust, which has shifted from the third party intermediaries that failed people during the crisis to the technology that makes financial exchanges simpler than ever.[12]

---

[9] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," Bitcoin, October 2008, accessed November 28, 2017, https://bitcoin.org/bitcoin.pdf.

[10] SEC v. Shavers, No. 4:13-CV-416, (E.D. Texas, Aug 6, 2013).

[11] Scott R. Bowling, "Understanding Bitcoin--Its Developing Regulatory Framework and Its Risks in Distressed Situations," *Journal Of Taxation &*

Regulation Of Financial Institutions 29, no. 1 (2015): 34, accessed November 28, 2017, Complementary Index (15473996).

[12] Morgen E. Peck, "Blockchains: How they work and why they'll change the world," *IEEE Spectrum* 54, no. 10 (2017): 26, accessed November 28, 2017, Complementary Index (00189235).
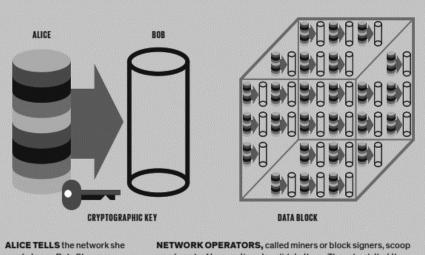
Miners & Signers

EVERY BLOCKCHAIN needs a way to determine who will add the next block of data. Two strategies prevail: proof of work and proof of stake. Both randomly assign the right to add new blocks. But proof of work gives preference to those with more computing power. And proof of stake—of which there are many versions, some wildly complex—gives preference to those with more coins.

ALICE

BOB

CRYPTOGRAPHIC KEY

DATA BLOCK

ALICE TELLS the network she wants to pay Bob. She uses a cryptographic key to digitally sign off on the transaction, proving that she owns those coins.

NETWORK OPERATORS, called miners or block signers, scoop up a bunch of transactions to validate them. They check that the digital signatures are correct and that there are enough coins for the requested transactions. Then they put those transactions into a new data block to be added to the blockchain.

Bitcoin is not a blockchain itself, but involves the usage of the blockchain.[13] Bitcoin transactions take place over an open, public, anonymous network, which is an application of the blockchain technology. Each coin transaction occurs over a public ledger and is digitally signed with the hash of the previous transaction and the public key of the next owner of the coin.[14] This allows any payee to be able to verify a chain of transactions in order to validate ownership. Every single Bitcoin has a blockchain, with a history of time-stamped transactions recording where it moved from one public key to another.[15] Since all transactions occur over a peer-to peer network, there is no need for a trusted third party.

(*Source*: Morgene Peck, "Blockchains: How They Work & Why They'll Change the World," *IEEE Spectrum* 54, no. 10 (2017): 31, Illustration by Greg Mably)

How does a Bitcoin transaction work?

A transaction between two parties in bitcoin requires three pieces of information – an input, an output, and an amount.[16] The input is the Bitcoin address of the sender's bitcoins. The output is the Bitcoin address of the party receiving the bitcoins. The amount is the amount of bitcoins being transferred. A Bitcoin address is a random sequence of letters and numbers that is used to direct payments to and from your virtual wallet, where your bitcoins are stored. In addition to an address, each party has a pair of cryptographic keys, comprised of their private key and public key. The private key is also a sequence of letters and numbers but it is not visible by anyone. It is used to sign transactions when you send bitcoins to someone else. For example, when Alice wants to send bitcoins to Bob, she signs the transaction with her private key, the input (address) of the coins, the amount, and the output (Bob's Bitcoin address). The bitcoin message then enters the

---

[13] Sean McLeod, "Bitcoin: The Utopia or Nightmare of Regulation," *Elon Law Review* 9, no. 2 (2017): 555, accessed November 28, 2017, HeinOnline (2154-0063).

[14] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," Bitcoin, October 2008, accessed November 28, 2017, https://bitcoin.org/bitcoin.pdf.

[15] Derek A. Dion, "I'LL GLADLY TRADE YOU TWO BITS ON TUESDAY FOR A BYTE TODAY: BITCOIN,

REGULATING FRAUD IN THE E-CONOMY OF HACKER-CASH," *University Of Illinois Journal Of Law, Technology & Policy* (2013): 168, accessed November 28, 2017, LexisNexis Academic: Law Reviews.

[16] Coindesk, "How do Bitcoin Transactions Work?" 2015. Accessed December 8, 2017. https://www.coindesk.com/information/how-do-bitcoin-transactions-work.

wider network of Bitcoin, where miners verify the transaction before it is added as a block to the blockchain and received by Bob.[17]

The Bitcoin Mining & Verification Process

Since Bitcoin is designed to work as a digital currency, its' supply and circulation is central to its value. As of now, there are almost 17 million Bitcoin in circulation.[18] The maximum amount of Bitcoin ever in existence will be 21 million. The process through which Bitcoin are brought into circulation is called "mining." Mining consists of the identification, review, and verification of transactions conducted in bitcoins by computers, called miners.[19] Miners solve a computational problem that allows them to chain together verified blocks of transactions into the blockchain and they are rewarded with newly created Bitcoins in the process. This process is best explained as follows:

When a transaction takes place in bitcoin, it is automatically made available for review by miners. As miners confirm transactions, those transactions are logged in a public register called the blockchain. As subsequent transactions are verified in the blockchain, the level of certainty that earlier transactions have occurred increases, reaching near-certainty at around 60 minutes. The incentive for people to devote their computing resources to bitcoin mining is that miners are rewarded by receiving bitcoins in exchange for their services. More efficient miners receive more bitcoins. The crux of the Bitcoin system is mining. [20]

Essentially, mining is the reason that there is no need for a third-party intermediary in Bitcoin. Miners confirm all transactions and this internal system ensures a level of certainty. The system

labels and protects each block with a unique hash value, which is generated based on the information on the block and an integer key.[21] Generating a hash is considered relatively easy, but reverse engineering a key from a hash is cryptographically difficult. It requires immense computing power and is only discovered through trial and error. Therefore, the hash-generating process is crowdsourced through miners who invest a large amount of computational power.[22] Through this mining process, new Bitcoins are introduced as a reward for the miner's contribution.

How is the Bitcoin system different from previous virtual currency systems?

Bitcoin comprises 58% of the cryptocurrency market.[23] About $4.9 billion worth of bitcoins are traded every day, with about 12,000 transactions per hour and 99,000 bitcoins sent per hour. There are 18.5 million Blockchain.info wallets and 500,000 Bitcoin.com wallets.[24] In one word, Bitcoin is *popular*. It is used in more transactions than any other cryptocurrency and has gained a higher price as a result. Recognizing that it has captured the attention of so many, it is important to also consider what it has brought to the table that other currencies did not.

Xin Li and Chong Alex Wang state in their paper, "The technology and economic determinants of cryptocurrency exchange rates: The case of Bitcoin," that the two basic promises of any currency system are: (1) users should be guaranteed to receive authentic currency that can be spent in future transactions, and (2) each unit of the currency can only be spent once by the owner, i.e., no double-spending.[25] Double spending is the risk associated with the easy

---

[17] Ibid.

[18] Blockchain.info, https://blockchain.info/charts/total-bitcoins?timespan=all

[19] Scott R. Bowling, "Understanding Bitcoin--Its Developing Regulatory Framework and Its Risks in Distressed Situations," *Journal of Taxation & Regulation of Financial Institutions* 29, no. 1 (2015): 34, accessed November 28, 2017, Complementary Index (15473996).

[20] Ibid.

[21] Xin Li and Chong Alex Wang, "The technology and economic determinants of cryptocurrency exchange

rates: The case of Bitcoin," *Decision Support Systems* 95 (2017): 50, accessed November 28, 2017, ScienceDirect (0167-9236).

[22] Ibid.

[23] Kai Sedgwick, "Bitcoin by Numbers: 21 Statistics That Reveal Growing Demand for the Cryptocurrency," Bitcoin.com. 2017. Accessed December 7, 2017. https://news.bitcoin.com/bitcoin-numbers-21-statistics-reveal-growing-demand-cryptocurrency.

[24] Ibid.

[25] Ibid.

reproduction of digital currencies, making it possible for them to be spent twice. It is difficult to ascertain whether a sum of digital money was copied by the holder and sent to another party, while the original was kept by the holder. Since it is not tangible, one can technically send the same money twice. Due to this, the need for an intermediary emerges. In order for virtual transactions to be efficient, there needs to be a third party verifying and recording all transactions. With Bitcoin, the use of a distributed peer-to-peer timestamp server proposes a solution to the problem of double-spending.[26] For example:

Imagine there are no intermediaries with ledgers, and digital cash is simply a computer file, just as digital documents are computer files. Alice could send $100 to Bob by attaching a money file to a message. But just as with email, sending an attachment does not remove it from one's computer. Alice would retain a copy of the money file after she had sent it. She could then easily send the same $100 to Charlie.[27]

This is the double-spending problem in simple terms. However, Bitcoin has been able to eliminate this problem. Every transaction made is time-stamped and cannot be modified, effectively notarizing the transaction and preventing any Bitcoin amount from being double-spent.[28] If anything, it has increased the trust in regards to financial transactions more than an intermediary

could. It solves the double-spending problem without an intermediary – using cryptographic, computational proof of the chronological order of transactions.[29] Bitcoin's use of blockchain technology creates a large, distributed public ledger of validated transactions, with a unique hash for each block.[30] It verifies the authenticity of each transaction and prevents this double-spending problem that was inhibiting the growth of such virtual currency systems.

USES OF BITCOIN & ITS IMPLICATIONS

Bitcoin is a digital currency and therefore, its primary use is as a medium of exchange. As with any form of "money," it can be used for many different purposes. This does not make Bitcoin, or any other type of currency, inherently good or bad. Bitcoin has many advantages and is undoubtedly revolutionary, but its emergence has raised concerns as well. In particular, its use for criminal activity distresses many and creates a demand for regulation to some extent.

Bitcoin was designed to reduce the transaction costs that are associated with third parties validating transactions and mediating disputes.[31] As Sean McLeod states, "Bitcoin provides a unique benefit for its users: the technology can be used to send money to all areas of the globe for a fraction of the cost compared to other money transfer systems such as Western Union and MoneyGram."[32] This aspect of Bitcoin is undisputed; Bitcoin undeniably creates ease and

[26] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," Bitcoin, October 2008, accessed November 28, 2017, https://bitcoin.org/bitcoin.pdf.
[27] Jerry Brito and Andrea Castillo, "BITCOIN: A PRIMER FOR POLICYMAKERS," *Policy* 29, no. 4 (2014): 3, accessed November 28, 2017, Academic Search Complete (1032-6634).
[28] Derek A. Dion, "I'LL GLADLY TRADE YOU TWO BITS ON TUESDAY FOR A BYTE TODAY: BITCOIN, REGULATING FRAUD IN THE E-CONOMY OF HACKER-CASH," University Of Illinois Journal Of Law, Technology & Policy (2013): 168, accessed November 28, 2017, LexisNexis Academic: Law Reviews.
[29] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," Bitcoin, October 2008,

accessed November 28, 2017, https://bitcoin.org/bitcoin.pdf.
[30] Xin Li and Chong Alex Wang, "The technology and economic determinants of cryptocurrency exchange rates: The case of Bitcoin," Decision Support Systems 95 (2017): 50, accessed November 28, 2017, ScienceDirect (0167-9236).
[31] Derek A. Dion, "I'LL GLADLY TRADE YOU TWO BITS ON TUESDAY FOR A BYTE TODAY: BITCOIN, REGULATING FRAUD IN THE E-CONOMY OF HACKER-CASH," University Of Illinois Journal Of Law, Technology & Policy (2013): 167, accessed November 28, 2017, LexisNexis Academic: Law Reviews.
[32] Sean McLeod, "Bitcoin: The Utopia or Nightmare of Regulation," Elon Law Review 9, no. 2 (2017): 565-566, accessed November 28, 2017, HeinOnline (2154-0063).

simplicity in the area of money transfer. The mining fee that is associated with these transfers is much less than the charges one would normally pay for Western Union or MoneyGram transfers. In addition to the savings in cost, the transfer takes place within minutes, another convenient aspect. Marc Andreessen also emphasizes Bitcoin's power to bring about a great reduction in transaction costs. He writes:

Every day, hundreds of millions of low-income people go to work in hard jobs in foreign countries to make money to send back to their families in their home countries – over $400 billion in total annually, according to the World Bank. Every day, banks and payment companies extract mind-boggling fees, up to 10 percent and sometimes even higher, to send this money.

Switching to Bitcoin, which charges no or very low fees, for these remittance payments will therefore raise the quality of life of migrant workers and their families significantly. In fact, it is hard to think of any one thing that would have a faster and more positive effect on so many people in the world's poorest countries.[33]

Bitcoin can have an effect on the lives of migrant workers worldwide. In fact, many migrant workers have embraced this system and use it to send money back to their home countries. This is true for Africa especially, where a service called BitPesa allows one to transfer bitcoins to Kenyan shillings and Ghanaian cedi for a flat fee of 3 percent, compared to the average 12.3 percent fee paid to other money transmitters. As a result of the savings, BitPesa's user base is growing by 60 percent each month.[34] Using a mobile payment system on a basic cell phone, that is available to most in Kenya, called M-Pesa, Kenyans are able to pay school fees, buy groceries, and make other purchases by converting their bitcoins into the M-Pesa system. Indonesian migrant workers, who work in Saudi Arabia, Malaysia or on cruise ships, also send home bitcoins. Prior to this, many would save weeks' worth of wages to buy a gram of gold to send back home and then their families would liquidate the gram of gold to get Indonesian rupiah. Since bitcoins are infinitely divisible (which I discuss in the next paragraph), it is much simpler to send home a small amount of a bitcoin in such cases. The lack of regulation is not especially a concern in regards to money transfers of this sort. Bitcoin's processes and the peer-to-peer approach ensure the structure and longevity of the entire record system and effectively transfer wealth. McLeod even states that should there be a major banking crisis or a raise in banking fees, Bitcoin is an attractive route.[35]

Another appealing feature of Bitcoin is its "infinite divisibility."[36] This allows micropayments, which have never been feasible prior since it has always been inefficient to run such small amounts through the existing banking systems. With Bitcoin, "you can specify an arbitrarily small amount of money, like a thousandth of a penny, and send it to anyone in the world for free or near-free."[37] This creates new possibilities in content monetization – it creates a way to charge for an article rather than the whole newspaper, or per section, per hour, per video play, per archive access, or per news alert.

Bitcoin's ability to be divided into such relatively small amounts can also help fight online spam. This is an especially interesting application of the technology. As email is currently free, spammers are able to send billions of emails for no

---

[33] Marc Andreessen, "Why Bitcoin Matters," *The New York Times*, January 21, 2014, accessed November 28, 2017, https://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters/

[34] Hazel Sheffield, "Bitcoin is being used by African migrant workers to send money home," Independent, 2015. Accessed December 7, 2017. http://www.independent.co.uk/news/business/news/bitcoin-is-being-used-by-african-migrant-workers-to-send-money-home-10098169.html.

[35] Sean McLeod, "Bitcoin: The Utopia or Nightmare of Regulation," Elon Law Review 9, no. 2 (2017): 567, accessed November 28, 2017, HeinOnline (2154-0063).

[36] Marc Andreessen, "Why Bitcoin Matters," The New York Times, January 21, 2014, accessed November 28, 2017, https://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters/

[37] Ibid.

charge at all. If future email systems and social networks stopped accepting messages without tiny amounts of Bitcoin – "tiny enough to not matter to the send, but large enough to deter spammers" – then it is likely that we will see a reduction in the amount of spam messages we currently receive.[38]

Bitcoin began as a currency for computer geeks or those who viewed U.S. monetary policy as "unconstitutional."[39] However, it quickly became something more – it has become increasingly the preferred method of payment for those involved in the online drug market, casinos, criminal hacker groups, terrorist activity, weapons, and child abuse content.[40] This is due to the fact that Bitcoin offers a level of anonymity to its users. While the ledger of transactions is public, it is not easy to trace any specific transaction to its owner. Effectively, it is public but anonymous. As stated by Grinberg, "all Bitcoin transactions are public, but are considered anonymous because nothing ties individuals or organizations to the accounts that are identified in the transactions."[41] This creates possibilities and potential for criminals to cover the tracks of their ill-gotten gains.[42]

One of the illegal uses of Bitcoin is money laundering. Since Bitcoin cannot be traced back to any original individual or source, it is very useful for money laundering practices. For example, a tech-savvy drug dealer could convert his cash into Bitcoins and then disperse them among a multitude of wallets. Then, as the criminal needed cash, he could reconvert the Bitcoins into U.S.

dollars. Since the wallets are public but contain no information on the user, it could be quite a challenge for investigators to sort out the criminal's pattern for laundering cash.[43]

There was no similar regulatory legislation in place to prevent money laundering through Bitcoin, as there is for financial institutions. Bitcoin exchanges do not normally concern themselves with the activities taking place with bitcoins, and their users were also not protected in the case of a threat or bankruptcy. As Bitcoin is not under the jurisdiction of any government, governments are unable to protect users. However, due to pressure from government bodies to create a safety net, Bitcoin exchanges have opened their doors to regulation. Recognizing that regulated exchanges pose benefits to both users and governments, they are embracing it despite the fact that there are Bitcoin users who do not fundamentally believe in regulation of the system. Exchanges have begun to offer aid by reporting any suspicious transactions, as well as complying with money-laundering statutes, mandated by the FBI.[44][45]

In addition to money laundering, Bitcoin can also make it easy to purchase illicit goods or support illegitimate groups. As stated, Bitcoin is anonymous so it cannot be tracked to any individual. If any illegal activity is somehow traced, it cannot be frozen for seizure since no government or regulatory authority has power over Bitcoin transactions. Individuals can

[38] Ibid.

[39] Derek A. Dion, "I'LL GLADLY TRADE YOU TWO BITS ON TUESDAY FOR A BYTE TODAY: BITCOIN, REGULATING FRAUD IN THE E-CONOMY OF HACKER-CASH," University Of Illinois Journal Of Law, Technology & Policy (2013): 169, accessed November 28, 2017, LexisNexis Academic: Law Reviews.

[40] Ibid.

[41] Reuben Gringberg, "Bitcoin: An Innovative Alternative Digital Currency," *Hastings Science and Technology Law Journal* 4 (2011): 179.

[42] Derek A. Dion, "I'LL GLADLY TRADE YOU TWO BITS ON TUESDAY FOR A BYTE TODAY: BITCOIN, REGULATING FRAUD IN THE E-CONOMY OF HACKER-CASH," University Of Illinois Journal Of Law, Technology & Policy (2013): 186, accessed

November 28, 2017, LexisNexis Academic: Law Reviews.

[43] Ibid.

[44] Brett Wolf, "Bitcoin exchanges offer anti-money-laundering aid," *REUTERS*, June 15, 2011, accessed November 28, 2017, https://www.reuters.com/article/financial-bitcoin/bitcoin-exchanges-offer-anti-money-laundering-aid-idUSN1510930920110615.

[45] Federal Bureau of Investigation, Directorate of Intelligence, "Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity," *WIRED*, April 24, 2012, accessed November 28, 2017, https://www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf

anonymously contribute to criminal and terrorist organizations using bitcoins and their actions are virtually untraceable and unstoppable.

In fact, Bitcoin's early adoption was mostly for these types of transactions. With the establishment of the "Silk Road" in January 2011, Bitcoin had a spike in popularity. Silk Road was an online marketplace, mostly used for the trading of illicit drugs, which relied on Tor and Bitcoin to maintain the anonymity of buyers and sellers.[46] Silk Road was not accessible by any normal URL, but only through The Onion Router (TOR) anonymity network. TOR operates by bouncing web requests though an encrypted network of servers all over the world and making it impossible to connect traffic to any specific user.[47] Therefore, users were able to shop for illegal substances on Silk Road using Bitcoin in complete anonymity. However, the FBI was able to find the administrators of the online marketplace and took down Silk Road twice, in October 2013 and after it reemerged as "Silk Road 2.0" in November 2013.

Since this was the main use of Bitcoin in its early stages, it immediately painted an image of Bitcoin as a dark-net market currency – one whose primary use was to facilitate illegal activities, such as money laundering, financing terrorism, and dealing in illegal drugs. Hence, it becomes understandable that governments took a special interest in the features that were allowing Bitcoin users to remain anonymous and untraceable. As Irwin et al. found in their study, due to high levels of anonymity, low levels of detection, and ease to

transact, such illicit activities can easily take place in the virtual environment.[48]

This aspect of Bitcoin has raised concerns for law enforcement and government authorities. In a leaked 2012 Intelligence Assessment, FBI analysts concluded that a key advantage of Bitcoin for criminals is that "law enforcement faces difficulties detecting suspicious activity, identifying users, and obtaining transaction records."[49] Another report by the European Central Bank states that the lack of regulation and due diligence may enable "criminals, terrorists, fraudsters, and money laundering" and that "the extent to which any money flows can be traces back to a particular user is unknown."[50] Bitcoin has been instrumental in hiding illicit transactions, through money laundering and Silk Road activities, for example. This has undoubtedly presented issues in regulating such activity.

LITERATURE REVIEW

The use of blockchain by Bitcoin erases the need for central authorities, such as central banks of governments or intermediary banking.[51] The structure of Bitcoin regulates transactions through the peer-to-peer system. Therefore, a centralized system is no longer necessary – the task of regulation is decentralized and distributed amongst the users who take part in the system. Every transaction is specifically validated, which is central to Bitcoin's trust structure. Specifically, the currency is not dependent on any state; it is built on code and lives in the cloud. It is separate from the nation state and is inherently resistant to

---

[46] Primavera De Filippi and Benjamin Loveluck, "The invisible politics of Bitcoin: governance crisis of a decentralised infrastructure," *Internet Policy Review* 5, no. 3 (2016): 6, accessed November 28, 2017, Directory of Open Access Journals (2197-6775).

[47] Henrik Karlstrøm, "Do libertarians dream of electric coins? The material embeddedness of Bitcoin," *Distinktion: Scandinavian Journal Of Social Theory* 15, no. 1 (2014): 32, accessed November 28, 2017, Political Science Complete (1600-910X).

[48] Angela S.M. Irwin et al., "Money laundering and terrorism financing in virtual environments: a feasibility study," *Journal of Money Laundering Control* 17, no. 1 (2014): 72.

[49] Federal Bureau of Investigation, Directorate of Intelligence, "Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity," WIRED, April 24, 2012, accessed November 28, 2017, https://www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf

[50] European Central Bank, "Virtual Currency Schemes," *ECB*, October 2012, accessed November 28, 2017, https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf.

[51] Peter Yeoh, "Regulatory issues in blockchain technology," *Journal Of Financial Regulation & Compliance* 25, no. 2 (2017): 196, accessed November 28, 2017, Complementary Index (13581988).

government control.[52] This creates discussion of the risks that may be associated with having a decentralized currency system. While many praise this characteristic of the virtual currency system, others believe that there are regulatory and legal gaps that can prove harmful to individuals involved. In the following section, I look at both sides of this discussion in order to assess what the literature on Bitcoin says regarding its regulation.

On one hand, there are those who argue that Bitcoin should see little to no regulation by government. Daniela Sonderegger writes in her article, "A Regulatory and Economic Perplexity," that Bitcoin is unnerving because it creates "a world where the ability of a central bank to guide the economy is destroyed, by design."[53] She discusses the fact that part of the goal of Bitcoin, and similar digital cryptocurrencies, is "to take down global banking or to wage a war against the Federal Reserve," as stated by Elizabeth Ploshay, a writer for Bitcoin Magazine.[54] Undoubtedly, advocates of an unregulated Bitcoin system have political motive to separate the government from its monetary role. There is a mistrust of existing financial institutions and the state's capabilities of properly conducting monetary policy. This makes Bitcoin's system attractive, as it leaves such actions and trustworthiness to computational and mathematical powers – not people. Sonderegger also argues that Bitcoin exists solely on the Internet. It is not a physical entity or asset pertaining to any specific government. Therefore, effective regulation can only exist through worldwide cooperation, which would be incredibly complicated, in addition to costly.

When the Bitcoin system was developed by Satoshi Nakamoto, it stemmed out of distrust for central authorities. It was created to be sufficient on its own. The "proof of work system" and the blockchain are specifically designed to make it self-regulating and independent of any

sort of intervention. Therefore, according to Sonderegger, it is unlikely that a government will be successful in implementing regulation.[55] However, regardless of what the intent of the system was, it is important to consider whether the self-regulating capabilities of Bitcoin have been sufficient on their own and whether the uses which concern governments now (as a criminal haven of sorts) makes outside intervention necessary.

Another perspective is offered in "Bitcoin: A Primer for Policymakers" by Jerry Brito and Andrea Castillo. Brito and Castillo extensively review the parameters of Bitcoin and its functions and conclude that, "it is important that policymakers allow this experimentation to continue," advocating for innovation.[56] The first aspect they discuss is the anonymity feature of Bitcoin transactions. They argue that it is actually "pseudonymity," not anonymity. This is due to the fact that transactions to and from a particular Bitcoin address, or public key, can actually be traced to some extent – unlike cash where there is no such historical record. This creates a pseudonym for the identity of the person – they cannot be identified but their transactions can still be traced on the blockchain.

Brito and Castillo go on to argue that it is not that difficult for government or other authorities to tie a real-world identity to a pseudonymous Bitcoin address. It can be traced through an IP address, or through Bitcoin exchanges. In order to achieve complete anonymity, it requires a bit more effort. Those users who would have to use Tor software, as well as be cautious not to transact with any Bitcoin address that could be traced back to any identity.[57] In addition to this, as of December 1, 2016, the FBI has the power to hack into multiple computers anywhere in the world, as granted by the changes to Rule 41 by the Supreme Court. Rule 41 allows any United States judge to issue search warrants for the FBI and law

---

[52] Daniela Sonderegger, "A Regulatory and Economic Perplexity: Bitcoin Needs Just a Bit of Regulation," *Washington University Journal Of Law & Policy* 47, (2015): 175, accessed November 28, 2017, LexisNexis Academic: Law Reviews.
[53] Ibid.
[54] Ibid: 176.

[55] Ibid: 203.
[56] Jerry Brito and Andrea Castillo, "BITCOIN: A PRIMER FOR POLICYMAKERS," Policy 29, no. 4 (2014): 11, accessed November 28, 2017, Academic Search Complete (1032-6634).
[57] Ibid: 5

enforcement agencies to remotely hack computers.[58] This decision was made with anonymity networks such as Tor in mind. It is an attempt to make it easier to investigate cyber criminals that are "concealed through technological means."[59] For Bitcoin users, this means that the FBI can spy on them all over the world if they are using Tor software to anonymize their locations and identities.[60]

In addition to this, a study done by Elli Androulaki, et al, revealed that behavior-based clustering techniques could reveal 40% of Bitcoin users in their simulated experiment.[61] Although Bitcoin users do still experience a higher level of privacy than users of traditional digital-transfer services, it is still relatively difficult to stay completely anonymous, according to Brito and Castillo.

Further, they briefly review the benefits of the technology as a "new payments system." As we know, it reduces transaction costs by removing the third-party intermediary. Due to this, it "holds much promise as a way to lower transaction costs for small businesses and global remittances, alleviate global poverty by improving access to capital, protect individuals against capital controls and censorship, ensure financial privacy for oppressed groups, and spur innovation."[62] Clearly, Bitcoin has a great amount of potential and the ability to impact many different areas. However, in order for the Bitcoin system to be able to impact the world in this way, it is essential to diminish the opportunities for criminality while still maintaining the advantages it brings.

The three main concerns Brito and Castillo discuss are price volatility, security breaches, and criminal uses of Bitcoin. In terms of price volatility, they speculate that Bitcoin's value fluctuates resembling traditional bubbles – as overoptimistic media coverage encourages new investors, the value increases but eventually plummets. The volatility aspect is not as significant if Bitcoin is used as a medium of exchange and not as a store of value. This explains why it has grown more popular among merchants despite its price volatility.[63]

The second concern is the security challenges. For one, bitcoins are stored digitally, primarily in virtual wallets. If the digital file is lost or the hard-drive malfunctions, the money is lost. In addition, it is susceptible to hacking – if you do not protect your private Bitcoin address, it can be left open to theft and if you do not encrypt your wallet, the bitcoins can be stolen through malware.[64] Bitcoin exchanges have also been victims of attack – hackers successfully stole 24,000 BTC from an exchange known as Bitfloor in 2012.[65]

Lastly, Brito and Castillo discuss the criminal uses of Bitcoin. This entails the use of Tor and Bitcoin to purchase illicit goods on the black market site, Silk Road, as well as money laundering to finance terrorism and illegal trafficking. As mentioned previously, Bitcoin offers pseudonymity and this allows people to take part in such activity while remaining unidentifiable to an extent. However, they point out that this is not a new issue – it is the same as traditional cash. They state, "Cash has historically been the vehicle of choice for drug traffickers and money

---

[58] Swati Khandelwal, "Rule 41 – FBI Gets Expanded Power to Hack any Computer in the World," The Hacker News. 2016. Accessed December 8, 2017. https://thehackernews.com/2016/11/fbi-rule-41-hacking.html.

[59] Ibid.

[60] JP Buntinx, "FBI Can Obtain A Warrant If You Run Tor Come December," The Merkle. 2016. Accessed December 8, 2017. https://themerkle.com/fbi-can-obtain-a-warrant-if-you-run-tor-come-december.

[61] Elli Androulaki et al., "Evaluating User Privacy in Bitcoin," *Financial Cryptography & Data Security* (2013): 34-51, Complementary Index (9783642398834).

[62] Jerry Brito and Andrea Castillo, "BITCOIN: A PRIMER FOR POLICYMAKERS," Policy 29, no. 4 (2014): 6, accessed November 28, 2017, Academic Search Complete (1032-6634).

[63] Ibid: 9.

[64] Stephen Doherty, "All your Bitcoins are ours…," *Symantec Official Blog*, June 16, 2011, accessed November 28, 2017, https://www.symantec.com/connect/blogs/all-your-bitcoins-are-ours.

[65] Jerry Brito and Andrea Castillo, "BITCOIN: A PRIMER FOR POLICYMAKERS," Policy 29, no. 4 (2014): 9, accessed November 28, 2017, Academic Search Complete (1032-6634).

launderers, but policymakers would never seriously consider banning cash."[66]

In conclusion, it is important that regulators are "wary of the perils of overregulation," when it comes to Bitcoin. Regulators could easily prevent businesses from benefitting from Bitcoin while not doing anything effective to prevent the criminal use. If Bitcoin becomes a complicated means of transferring currency, it can make it unattractive for its regular users. As of now, its benefits as a currency and payment transfer system are evident, but the risks it presents in terms of criminality tend to overshadow those benefits. This relationship is expected, as it is certainly crucial to address such concerns before they become uncontrollable. As such, Brito and Castillo argue that, "the challenge for policymakers and regulators is to develop a system that addresses concerns about money laundering and illicit purchases, without smothering the benefits that Bitcoin is poised to provide to legitimate users in their everyday lives."[67] What is important is that regulation is calculated and purposeful, in order to prevent criminal use without bringing an end to the benefits of the system as well.

On a similar note, Hendrickson et al. write in "The Political Economy of Bitcoin," that Bitcoin has several features that offer advantages to its users but also provide grounds for government action to discourage or prevent Bitcoin use.[68] As previously discussed, Bitcoin enables people to complete illegal transactions, which is something that a government has already committed to prohibit. Therefore, it would be appropriate for governments to intervene in the processes that allow criminal activity to take place in the Bitcoin system. In addition, the inherent nature and technology of Bitcoin precludes a government from accomplishing tasks assigned to it, such as conducting monetary policy or raising revenues. As Bitcoin gains more traction, governments are compelled to assess their role regarding the cryptocurrency.

As part of Bitcoin's makeup, users are unidentifiable in regards to their actual identities. They are only identifiable through their virtual addresses, which do not necessarily have to be linked to any identifying information. In addition to this, the system operates without regard to national borders. Anyone can send money to anyone anywhere. You do not have to disclose or report any transactions – therefore, many users have been able to circumvent existing regulatory framework.[69] This prevents a great challenge to governments. With a traditional financial account, they have the power to freeze any account that they believe may be engaged in illegal activities. In addition to that, they can easily identify the account holder. However, with Bitcoin, the government is unable to freeze, reverse, or identify anyone in relation to any suspicious activity.[70] If the government is unable to perform such actions in relation to an account perceived as a threat, the illegal activity (such as criminal or terrorist activity) can continue to receive funding in Bitcoin, and continue to cause harm.

The second challenge that governments face is that Bitcoin impedes it from conducting monetary policy goals or raising revenues.[71] With a traditional currency, such as the US Dollar, the Federal Reserve is able to control the money supply in circulation. However, with Bitcoin, supply of bitcoin is regulated through an algorithm. This algorithm is built into the system and cannot be modified by any sort of central authority.

At its fullest potential, if individuals move towards Bitcoin and away from traditional currency, the central banks will become obsolete in terms of their control over money supply. Although this is not a concern as of now, it could be one in the future if Bitcoin use continues to

---

[66] Jerry Brito and Andrea Castillo, "BITCOIN: A PRIMER FOR POLICYMAKERS," Policy 29, no. 4 (2014): 10, accessed November 28, 2017, Academic Search Complete (1032-6634).
[67] Ibid.
[68] Joshua R. Hendrickson, Thomas L. Hogan, and William J. Luther, "THE POLITICAL ECONOMY OF

BITCOIN," *Economic Inquiry* 54, no. 2 (2016): 927, accessed November 28, 2017, Academic Search Complete (0095-2583).
[69] Ibid.
[70] Ibid: 928.
[71] Ibid: 929.

grow. Bitcoin may have an effect on federal budgets, because it can reduce a government's ability to raise revenues from seigniorage. Seigniorage is the difference between the value of money and the cost to produce it. Governments make economic profit through positive seigniorage when they expand the money supply. For example, it does not cost the U.S. government $100 to produce a $100 bill. According to the Federal Reserve, it only costs 15.5 cents per $100 note.[72] Therefore, the economic profit, known as seigniorage, gained is $99.845 – the difference between the two amounts.

With Bitcoin, the miners are the ones essentially conducting monetary policy, as they are the ones who increase the supply of Bitcoin. As articulated in the beginning of this paper, miners are awarded with new Bitcoin for using their computational power. It also gradually becomes more and more difficult to mine new Bitcoin, since there will only ever be about 21 million, which is very different from the way governments expand the money supply. The only "seigniorage" income in Bitcoin is the bitcoins that the miners receive, but the cost to mine or produce them is not as low as it is to produce paper currency. Therefore, if Bitcoin were to become a mainstream currency, this would undoubtedly be a concern for governments who risk losing out on seigniorage income. However, as of now, it does not seem to be a pressing concern, but has the potential to become one as Bitcoin usage increases.

Although many recognize the benefits of the blockchain technology that Bitcoin uses, there are those who claim that without proper regulation, the technology poses plenty of risks.[73] In the case of having no intermediary regulating transactions, Kavita Jain, who is the director of Emerging Regulatory Issues at the Financial Industry Regulatory Authority, stated,

The point about disintermediation is a little overhyped by people who are enthusiastic about the potential of this technology. Sure, people don't want to pay [a fee]. But some prefer to pay knowing that there is a body that is going to look after their interests as opposed to interacting with someone on the network they don't know.[74]

There is a two-part counter-argument to this statement. One, the reason Bitcoin does not rely on an intermediary is because it relies on something relatively more powerful – cryptography and mathematical processes that are able to "look after interests." Bitcoin was developed as a response to the financial crisis – the financial crisis that was brought on arguably due to risky behavior by intermediaries. Cutting out those middlemen effectively reduces that specific risk, as well as the fees associated with transacting through a financial institution.

Secondly, going hand in hand with the first point, trusting an intermediary does not mean that there will not be issues. As Teddy Cho points out, "you are going to have those issues and mistakes today and you will have them in a slightly different form if they are written up in blockchain." However, by putting agreements "into code and block, you could do away with some of the clucky legal agreements we have had to deal with in the last couple of decades."[75] In other words, blockchain application simplifies financial transactions and the lack of intermediaries does not necessarily increase risk in the process.

One of the legal and regulatory concerns regarding Bitcoin deals with a gap in legal framework to address situations of distress, specifically bankruptcy of Bitcoin exchanges. Scott R. Bowling writes about this in his paper, "Understanding Bitcoin – Its Developing Regulatory Framework and Its Risks in Distressed

---

[72] Board of Governors of the Federal Reserve System, "How much does it cost to produce currency and coin?" The Federal Reserve. 2017. Accessed December 10, 2017. https://www.federalreserve.gov/faqs/currency_12771.htm.

[73] Frank Devlin, "BLOCKCHAIN: REVOLUTION, REGULATION, AND THE WAY FORWARD," *RMA Journal* 100, no. 1 (2017): 48, accessed November 28, 2017, Business Source Elite (1531-0558).
[74] Ibid.
[75] Ibid.

Situations. "[76] The challenge here is that Bitcoin is not considered money, a security, a commodity, or a derivative and due to this, there is no clear guidance on how the Bankruptcy Code would apply to Bitcoin exchange operations.[77]

Bowling references the case of Mt. Gox, which was a Tokyo-based exchange that lost millions of its own and its customer's bitcoins.[78] Under the Bankruptcy code, a company is eligible for chapter 11 relief if it has assets in the United States and is a railroad, is eligible for chapter 7 relief (unless it is a stockbroker or commodity broker), or an uninsured State member bank or insurance company.

The first piece of this criterion implies that a company must have assets in the United States. This brings forth an interesting argument – where do bitcoins exist? Bowling states that Bitcoin generally exists only on the internet, so it is not clear how they would constitute as assets in the United States for purposes of bankruptcy eligibility.[79] Due to this, it may be difficult for a company to establish that the exchange has assets in the United States.

Furthermore, Bowling's analysis finds that most types of bitcoin exchanges do not seem to constitute as stockbrokers or banks under the Bankruptcy Code, but some may constitute as commodity brokers.[80] Therefore, it may not be eligible for chapter 11 relief. In summation, because Bitcoin is still in its early stages, there does not seem to be proper legislation in terms of Bankruptcy Code. This means that anyone who is entering this market should be aware that there are substantial risks involved.

According to The CPA Journal, the SEC, the Financial Crimes Enforcement Network (FinCEN), and the IRS have all issued some form of regulation regarding digital currencies in the past few years.[81] Janet Yellen, the chair of The Federal Reserve, commented that the Fed does not have the ability to supervise or regulate Bitcoin given that there is no intersection between Bitcoin and banks.[82] In early 2015, the IRS issued a notice about Bitcoin for tax purposes. This notice stated that payments made with bitcoins, Bitcoin investments, and income derived from mining would be treated as property.[83] This ruling is contradictory, according to Rick Barlin, as it states that virtual currencies can be treated like real currencies in certain circumstances.

Bitcoins received as payment to an employee would be considered wages; payment to an independent contractor would be subject to self-employment tax. If a bitcoin is bought on an exchange and then used to buy a product, the sale is treated like a barter transaction, and the gain or loss is the difference in basis between the value of the product received and the value of the bitcoin at that time.

… Unlike with taxes, where an asset must be sold before it is recognized, the receipt of a bitcoin or other virtual currency must be recorded. Furthermore, because bitcoins are treated like real currency, their exchange rate at the balance sheet date must be considered and adjusting entries must be made to reflect conversion to U.S. dollars.[84]

FinCEN's Virtual Currency Guidance, which was issued on March 18, 2013, clarified the

---

[76] Scott R. Bowling, "Understanding Bitcoin--Its Developing Regulatory Framework and Its Risks in Distressed Situations," *Journal Of Taxation & Regulation Of Financial Institutions* 29, no. 1 (2015): 33-43, accessed November 28, 2017, Complementary Index (15473996).

[77] Ibid: 38.

[78] Ibid: 35.

[79] Ibid: 42.

[80] Ibid.

[81] Rick Barlin, "Regulation on the Rise as Bitcoin Gains Popularity," *CPA Journal* (2017): 10-11, accessed November 28, 2017, Business Source Elite (0732-8435).

[82] Vivian A. Maese, "Divining the Regulatory Future of Illegitimate Cryptocurrencies," *Wall Street Lawyer* 18, no. 5 (2014): 8.

[83] Daniela Sonderegger, "A Regulatory and Economic Perplexity: Bitcoin Needs Just a Bit of Regulation," *Washington University Journal Of Law & Policy* 47, (2015): 200, accessed November 28, 2017, LexisNexis Academic: Law Reviews.

[84] Rick Barlin, "Regulation on the Rise as Bitcoin Gains Popularity," CPA Journal (2017): 11, accessed November 28, 2017, Business Source Elite (0732-8435).

application of the Bank Secrecy Act, regarding Money Services Businesses regulations, to "persons creating, obtaining, distributing, exchanging, accepting, or transmitting virtual currencies."[85] The guidance uses the terms "user," "exchanger," and "administrator" to differentiate between different types of participants in virtual currency arrangements.

A *user* is a person that obtains virtual currency to purchase goods or services.[7] An *exchanger* is a person engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency. An *administrator* is a person engaged as a business in issuing (putting into circulation) a virtual currency, and who has the authority to redeem (to withdraw from circulation) such virtual currency.[86]

Under these regulations, a user of a virtual currency is not a Money Services Business, and therefore is not subject to the registration, reporting, and recordkeeping regulations. However, a money transmitter, which would fall under an administrator or exchanger, is considered a Money Services Business. The regulation subjects Bitcoin administrators and exchanges to increased costs of compliance associated with money transmitting regulations, which is cause for concern.[87] In addition, Bitcoin exchangers are subject to federal and state licensing requirements – which means that they must register with all states requiring licensing since Bitcoin does not function in any specific

state, but on the Internet, making it accessible in every state.[88]

This guidance also declared that, "virtual currency does not have legal tender in any jurisdiction."[89] "Real" currency is the "the coin and paper money of the United States or of any other country that is [i] designed as legal tender and that [ii] circulates and [iii] is customarily used and accepted as a medium of exchange in the country of issuance."[90] "Virtual" currency is a medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency and does not have legal tender status in any jurisdiction.[91] This means that companies must convert the Bitcoin into legal tender, such as what Overstock.com does. However, this can lead to major reporting issues for bookkeeping and tax purposes.[92]

The Central Bank of Finland released a research paper titled, "Monopoly without a Monopolist: An Economic Analysis of the Bitcoin Payment System," on September 5, 2017. The paper was written by three researchers from Columbia Business School – Gur Huberman, Jacob D. Leshno, and Ciamac Moallemi. It asserts that Bitcoin may be more comparable to cash than to a modern electronic payment system. They argue that Bitcoin does not need regulation. When comparing Bitcoin to a monopoly run by managing organizations, the paper argues that Bitcoin is not run by a managing organization, but rather a protocol – "Bitcoin is a monopoly run by a

---

[85] Department of the Treasury - Financial Crimes Enforcement Network, "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies," FinCEN, March 18, 2013, accessed November 28, 2017, https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering.

[86] Ibid.

[87] Daniela Sonderegger, "A Regulatory and Economic Perplexity: Bitcoin Needs Just a Bit of Regulation," *Washington University Journal Of Law & Policy* 47, (2015): 188, accessed November 28, 2017, LexisNexis Academic: Law Reviews.

[88] Marco Santori, "Bitcoin Law: Money transmission on the state level in the US," *CoinDesk*, September 28,

2013, accessed November 28, 2017, http://www.coindesk.com/bitcoin-law-money-transmission-state-level-us.

[89] Department of the Treasury - Financial Crimes Enforcement Network, "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies," FinCEN, March 18, 2013, accessed November 28, 2017, https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering.

[90] Ibid.

[91] Ibid.

[92] Rick Barlin, "Regulation on the Rise as Bitcoin Gains Popularity," CPA Journal (2017): 11, accessed November 28, 2017, Business Source Elite (0732-8435).

protocol."[93] It is not controlled by any single person or group, but by a computer algorithm. In the case of a traditional monopolistic setting, regulation is often imposed in order to prevent or mitigate abuse of power – which is not a concern within the dynamics of Bitcoin. Huberman et al. state, "Bitcoin is not regulated. It cannot be regulated. There is no need to regulate it because as a system it is committed to the protocol as is and the transaction fees it charges the users are determined by the users independently of the miners' efforts."[94] A pivotal part of this paper is where the authors state that "Bitcoin's design as an economic system is revolutionary." This is vital recognition that the system needs from governmental bodies, as it is often undermined when viewed from a regulatory perspective. With the practical issues of criminality and security as a concern, regulators can often fail to appreciate the potential and usefulness that blockchain and Bitcoin technology provides.

FURTHER CONVERSATION

The conversation around Bitcoin and regulation is only worthwhile if Bitcoin or its technological innovation is here to stay. Many believe it is revolutionary, but there are others who do not think it will last. After releasing the whitepaper introducing Bitcoin to the world, Satoshi Nakamoto sent an email explaining the thought-process behind it. He stated, "The root problem with conventional currency is all the trust that is required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust… With e-currency based on cryptographic proof, without the need to trust a third-party

middleman, money can be secure and transactions complete."[95]

However, Kevin Dowd and Martin Hutchinson, argue in their paper, "Bitcoin Will Bite the Dust," that Bitcoin was designed not to require trust, but now depends on it. Because of this, it is living on borrowed time.[96] They regard Bitcoin as "an instructive creative failure," one that will fail but will guide and lead to superior private currencies in the future, crypto and otherwise.[97] Post Bitcoin's introduction to the world, there has been over 35 cryptocurrencies introduced. From Ethereum to Litecoin, they all bring forth something new to add to the system and this innovation does not seem to be coming to a halt anytime soon. As such currency systems gain more and more popularity, there will always be others working on the next Bitcoin – a better version that aims to solve the issues and compensate for what Bitcoin may lack. All in all, Bitcoin brings forth the possibilities that are available in the virtual currency world but fails to demonstrate that it is immune to failure.

François Velde of the Federal Bank of Chicago states that, "it is hard to imagine a world where the main currency is based on an extremely complex code understood by only a few and controlled by even fewer, without accountability, arbitration, or recourse."[98] He writes that people are so invested in Bitcoin because it may develop into a full-fledged currency. But as of now, it has been used mostly as a means to transfer funds outside of traditional and regulated channels or as a speculative investment opportunity. Velde writes that if Bitcoin "becomes widely accepted, it is unlikely that it will remain free of government intervention, if only because the governance of the bitcoin code and network is opaque and

[93] Gur Huberman, Jacob D. Leshno, and Ciamac Moallemi, "Monopoly without a monopolist: An economic analysis of the bitcoin payment system," *Bank of Finland Research Discussion Papers* 27, (2017): 36.
[94] Ibid.
[95] Satoshi Nakamoto to P2P foundation, "Bitcoin open source implementation of P2P currency," February 11, 2009, accessed November 29, 2017,

http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source.
[96] Martin Hutchinson and Kevin Dowd, "BITCOIN WILL BITE THE DUST," *CATO Journal* 35, no. 2 (2015): 378, accessed November 29, 2017, Business Source Elite (0273-3072).
[97] Ibid: 380.
[98] François R. Velde, "Bitcoin: A primer," *Chicago Fed Letter* no. 317 (2013): 3, accessed November 29, 2017, Business Source Elite (0895-0164).

vulnerable."[99] Similar to Dowd and Hutchinson, he recognizes that the system is a remarkable technical achievement that may be useful in other ways to financial institutions or even governments.

CONCLUDING THOUGHTS

Within the discussion of Bitcoin and regulation, there is also a larger conversation regarding governance of the Internet and virtual world overall. An overwhelming consensus is that regulation is detrimental to innovation. As Adam Scholl of the World Policy Blog writes,

This year alone, scientists validated the Standard Model of physics, quantum teleported information 90 miles, sent messages using neutrinos, built a quantum computer inside a diamond, piloted driverless cars across an entire continent, and declared their intent to 3D print robot dinosaurs. In the private sector, Google executives Larry Page and Eric Schmidt teamed up with Ross Perot Jr., James Cameron, and others to announce plans to lasso asteroids in space, mine them on the moon using robots, and send trillions in profit back to Earth… Technological innovation, needless to say, is accelerating.[100]

This statement, which is from 2012, speaks volumes about the possibilities that technology brings. In 2017, it is even more amplified. We are progressing towards a world where anything is possible, and blockchain and Bitcoin are steps towards that virtual future.

However, it would be unwise to overlook the security and regulatory concerns that may come along with some of these innovations. While security and innovation both hold ample significance in society, a balance and cooperation must be sought between the two. Blockchain has been an attempt to do this – it creates its own regulatory processes that effectively diminish the need for a regulatory body. However, blockchain has not alleviated all concerns. Through this paper and the research presented, it is evident that with the application of blockchain to Bitcoin, there are still some issues that must be addressed. Its self-

regulation is only sufficient to an extent. There are still concerns, such as its use in criminal and terrorist activity. The system itself does not seem to be able to address such issues – it does not prevent such activity, (in fact, it arguably promotes it) nor does it make it easier for law enforcement to step in. Therefore, there is a need for some sort of regulation in this area. The virtual world is complex and as society shifts more in that direction, it is essential that consensus over such issues is reached. With Bitcoin, the conversation is still ongoing – and in many ways, it is only the beginning.

REFERENCES

Andreessen, Marc. "Why Bitcoin Matters." *The New York Times.* January 21, 2014. Accessed November 28, 2017. https://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters/

Androulaki, Elli et al. "Evaluating User Privacy in Bitcoin." Financial Cryptography & Data Security (2013): 34-51. Complementary Index (9783642398834).

Antonopoulos, Andreas M. "Bitcoin security model: Trust by computation." *Medium.* February 2014. Accessed November 28, 2017. https://medium.com/@aantonop/bitcoin-security-model-trust-by-computation-d5b93a37da6e.

Barlin, Rick. "Regulation on the Rise as Bitcoin Gains Popularity." *CPA Journal* (2017): 10-11. Accessed November 28, 2017. Business Source Elite (0732-8435).

Brito, Jerry and Andrea Castillo. "BITCOIN: A PRIMER FOR POLICYMAKERS." Policy 29, no. 4 (2014): 3-12. Accessed November 28, 2017. Academic Search Complete (1032-6634).

Board of Governors of the Federal Reserve System. "How much does it cost to produce currency and coin?" The Federal Reserve. 2017. Accessed December 10, 2017.

---

[99] Ibid: 4.

[100] Adam Scholl, "The Problem with Internet Regulation," *World Policy Blog*, September 25, 2012,

accessed November 29, 2017, http://www.worldpolicy.org/blog/2012/09/25/problem-internet-regulation.

https://www.federalreserve.gov/faqs/currency_12771.htm.

Bowling, Scott R. "Understanding Bitcoin--Its Developing Regulatory Framework and Its Risks in Distressed Situations." *Journal Of Taxation & Regulation Of Financial Institutions* 29, no. 1 (2015): 33-43. Accessed November 28, 2017. Complementary Index (15473996).

Buntinx, JP. "FBI Can Obtain A Warrant If You Run Tor Come December." The Merkle. 2016. Accessed December 8, 2017. https://themerkle.com/fbi-can-obtain-a-warrant-if-you-run-tor-come-december.

Carlozo, Lou. "What is blockchain?." *Journal Of Accountancy* 224, no. 1 (2017): 1-2. Accessed November 28, 2017. Business Source Elite (0021-8448).

Coindesk. "How do Bitcoin Transactions Work?" 2015. Accessed December 8, 2017. https://www.coindesk.com/information/how-do-bitcoin-transactions-work.

Department of the Treasury - Financial Crimes Enforcement Network. "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies." *FinCEN*, March 18, 2013. Accessed November 28, 2017. https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering.

Devlin, Frank. "BLOCKCHAIN: REVOLUTION, REGULATION, AND THE WAY FORWARD." *RMA Journal* 100, no. 1 (2017): 48-51. Accessed November 28, 2017. Business Source Elite (1531-0558).

Dion, Derek A. "I'LL GLADLY TRADE YOU TWO BITS ON TUESDAY FOR A BYTE TODAY: BITCOIN, REGULATING FRAUD IN THE E-CONOMY OF HACKER-CASH." *University Of Illinois Journal Of Law, Technology & Policy* (2013): 165-201. Accessed November 28, 2017. LexisNexis Academic: Law Reviews.

Doherty, Stephen. "All your Bitcoins are ours…" Symantec Official Blog, June 16, 2011. Accessed November 28, 2017. https://www.symantec.com/connect/blogs/all-your-bitcoins-are-ours.

European Central Bank. "Virtual Currency Schemes." *ECB*. Oct 2012. Accessed November 28, 2017. https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf.

Federal Bureau of Investigation, Directorate of Intelligence. "Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity." *WIRED*. April 24, 2012. Accessed November 28, 2017. https://www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf

Filippi, Primavera De and Benjamin Loveluck. "The invisible politics of Bitcoin: governance crisis of a decentralised infrastructure." *Internet Policy Review* 5, no. 3 (2016): 1-28. Accessed November 28, 2017. Directory of Open Access Journals (2197-6775).

Franklin, Mitchell. "A PROFILE OF BITCOIN CURRENCY: AN EXPLORATORY STUDY." *International Journal Of Business & Economics Perspectives* 11, no. 1 (2016): 80-92. Accessed November 28, 2017. Complementary Index (1931907X).

Gringberg, Reuben. "Bitcoin: An Innovative Alternative Digital Currency." *Hastings Science and Technology Law Journal* 4 (2011): 159-207.

Hendrickson, Joshua R., Thomas L. Hogan, and William J. Luther. "THE POLITICAL ECONOMY OF BITCOIN." *Economic Inquiry* 54, no. 2 (2016): 925-939. Accessed November 28, 2017. Academic Search Complete (0095-2583).

Huberman, Gur, Jacob D. Leshno, and Ciamac Moallemi. "Monopoly without a monopolist: An economic analysis of the bitcoin payment system." *Bank of Finland Research Discussion Papers* 27, (2017): 1-56.

Hutchinson, Martin and Kevin Dowd. "BITCOIN WILL BITE THE DUST." *CATO Journal* 35, no. 2 (2015): 357-382. Accessed November 29, 2017. Business Source Elite (0273-3072).

Irwin, Angela S.M. et al. "Money laundering and terrorism financing in virtual environments: a feasibility study." *Journal of Money Laundering Control* 17, no. 1 (2014): 50-75.

Karlstrøm, Henrik. "Do libertarians dream of electric coins? The material embeddedness of

Bitcoin." *Distinktion: Scandinavian Journal Of Social Theory* 15, no. 1 (2014): 23-36. Accessed November 28, 2017. Political Science Complete (1600-910X).

Khandelwal, Swati. "Rule 41 – FBI Gets Expanded Power to Hack any Computer in the World." The Hacker News. 2016. Accessed December 8, 2017. https://thehackernews.com/2016/11/fbi-rule-41-hacking.html.

Li, Xin and Chong Alex Wang. "The technology and economic determinants of cryptocurrency exchange rates: The case of Bitcoin." *Decision Support Systems* 95 (2017): 49-60. Accessed November 28, 2017. ScienceDirect (0167-9236).

Maese, Vivian A. "Divining the Regulatory Future of Illegitimate Cryptocurrencies." *Wall Street Lawyer* 18, no. 5 (2014): 7-10.

McLeod, Sean. "Bitcoin: The Utopia or Nightmare of Regulation." *Elon Law Review* 9, no. 2 (2017): 553-578. Accessed November 28, 2017. HeinOnline (2154-0063).

Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System." Bitcoin. October 2008. Accessed November 28, 2017, https://bitcoin.org/bitcoin.pdf.

Nofer, Michael, et al. "Blockchain." *Business and Information Systems Engineering* 59, no. 3 (2017): 183-187. Accessed November 28, 2017. Complementary Index (18670202).

Peck, Morgen. "Blockchains: How they work and why they'll change the world." *IEEE Spectrum* 54, no. 10 (2017): 26-35. Accessed November 28, 2017. Complementary Index (00189235).

Santori, Marco. "Bitcoin Law: Money transmission on the state level in the US." *CoinDesk*, September 28, 2013. Accessed November 28, 2017. http://www.coindesk.com/bitcoin-law-money-transmission-state-level-us.

Scholl, Adam. "The Problem with Internet Regulation." *World Policy Blog*. September 25, 2012. Accessed November 29, 2017. http://www.worldpolicy.org/blog/2012/09/25/problem-internet-regulation.

Sedgwick, Kai. "Bitcoin by Numbers: 21 Statistics That Reveal Growing Demand for the Cryptocurrency." Bitcoin.com. 2017. Accessed December 7, 2017. https://news.bitcoin.com/bitcoin-numbers-21-statistics-reveal-growing-demand-cryptocurrency.

Sheffield, Hazel. "Bitcoin is being used by African migrant workers to send money home." Independent. 2015. Accessed December 7, 2017. http://www.independent.co.uk/news/business/news/bitcoin-is-being-used-by-african-migrant-workers-to-send-money-home-10098169.html.

Sonderegger, Daniela. "A Regulatory and Economic Perplexity: Bitcoin Needs Just a Bit of Regulation." *Washington University Journal Of Law & Policy* 47, (2015): 175-215. Accessed November 28, 2017. Lexis Nexis Academic: Law Reviews.

Suda, Molly, Ben Tejblum, and Andrew Francisco. "Chain Reactions: Legislative and Regulatory Initiatives Related to Blockchain in the United States: An overview and critique of existing approaches." *Computer Law Review International* 18, no. 4 (2017): 97-103. Accessed November 28, 2017. Complementary Index (16107608).

Velde, François R. "Bitcoin: A primer." *Chicago Fed Letter* no. 317 (2013): 1-4. Accessed November 29, 2017. Business Source Elite (0895-0164).

Wolf, Brett. "Bitcoin exchanges offer anti-money-laundering aid." *REUTERS*, June 15, 2011. Accessed November 28, 2017. https://www.reuters.com/article/financial-bitcoin/bitcoin-exchanges-offer-anti-money-laundering-aid-idUSN1510930920110615.

Yeoh, Peter. "Regulatory issues in blockchain technology." *Journal Of Financial Regulation & Compliance* 25, no. 2 (2017): 196. Accessed November 28, 2017. Complementary Index (13581988).