THE BLOCK IS HOT: A SURVEY OF THE STATE OF BITCOIN REGULATION AND SUGGESTIONS FOR THE FUTURE

Misha Tsukerman†

Bitcoin, the famous and sometimes infamous digital currency, has two key uses. First, it can serve as a currency to buy and sell goods and services.[1] Second, as its value has fluctuated dramatically within recent years, many users purchase Bitcoins for speculative purposes.[2] Bitcoin exists wholly as lines of computer code[3] governed by the Bitcoin protocol, the program that dictates the generation and transfer of Bitcoins.[4] Unlike fiat currencies such as the U.S. dollar ("USD"), Japanese yen, or euro, Bitcoin is not backed by the government of any nation or by a physical commodity such as gold.[5] Instead, the value of Bitcoin is based on the trust people put in it and its scarcity.[6] In 2013, the market price of a single Bitcoin ranged from thirteen to 1200 USD.[7] Bitcoin relies on cryptography[8] to validate and govern its production and use, with each transaction recorded on an online public ledger called the "blockchain."[9]

---

† J.D. Candidate, 2016, University of California, Berkeley, School of Law.

1. Matthew Kien-Meng Ly, *Coining Bitcoin's "Legal-Bits": Examining the Regulatory Framework for Bitcoin and Virtual Currencies*, 27 HARV. J.L. & TECH. 587, 591 (2014).

2. CRAIG K. ELWELL ET AL., CONG. RESEARCH SERV., BITCOIN: QUESTIONS, ANSWERS, AND ANALYSIS OF LEGAL ISSUES 1 at 6 (2014).

3. Nikolei M. Kaplanov, *Nerdy Money: Bitcoin, the Private Digital Currency, and the Case Against Its Regulation*, 25 LOY. CONSUMER L. REV 111, 116 (2012).

4. Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, BITCOIN.ORG (Nov. 8 2008), https://bitcoin.org/bitcoin.pdf (Satoshi Nakamoto is not necessarily one person or an actual name. *See infra* note 34.).

5. Kaplanov, *supra* note 3, at 115.

6. *See* Reuben Grinberg, *Bitcoin: An Innovative Alternative Digital Currency*, 4 HASTINGS SCIENCE & TECH. L.J. 159, 168, 175 (2012)(noting that confidence in Bitcoin as a limited resource is integral to the value of Bitcoin).

7. Ly, *supra* note 1 at 591.

8. Cryptography is more generally the "process of writing or reading secret messages or codes." *Cryptography Definition*, MERRIAM-WEBSTER.COM, http://www.merriam-webster.com/dictionary/cryptography (last visited Nov. 26, 2014).

9. Nakamoto, *supra* note 4.

Virtual currencies such as Bitcoin were not viable in the past because of the "double-spending" problem, where an owner of a digital currency file could easily make an exact copy of that file and send it to more than one person.[10] A currency that is non-rivalrous and can be held at the same time by more than one user is valueless.[11] What makes Bitcoin, the most popular virtual currency,[12] rivalrous and scarce is that it can only be transferred within the blockchain.

The blockchain is a privately operated and completely decentralized system, requiring no traditional financial institution or central controlling entity for transactions.[13] The blockchain acts as an online record keeping system that tracks the ownership of specific Bitcoins from their creation (in a process called mining)[14] through every subsequent transaction.[15] The blockchain does not exist in a central location, but rather through a peer-to-peer ("P2P") network[16] composed of all Bitcoin users.[17] Bitcoin "miners" use their computer's processing power to maintain the Bitcoin network, and are rewarded in Bitcoins through the Bitcoin protocol.[18]

10. JERRY BRITO & ANDREA CASTILLO, BITCOIN, A PRIMER FOR POLICYMAKERS 3–4, (Mercatus Center 2013).

11. Josh Fairfield, *BitProperty*, 88 S. CAL. L. REV. at 15 (forthcoming 2015), *available at* http://ssrn.com/abstract=http://ssrn.com/abstract=2504710.

12. *See* CoinMarketCap, *infra* note 59 (showing Bitcoin's market capitalization over seven times higher than the next most popular virtual currency). Bitcoin is also the only virtual currency to have an NCAA football game named after it. In an effort to move the chains of public perception, the Bitcoin payments firm BitPay sponsored the St. Petersburg Bowl between North Carolina State University and the University of Central Florida on December 26, 2014. Formerly the "Beef 'O' Brady Bowl," tickets and merchandise at the "Bitcoin St. Petersburg Bowl" game could be purchased with Bitcoin. *See* Michael J. Casey, *BitPay to Sponsor St. Petersburg Bowl in First Major Bitcoin Sports Deal*, WALL ST. J. (June 18, 2014), http://www.wsj.com/articles/bitpay-to-sponsor-st-petersburg-bowl-in-first-major-bitcoin-sports-deal-1403098202.

13. ELWELL ET AL., *supra* note 2, at 1

14. Discussed *infra* Section I.B.

15. ELWELL ET AL., *supra* note 2, at 3.

16. A P2P network is a "network of personal computers, each of which acts as both client and server, so that each can exchange files . . . with every other computer on the network." *Peer-to-peer Network Definition*, DICTIONARY.COM, http://dictionary.reference.com/browse/peer-to-peer%20network (last visited Nov. 28, 2014). This is different from a client/server network where "one centralized, powerful computer (called the server) is a hub to which many less powerful personal computers . . . (called clients) are connected. The clients run programs and access data that are stored on the server." *Server Network Definition*, DICTIONARY.COM, http://dictionary.reference.com/browse/client/server%20network (last visited Nov. 28, 2014).

17. Fairfield, *supra* note 11, at 18 (the blockchain is a decentralized and distributed list).

18. Nakamoto, *supra* note 4.

Thus, no particular party can be said to "control" the blockchain. Profits realized from mining Bitcoin and transaction fee commissions in Bitcoin remain the key incentives for maintenance of the blockchain.[19]

The promise of the blockchain as a decentralized trustless public ledger extends far beyond simply tracking different Bitcoins. The true technological revolution the blockchain represents is the creation of a system that for the first time allows for scarce, rivalrous digital property.[20] The blockchain is prohibitively difficult to hack and falsify and could be used as a reliable system to track the ownership of real property, such as land deeds or automobiles, drastically lowering search and transaction costs.[21] The blockchain has even been suggested as a system to prevent voter fraud.[22] Yet, for these gains to be fully realized, and for the benefits of the network effect,[23] there must be broader adoption of Bitcoin by the general public. Bitcoin will have to come out of the shadows and be seen and used by the general public for more than speculation and the online purchase of drugs and other contraband.[24]

As Josh Fairfield observes,[25] the blockchain "is not financial, it is not asset-based, it is not insurance, or securities, or any one of a number of uses. . . . [It] is simply a protocol for tracking information about rivalrous digital interests."[26] Thus, this Note posits that the job of regulators is to allow the blockchain to thrive and allow for consumer confidence in its potential to create a safe and reliable system of public records to allow for the safe transfer of real property.

---

19. Fairfield, *supra* note 11, at 19.

20. *See id.* at 5.

21. *See generally* Fairfield, *supra* note 11.

22. *See generally* Matt Odell, *How Bitcoin Could Make Voter Fraud and Stolen Elections Impossible*, ENTREPRENEUR (Nov. 20, 2014), http://www.entrepreneur.com/article/239809.

23. "A product displays positive network effects when more usage of the product by any user increases the product's value for *other* users (and sometimes all users)." Arun Sundarajan, *Network Effects*, @DIGITALARUN, http://oz.stern.nyu.edu/io/network.html (last visited Feb. 10, 2015).

24. *Infra* Section III.A.

25. Professor Fairfield is an internationally recognized law and technology scholar. Professor Fairfield specializes in digital property, electronic contracts, big data privacy, and virtual communities. *See* Biography of Professor Joshua A.T. Fairfield, WASHINGTON AND LEE UNIVERSITY SCHOOL OF LAW, http://law2.wlu.edu/faculty/profiledetail.asp?id=242 (last visited Feb. 25, 2015).

26. Fairfield, *supra* note 11, at 67.

Trust in a currency is essential to its adoption[27] and while Bitcoin can provide many benefits over cash and credit card transactions,[28] virtual currency, like all digital technologies is capable of massive and systemic failure.[29] This current age is one of massive cyber intrusions and hacks.[30] Even the economic collapse in 2008 was partly driven by technological failure.[31] While the Bitcoin protocol's technical features create an inherent level of security,[32] it is, of course, the risks that have not yet been imagined that are the most dangerous. Unlike with cash, an undiscovered vulnerability in the Bitcoin protocol could lead to catastrophic failure of the entire Bitcoin ecosystem. Preventing and mitigating these risks will require smart, flexible, and active regulation. This regulation must be balanced against concerns over stifling innovation. As with the internet, regulators must strike a balance between protecting the public from Bitcoin's bad actors, while allowing people to experiment with, and develop the technology.[33]

This Note first examines the history of Bitcoin and the mechanics of the Bitcoin protocol and the blockchain in Part I. Part II then discusses some of the potential uses of Bitcoin, from its potential as a currency, to the use of the blockchain to track other property interests. Part III examines some of risks associated with Bitcoin, from its use in online

27. *See* Supriya Singh, *Electronic Commerce and the Sociology of Money*, 4 SOCIOLOGICAL RESEARCH ONLINE 3.4 (Feb. 29, 2000), http://www.socresonline.org.uk/4/4/singh.html.

28. *See infra* Part II.

29. *See, e.g.*, Bent Flyvbjerg & Alexander Budzier, *Why Your IT Project May Be Riskier Than You Think*, HARV. BUS. REV. (Sep. 2011), https://hbr.org/2011/09/why-your-it-project-may-be-riskier-than-you-think/ (discussing the frequency with which large IT projects fail on a massive scale); Eric Scigliano, *10 Technology Disasters*, MIT TECH. REV. (June 1, 2002), http://www.technologyreview.com/featuredstory/401465/10-technology-disasters/ (highlighting the factors that consistently cause new technologies to fail).

30. *See, e.g.*, ASSOCIATED PRESS, *Sony Hack Adds to Security Pressure on Companies*, N.Y. TIMES (Dec. 19, 2014), http://www.nytimes.com/aponline/2014/12/19/world/asia/ap-as-sony-hack-company-security.html; Nicole Perlroth, *Target Struck in the Cat-and-Mouse Game of Credit Theft*, N.Y. TIMES (Dec. 19, 2013), http://www.nytimes.com/2013/12/20/technology/target-stolen-shopper-data.html.

31. *See* Kenneth A. Bamberger, *Technologies of Compliance: Risk and Regulation in a Digital Age*, 88 TEX. L. REV. 669, 675 (2009).

32. *See infra* Section I.B.1.

33. *See* Mohit Kaushal & Sheel Tyle, *The Blockchain: What it is and Why it Matters*, BROOKINGS INSTITUTION (January 13, 2015), http://www.brookings.edu/blogs/techtank/posts/2015/01/13-blockchain-innovation-kaushal (noting that regulators recognized the unique nature of internet required light regulation to not stifle innovation).

black markets, the consumer protection risks to users, and Bitcoin's potential as a tax evasion mechanism. Part IV analyzes the current regulatory environment for Bitcoin and Bitcoin's role in criminal litigation. Finally, Part V suggests policy changes to disclosure requirements and tax classifications to facilitate the broader adoption of Bitcoin as a currency by the general public.

I. THE BASICS OF BITCOIN AND THE BLOCKCHAIN

This Section will describe what Bitcoins are, how the blockchain solves the double-spending problem, the security features inherent in the Bitcoin protocol, Bitcoin mining, and the blockchain as a public ledger.

A. BITCOIN BASICS

Satoshi Nakamoto, a pseudonym of a computer programmer or group of programmers,[34] proposed Bitcoin in a 2008 white paper as an open source, peer-to-peer, digital currency.[35] Bitcoins are computer files, like mp3s and gifs, and are stored in a program called a "wallet"[36] or on an online service such as Coinbase.[37] Bitcoin wallets can be held on the hard drive of a user's personal computer or on an external hard drive.[38] Like

34. In 2014, Newsweek reporter Leah McGrath Goodwin believed that she had found Bitcoin's founder in Dorian Satoshi Nakamoto in Temple City, California. Dorian Nakamoto, a former electrical engineer, has categorically denied that he is the founder of Bitcoin. *See* Leah McGrath Goodwin, *The Face Behind Bitcoin*, NEWSWEEK (March 6, 2014), http://www.newsweek.com/2014/03/14/face-behind-bitcoin-247957.html. The day after the story broke, the Satoshi Nakamoto account made its first post since announcing Bitcoin on the P2P Foundation Website, stating that he or she (or they) were not Dorian Nakamoto. This was the first post by the Satoshi Nakamoto account in over five years, and the mystery continues. *See* Satoshi Nakamoto, Reply to discussion titled *Bitcoin open source implementation of P2P currency* (Mar. 7, 2014), http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source?commentId=2003008%3AComment%3A52186.

35. Nakamoto, *supra* note 4.

36. Kaplanov, *supra* note 3, at 116, 124.

37. COINBASE, https://www.coinbase.com/ (last visited Feb. 10, 2015).

38. *See* CFPB, *Risks to consumers posed by virtual currencies*, at 4 (Aug. 2014), http://files.consumerfinance.gov/f/201408_cfpb_consumer-advisory_virtual-currencies.pdf (private keys can be stored on external hard drives). Dutch Bitcoin enthusiast and entrepreneur Martijn Wismeijer has implanted two microchips into his palms to keep his Bitcoin wallet handy. Cyrus Farivar, *Man has NFC chips injected into his hands to store cold Bitcoin wallet*, ARS TECHINCA (Nov. 15, 2014), http://arstechnica.com/business/2014/11/man-has-nfc-chips-injected-into-his-hands-to-store-cold-bitcoin-wallet/.

cash, Bitcoins can be destroyed, lost, or stolen.[39] For instance, if a user had their Bitcoins stored on a computer that became inoperable after being dropped, or an external hard drive storing Bitcoins was lost,[40] those Bitcoins would be irretrievable.[41] Bitcoins can only be sent or received by logging the transaction on the public ledger, the aforementioned blockchain.[42]

Bitcoins lack intrinsic value and do not derive value from a government; rather, a Bitcoin's value is purely a function of supply and demand.[43] Unlike paper "fiat currency"[44] that derives value from a government, Bitcoin is neither the creation of, nor backed by, any government.

Bitcoins can be obtained in three ways: (1) in exchange for conventional money in person or on an online exchange, (2) in exchange for the sale of goods or services, and (3) through mining.[45] Mining uses a computer's processing power to solve complex math problems both to maintain the blockchain public ledger and to "discover" new Bitcoins.[46]

Initially, Bitcoin appealed to a core group of anti-establishment enthusiasts on the fringes of the financial system, but more recently Bitcoin has become popular among venture capitalists and investment firms anticipating the wider adoption of the currency.[47] A number of leading retail businesses including Expedia, Overstock, Newegg, and the

39. *See* Grinberg, *supra* note 6, at 180 (2012).

40. U.K. Resident James Howell threw out an external hard drive in 2013 containing 7,500 Bitcoins. At the time, collectively these Bitcoins were valued at $9 million dollars. Kelly Phillips Erb, *From Treasure To Trash: Man Tosses Out Bitcoin Wallet On Hard Drive Worth $9 Million*, FORBES (Nov. 30, 2013), http://www.forbes.com/sites/kellyphillipserb/2013/11/30/from-treasure-to-trash-man-tosses-out-bitcoin-wallet-on-hard-drive-worth-9-million/.

41. *See* CFPB, *supra* note 38, at 4.

42. Kaplanov, *supra* note 3, at 116.

43. *Id.* at 115. Or as venture capitalist Marc Andreessen argues: "It's not as much that the Bitcoin currency has some arbitrary value and then people are trading with it; it's more that people can trade with Bitcoin (anywhere, everywhere, with no fraud and no or very low fees) and as a result it has value." Marc Andreessen, *Why Bitcoin Matters*, N.Y. TIMES (Jan. 21, 2014), http://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters/.

44. *Fiat Money Definition*, DICTIONARY.COM http://dictionary.reference.com/browse/fiat+money (last visited on Jan. 24, 2015).

45. ELWELL ET AL., *supra* note 2, at 2.

46. *Id.*

47. Sydney Ember, *New York Proposes First State Regulations for Bitcoin*, N.Y. TIMES (July 17, 2014), http://dealbook.nytimes.com/2014/07/17/lawsky-proposes-first-state-regulations-for-bitcoin/.

Dish Network now accept Bitcoin.[48] Merchants such as Overstock deal with the price volatility of Bitcoin by immediately converting their Bitcoin revenue into dollars or some other more stable currency.[49] Overstock CEO Patrick Byrne has explained that "[u]ntil [Overstock] can hedge [the pricing risks] through some kind of derivative instrument, [the company doesn't] want to take that direct exposure."[50]

Bitcoin protocol seeks to solve the double-spending problem inherent in noncash payment systems and the need for a trusted third party (such as a bank or credit card company) to verify the integrity of the transaction.[51] There is no double-spending with cash, as the physical dollar bill must be surrendered. In a traditional noncash payment system a trusted intermediary, such as a bank or credit card company, maintains a private ledger to track account balances and prevent the double-spending.[52]

The double-spending problem is a specific version of the duplication problem, which has plagued the creation of rivalrous digital assets such as scarce digital property and currency.[53] The duplication problem occurs when an owner of a digital asset, such as an mp3, can simply duplicate the file at nearly zero cost (besides the cost of the electricity powering the computer) and thus transfer the file without losing possession of it.[54] Before the advent of the blockchain, *A* could pay both *B* and *C* with Bitcoin *X*. Something that can be sold without actually giving up possession loses much, if not all of its value.

The Bitcoin protocol solves this by making the blockchain the only way to transfer Bitcoins. Every Bitcoin transaction is broadcast to the entire network of Bitcoin users and the specific Bitcoin is assigned to a new owner on the public ledger.[55] Once a transaction has been broadcast,

48. *See, e.g.*, Shawn Knight, *Dell joins the growing list of major retailers now accepting Bitcoins,* TECHSPOT (July 18, 2014), http://www.techspot.com/news/57461-dell-joins-the-growing-list-of-major-retailers-now-accepting-bitcoins.html.

49. Rob Wile, *Bitcoin Is Experiencing Its Longest Stretch Of Price Stability In A While*, BUSINESS INSIDER (Jan. 29, 2014), http://www.businessinsider.com/bitcoin-volatility-slows-2014-1.

50. *Id.*

51. Nakamoto, *supra* note 4, at 1.

52. BRITO & CASTILLO, *supra* note 10, at 4.

53. Fairfield, *supra* note 11, at 14–15.

54. *Id.* at 15.

55. Andreas M. Antonopoulos, *Mastering Bitcoin*, Chapter 1 (2015), http://chimera.labs.oreilly.com/books/1234000001802/index.html.

it is recorded, time-stamped, and cannot be modified.[56] Thus the blockchain accomplishes this task publicly, and requires no third party to verify the transaction.[57] Essentially, *A* transfers ownership of Bitcoin *X* to *B*, and the blockchain records *B* as the new owner of Bitcoin *X*. *A* can no longer double-spend Bitcoin *X* by transferring it to *C* as well since *A* is no longer the owner of that Bitcoin on the public ledger.[58]

There are also a number of other digital currencies, such as Dogecoin, Litecoin, and Darkcoin,[59] but Bitcoin—by name recognition, blockchain hash rate,[60] transaction count, and real world applications—remains by far the most popular.[61]

B. BLOCKCHAIN BASICS: THE MECHANICS OF THE BLOCKCHAIN

The Bitcoin protocol both rewards actors for devoting the processing power of their computers to maintaining the blockchain and makes it prohibitively difficult to falsify a transaction through the mining process.[62]

A useful way to picture the blockchain is as a giant book, with each new block a page added to the top. Each new page contains all the transactions in the network that have been completed since the last page was added. All the Bitcoin miners are competing in a race to solve a complex math problem that will add the next page (block) on top of all the older pages on the public ledger.[63] Whichever miner successfully adds the next page is rewarded in Bitcoins by the Bitcoin protocol.[64]

This analogy is helpful in understanding what makes the blockchain a secure public ledger. For a bad actor to falsify the blockchain, they would have to write all the old pages of the "book" as well as new false counterfeit pages at a speed faster than all the honest users in the network. This task

56. 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*, 2013 J.L. TECH. & POL'Y 165, 168 (2013).

57. BRITO & CASTILLO, *supra* note 10, at 4.

58. *See id.*

59. *See Crypto-Currency Market Capitalizations,* COINMARKETCAP, http://coinmarketcap.com/ (last updated Feb. 10, 2015).

60. The number of attempts Bitcoin miners make at solving a particular block of transactions. *See infra* Section I.B.2.

61. *See* Jon Evans, *A Bitcoin Battle Is Brewing*, TECHCRUNCH (Dec. 6, 2014), http://techcrunch.com/2014/12/06/a-bitcoin-battle-is-brewing.

62. ELWELL ET AL., *supra* note 2, at 2.

63. *See* Fairfield, *supra* note11, at 17–21 (describing the process for proving blocks and adding them to the blockchain).

64. *See id.* at 19.

is nearly impossible,[65] and if a major technological breakthrough occurred that allowed a bad actor to marshal hitherto unforeseen amounts of computing power, he or she would be better served by simply applying that power to honest mining.[66] Application of all that computational power to Bitcoin mining would allow that actor to prove blocks at a faster rate than the rest of the network and would create a more predictable source of income.[67] Additionally, a massive hacking of the entire blockchain would cause the value of Bitcoins to plummet, thus making the loot of their crime substantially less valuable.[68] This decentralized mechanism for guaranteeing the security of the system is what makes the blockchain revolutionary. Rather than having a trusted (and hackable[69]) intermediary to verify transactions (such as a bank or credit card company), while imposing large fees for their trouble, the blockchain is a trustless public ledger with substantially lower transaction fees.[70] Put another way, the Bitcoin protocol has created a system that incentivizes good behavior without the need for oversight from a central authority.[71] The resources in terms of sheer computing power required to be a bad

65. Put another way, an attacker would have to guess the hashes enough times to look like the rest of the system, matching the combined processing power of the entire network, and to continue guessing faster than the current block chain. The protocol accepts the block chain with the higher degree of difficulty. Thus an attacker would have to guess more hashes, faster, and at a greater degree of difficulty than the rest of the network. *Id.* at 21.

66. Nakamoto, *supra* note 4, at 4. Notably, two computer scientists at Cornell, Ittay Eyal and Emin Gün Sirer, believe this confidence is misplaced and that the blockchain could be falsified with only a third of miners, as opposed to over half, colluding dishonestly. Eyal and Sirer propose the possibility of a "selfish mining pool" which for reasons based in the Bitcoin Protocol could, with more than one third of miners, severely undermine the system, ultimately destroying its decentralized character. In practice, this would entail a pool of selfish miners working, as honest miners do, on solving a new block to put on top of the blockchain. But instead of publishing that block immediately, the selfish miners would keep the block private. From here, the selfish miners will attempt to build on their lead by finding and solving another block, and just before the honest miners close the gap, the selfish miners would publish their hidden longer chain, nullifying the work of the honest miners. This increase in profits would incentivize more honest miners to join the selfish mining pool and eventually change the blockchain from a decentralized system with all of its benefits of security and finality to a centralized system, operating at the whim of colluding miners. ITTAY EYAL & EMIN GÜN SIRER, MAJORITY IS NOT ENOUGH (2014), *available at* http://www.cs.cornell.edu/~ie53/publications/btcProcArXiv.pdf.

67. *See* Nakamoto, *supra* note 4, at 4.

68. *See id.*

69. *See supra* note 30.

70. ELWELL ET AL, *supra* note 2, at 5.

71. Antonopoulos, *supra* note 55, at Chapter 8.

actor would be more profitably used to support the system rather than undermine it.[72] This is also the process for implementing the monetary supply, which makes the Bitcoin protocol more elegant still.[73]

1. The Security Features of Bitcoin and the Blockchain

The Bitcoin protocol is a very secure way to transfer currency because of its utilization of cryptography. Cryptography in the most basic sense is the ability to hide one's communications from people who lack the correct key to decode a communication[74] that might otherwise look like gibberish.[75] Cryptography has been used in one form or another at least since the ancient Greeks,[76] and with the advent of computers and their massive processing power, is the basis for Bitcoin's ability to be transferred securely.[77]

Security in the Bitcoin protocol is ensured through "cryptographic proof," allowing the parties to deal directly with each other, rather than through a third party.[78] Each user's account has two cryptographically related keys, a "public key" and a "private key."[79] The keys are mathematically related, but it is not possible to use the public key to derive the private key.[80] The public key, essentially a string of letters and numbers approximately twenty-seven to thirty-four characters long, is best thought of as an address listed on the blockchain that anyone in the public can see.[81] It acts as the destination at which a user receives Bitcoins.[82]

Only the owner of the Bitcoin knows the "private key", and can use it to authorize or "sign" a transfer of Bitcoins to a different account's[83] public key address. If a malicious actor were to discover another user's private key, that malicious actor would be able to steal that user's Bitcoins.[84]

It is irrelevant how or where the transaction is transmitted to the Bitcoin network as peer-to-peer networks connect each client (also known

72. *Id.*
73. *Id.*
74. *Cryptography Definition*, *supra* note 8.
75. *See* Dion, *supra* note 56, at 168 (a Bitcoin private key is "essentially a string of letters and numbers approximately twenty-seven to thirty-four characters long).
76. V.V. YASHCHENKO, CRYPTOGRAPHY: AN INTRODUCTION 6 (2000).
77. *See* Kaplanov, *supra* note 3, at 116.
78. *Id.*
79. Dion, *supra* note 56, at 167–68.
80. Fairfield, *supra* note 11, at 18.
81. Dion, *supra* note 56, at 168.
82. *Id.*
83. Typically another user, though users can have multiple accounts if they wish.
84. Dion, *supra* note 56, at 184.

as a node) to several other Bitcoin clients.[85] Any Bitcoin node that receives a valid transaction that the node has not seen before will forward the transaction to all connected nodes, and within seconds the transaction will reach a large percentage of nodes.[86]

The public key address contains no information about the user, and though Bitcoin users do enjoy a much higher level of privacy than users of traditional digital-transfer services, staying completely anonymous can be quite difficult.[87] Without knowing to whom a public key address corresponded, in one experiment, researchers found that behavior-based clustering-techniques were able to reveal 40 percent of Bitcoin users.[88] Yet, if a public key were linked to a person's identity, one could look through the recorded transactions on the blockchain and view all transactions associated with that public key.[89] Public key addresses on the public ledger can be identified years after an exchange is made.[90] Once Bitcoin exchanges become fully compliant with bank secrecy regulations requiring firms to collect personal data on their customers this privacy will be further eroded. A more detailed discussion of bank secrecy regulations is below.[91] Anonymity could be guaranteed for a short time if a user were to meet a Bitcoin holder in person and pay that owner for their Bitcoins in cash, but there is evidence that statistical techniques and pattern analysis can unmask up to 60 percent of Bitcoin users.[92]

2. Bitcoin Mining and the Maintenance of the Blockchain

A transaction is not part of the public ledger (blockchain) until verified and included in a block through a process called mining.[93] Mining is both the process for creating Bitcoins and the method for updating the blockchain with the most current transactions.

Transactions are bundled into blocks that are generated every ten minutes in a computationally intense process that requires miners to solve

85. Antonopoulos, *supra* note 55, at Chapter 2.
86. *Id.*
87. BRITO & CASTILLO, *supra* note 10, at 9.
88. Elli Androulaki et al., *Evaluating User Privacy in Bitcoin*, CRYPTOLOGY EPRINT ARCHIVE (2013), https://eprint.iacr.org/2012/596.
89. BRITO & CASTILLO, *supra* note 10, at 8.
90. *Id.* at 9.
91. *See infra* Section IV.B.1.a).
92. ALEX BIRYUKOV ET AL., DEANONYMISATION OF CLIENTS IN BITCOIN P2P NETWORK (2014), *available at* http://orbilu.uni.lu/bitstream/10993/18679/1/Ccsfp614s-biryukovATS.pdf.
93. *Id.*

a difficult mathematical problem.[94] These problems require a great deal of computation to prove, but very little computation to verify as proven.[95] This "proof-of-work" solution requires quadrillions of computations per second across the entire Bitcoin network.[96] These computations require the computer to guess numbers.[97] Josh Fairfield likens this process to rolling dice.[98] The computation does not in and of itself discover anything, but due to the length of the values to be guessed, it inherently has a mathematically predictable degree of difficulty that can be increased by making the values, or "hashes" longer.[99] The hash is a way of transforming an arbitrary amount of data into a fixed number that is not invertible (the data cannot be deduced from the hash).[100]

Bitcoin mining requires an incredible amount of computing power. In March 2014, an estimated 30,000 trillion hashes per second were computed on the network.[101] Taken as a whole, the Bitcoin network is more powerful than the combined computing power of the top five hundred supercomputers in the world.[102] Security expert Andreas M. Antonopoulos likens Bitcoin mining to a giant game of competitive Sudoku that resets every time a player solves the puzzle. It can take a lot of work to solve the puzzle, but checking the solution is quite simple.[103]

In exchange for proving blocks, miners are rewarded with transaction fees and a set amount of Bitcoins that diminishes as more Bitcoins are mined.[104] The Bitcoin protocol adjusts the difficulty of the computational problems to ensure that Bitcoins mining occurs at a predictable and limited rate;[105] the resulting diminishing returns are meant to simulate the actual diminishing returns that come in real mining.[106] To use Antonpoulos' Sudoku analogy again, the difficulty of the puzzle can be adjusted to require more computing power to solve a block by making the

94. *Id.*
95. *Id.*
96. *Id.*
97. Fairfield, *supra* note 11, at 19.
98. *Id.*
99. *Id.*
100. *Id.* at 20.
101. Lawrence Trautman, *Virtual Currencies; Bitcoin & What Now After Liberty Reserve, Silk Road, and Mt. Gox?*, 20 RICH. J.L. & TECH. 1, 50 (2014).
102. *Id.* at 50–51.
103. Antonopoulos, *supra* note 55, at Chapter 2.
104. BRITO & CASTILLO, *supra* note 10, 6–7.
105. Antonopoulos, *supra* note 55, at Chapter 2.
106. Like with shovels and dirt and rocks.

puzzle larger (by adding more rows or columns).[107] The protocol sets an arbitrary cap of twenty-one million Bitcoins.[108] 2140 is the predicted date the last "satoshi," or 0.00000001 of Bitcoin will be mined.[109] As this time approaches, miners will incur greater expenses due to the progressively more difficult hashes dictated by the protocol.[110]

Transaction costs will have to rise to allow mining to continue to be profitable.[111] Although transaction fees typically represent 0.5% or less of a Bitcoin miner's income,[112] the rest coming from newly minted Bitcoins, these fees still play an important role as they affect the prioritization of which blocks are processed first, since parties to a transaction can pay higher fees to incentivize miners to solve their block before other blocks.[113] This allows market forces to influence the speed at which a transaction is verified.[114] The minimum transaction fee is currently fixed at 0.0001 Bitcoin, or a tenth of a milli-Bitcoin per kilobyte, but if a user wants their transaction processed more quickly, they can include a higher fee to incentivize miners.[115]

Energy is the primary expense in mining Bitcoins, resulting in the creation of large computer centers in places like Washington State and Iceland, where energy costs are particularly low due to the abundance of hydroelectric and geothermal power.[116] In the early stages of mining, essentially any computer had the processing power to engage in Bitcoin mining, but as the hashes have gotten more difficult, only highly specialized equipment is capable of mining.[117] "Botnets" voluntarily enlist large pools of computers to combine computing power to mine Bitcoins more quickly, while splitting the profits based on the percentage of computing power contributed.[118] There is evidence that hackers have also

107. Antonopoulos, *supra* note 55, at Chapter 2.
108. *See* ELWELL ET AL., *supra* note 2, at 2.
109. BRITO & CASTILLO, *supra* note 10, at 7.
110. *Id.*
111. *See id.*
112. Antonopoulos, *supra* note 55, at Chapter 8.
113. *Id.* at Chapter 5.
114. *Id.*
115. Bitcoins are divisible to eight decimal places. The maximum amount of spendable units is more than 2 quadrillion (2000 trillion). *See id.*
116. *See* Nathaniel Popper, *Into the Bitcoin Mines*, N.Y. TIMES (Dec. 21, 2013), http://dealbook.nytimes.com/2013/12/21/into-the-bitcoin-mines/.
117. The specialized equipment used to mine Bitcoins is costly, ranging in price from three to nine thousand dollars. *See* Bitcoin Calculator, BITCOINWISDOM.COM, https://bitcoinwisdom.com/bitcoin/calculator (last visited Jan. 24, 2015).
118. *See, e.g.*, BTC GUILD, https://www.btcguild.com to join (last visited Jan. 24, 2015) ("one of the oldest remaining Bitcoin pools").

conscripted unwitting CPUs to the task.[119] In this scenario, hackers utilize a victim's processor power without their knowledge to mine for Bitcoins, presumably without sharing any profits from proven blocks.[120]

Once a block has been verified through the mining process it is added to the blockchain on top of all the previous blocks before it.[121] Thus, the blockchain essentially contains the history of every Bitcoin from its creation through the present day.[122]

II. POTENTIAL USES OF BITCOIN AND THE BLOCKCHAIN

The potential uses of Bitcoin and the blockchain range from the prosaic, such as lowering both transaction costs and risk of credit card fraud, to the more outré use as a (more) stable currency for residents of countries with volatile currencies, to the revolutionary by creating a new theory of digital property through the blockchain. This Part will first examine the potential benefits from Bitcoin based on its relatively low transaction costs. Then it will examine the goals of the two venture capitalists that have invested the most in Bitcoin and Bitcoin-based companies. Finally, this Part will discuss the creation of a new theory of digital property based on blockchain technology.

A. LOWERED TRANSACTION COSTS

Certain benefits of Bitcoin are fairly intuitive and do not require a substantial rethinking of the digital economy. Bitcoin's ability to lower transaction costs for users is of particular import and is one of its features that is driving its adoption today.

Bitcoin is particularly attractive to small businesses looking for ways to lower their transaction costs. Though credit cards have made transactions much easier for consumers, merchants must pay a variety of authorization fees, transaction fees, statement fees, interchange fees, and customer service fees, to name a few.[123] These fees amount to 2 to 3 percent of the transaction.[124] For a business with a 5 percent profit margin,[125] lowering

119. Dion, *supra* note 56, at 184–85.

120. A victim would have to observe a drop in the performance of their computer, a spike in their electricity bill, or an increased amount of data being sent to and from their computer to realize that their CPU had been enlisted in a botnet.

121. Antonopoulos, *supra* note 55, at Chapter 2.

122. *See* BRITO & CASTILLO, *supra* note 10, at 8.

123. *Id.* at 10–11.

124. CHRIS JAY HOOFNAGLE, JENNIFER M. URBAN & SU LI, BCLT, MOBILE PAYMENTS: CONSUMER BENEFITS & NEW PRIVACY CONCERNS 3 (Apr. 24, 2012).

transaction fees by 1 percent of the businesses' revenue gives an additional 20 percent profit. Additionally, merchants labeled "high risk" by credit card companies who have had difficulty finding payment processors have begun to turn to Bitcoin merchant service providers as an affordable and convenient alternative to credit card companies.[126]

Conducting business through Bitcoin also allows merchants to avoid chargeback fraud, where a consumer reverses payment based on a false claim that the product has not been delivered or a service has not been rendered.[127] The irreversibility of a Bitcoin transaction can prevent this type of fraud, as once a Bitcoin has been transferred on the blockchain, that transfer is irreversible. Traditional credit card services will still allow consumers to enjoy the capability to engage in chargebacks as a protection from unscrupulous merchants or merchant errors.[128] But a merchant may wish to give a discount for payments in Bitcoin to incentivize consumers to forgo their ability to chargeback a credit card transaction, to protect the merchant from potential fraud.

Bitcoin also holds great potential for lowering transaction costs required to send remittances back to relatives in developing countries. Remittances to developing countries were projected to reach $454 billion in 2015.[129] Wire services such as Western Union and MoneyGram charged an average fee of roughly 8 percent for sending remittances in the third quarter of 2014.[130] But with Bitcoin, the transaction fee is less than 0.0005 Bitcoins, or approximately 1 percent, assuming liquidity.[131]

125. The profit margin for restaurants in 2013 was 5.1%. *See* Mary Ellen Biery, *U.S. Restaurants Seeing Fatter Margins*, FORBES (June 22, 2014), http://www.forbes.com/sites/sageworks/2014/06/22/us-restaurants-margins/.

126. "High risk" merchants include jewelry businesses, software sellers, online storage providers, and travel services. These merchants are considered high risk because of their chargeback volume. Bailey Reutzel, *Some Risky Merchants Turn to Bitcoin Processor; Others Go It Alone*, PAYMENTS SOURCE (Nov. 8, 2013), http://www.paymentssource.com /news/some-risky-merchants-turn-to-bitcoin-processor-others-go-it-alone-30159 74-1.html.

127. BRITO & CASTILLO, *supra* note 10, at 12.

128. *Id.* at 12.

129. DILIP RATHA ET AL., MIGRATION AND REMITTANCES: RECENT DEVELOPMENTS AND OUTLOOK SPECIAL TOPIC: FORCED MIGRATION 1 (World Bank, Oct. 6, 2014), *available at* http://siteresources.worldbank.org/INTPROSPECTS/Resources/ 334934128990760745/MigrationandDevelopmentBrief23.pdf.

130. *Id.* at 1, 14 n.13.

131. BRITO & CASTILLO, *supra* note 10, at 14.

Professor Susan Athey, Economics of Technology Professor at the Stanford Graduate School of Business,[132] believes that these benefits would allow the world's unbanked poor to access global markets.[133] Currently, many people in developing countries do not have and are unable to obtain bank accounts, and as a result are completely cut off from international financial markets and participation in the global economy.[134] Even for those with credit cards, many merchants refuse to accept international credit card transactions because the fraud rate is too high.[135] Because the transfer of Bitcoins is instantaneous, merchants can accept the currency without fear of fraud.[136] Additionally, in countries with high inflation, people could use Bitcoin to purchase assets on the global market, like tractors, that better hold their value.[137]

B. BITCOIN AS A STABLE CURRENCY IN WEAK MARKETS AND THE BLOCKCHAIN AS A RECORDING SYSTEM FOR MORE THAN JUST BITCOIN

A number of venture capitalists have begun investing in Bitcoin and blockchain-based businesses.[138] This Section will examine the goals of the two venture capitalists that have invested the most to date, Tim Draper and Marc Andreessen.

Tim Draper,[139] co-founder of the investment firm Draper Fisher Jurvetson,[140] sees the future of Bitcoin in emerging economies.[141] Draper,

132. *Susan Athey*, STANFORD GRADUATE SCHOOL OF BUSINESS, http://www.gsb.stanford.edu/faculty-research/faculty/susan-athey (last visited Feb. 26, 2015).

133. Laura Shin, *Who Will Benefit From Digital Currency? Bitcoin Experiment Gives a Glimpse*, FORBES (Nov. 26, 2014), http://www.forbes.com/sites/laurashin/2014/11/26/who-will-benefit-from-digital-currency-bitcoin-experiment-gives-a-glimpse/.

134. *Id.*

135. *Id.*

136. *See id.*

137. *Id.*

138. *See* Nathaniel Popper, *$25 Million in Financing for Coinbase*, N.Y. TIMES (Dec. 12, 2013), http://dealbook.nytimes.com/2013/12/12/venture-capital-bets-big-on-bitcoin/.

139. Draper purchased nearly 30,000 Bitcoins for an estimated $19 million dollars auctioned off by the government from the now-defunct online black market Silk Road. *See* Olga Kharif, *Bitcoin Auction Winner Draper to Big Again in December*, BLOOMBERG (Nov. 18, 2014), http://www.bloomberg.com/news/2014-11-18/bitcoin-auction-winner-draper-to-bid-again-in-december.html. The United States Marshals Service held another sealed bid auction for another 50,000 Bitcoins in December 2014. *See For Sale: 50,000 bitcoins*, U.S. MARSHALS SERV. http://www.usmarshals.gov/assets/2014/dpr-bitcoins/ (last visited Jan. 24, 2015). Draper won 2,000 of the Bitcoins with the remaining balance won by the New York-based

with the help of Bitcoin exchange startup Mirror,[142] seeks to "create new services that can provide liquidity and confidence to markets that have been hamstrung by weak currencies."[143] Financial crises are a constant threat in much of the world, with countries like Argentina serving as instructive examples.[144] From the mid-1970s to 2002, Argentina had eight currency crises, four banking crises, and two sovereign defaults.[145] Graciela Kaminsky has identified ninety-six currency crises between January 1970 and February 2002 in countries across Europe, Asia, and South America.[146] Draper told CNBC's Squawk on the Street television show that he believes that "Bitcoin is a great alternative for . . . economies where inflation really saps the strength of a country's economy" and that he expects "Pagos in Argentina, Pagatech in Africa, and [Coincove in Mexico][147] . . . [to] thrive because people in those countries are not as confident in their own governments' fiat currency."[148] Notably, U.S. dollars already play a strong role in this respect with a vast amount of dollars held abroad as an alternative to local currencies because dollars are a more stable way to preserve wealth.[149] The Federal Reserve estimates that more than two-thirds of $100 bills are held overseas.[150]

exchange SecondMarket. Sydney Ember, *At an Auction of Bitcoins Seized From Silk Road, SecondMarket Wins Big*, N.Y. TIMES (Dec. 9, 2014), http://dealbook.nytimes.com/2014/12/09/secondmarket-nearly-sweeps-latest-bitcoin-auction/.

140. DRAPER FISHER JURVETSON, http://dfj.com/teams (last visited Feb. 11, 2015).

141. Sydney Ember, *Winner of Bitcoin Auction, Tim Draper, Plans to Expand Currency's Use*, N.Y. TIMES (July 2, 2014), http://dealbook.nytimes.com/ /07/02/venture-capitalist-tim-draper-wins-bitcoin-auction/,.

142. Mirror is owned by Vaurum. About Mirror, MIRRORX.COM, https://mirrorx.com/#/about (last visited Dec. 22, 2014).

143. Ember, *supra* note 141.

144. Trautman, *supra* note 101, at 67.

145. *Id.* at 68.

146. These countries include Argentina, Bolivia, Brazil, Chile, Columbia, Denmark, Finland, Indonesia, Israel, Malaysia, Mexico, Norway, Peru, Spain, Sweden, the Philippines, Thailand, Turkey, Uruguay, and Venezuela. *Id.* at 66 (citing GRACIELA KAMINSKY, VARIETIES OF CURRENCY CRISES 1 (Nat'l Bureau of Econ. Research, Working Paper No. 10193, 2003), *available at* http://www.nber.org/papers/w10193.pdf).

147. Pagos, Pagatech, and Coincove are mobile payments companies.

148. *Why VC Tim Draper bought all those bitcoins*, CNBC.COM (July 7, 2014), http://www.cnbc.com/id/101816404.

149. *See generally* RUTH JUDSON, CRISIS AND CALM: DEMAND FOR U.S. CURRENCY AT HOME AND ABROAD FROM THE FALL OF THE BERLIN WALL TO 2011 (Bd. of Governors of the Fed. Reserve Sys. Int'l Fin. Discussion Papers, IFDP 1058 Nov. 2012), *available at* http://www.federalreserve.gov/pubs/ifdp/2012/ 1058/ifdp1058.pdf.

150. *Id.* at 12.

Marc Andreessen, co-founder and partner of the venture capital firm Andreessen Horowitz[151] believes that the blockchain's security features are what will allow the technology to flourish.[152] As of March 2014, Andreessen's firm has made approximately $50 million in investments in blockchain related businesses, believed to be more than the investments of any other firm.[153] Andreessen argues that not only will payments in Bitcoin be much safer for consumers than credit cards,[154] but also that the inherent security features of the blockchain will allow for the transfer of digital titles and property.[155] Andreessen suggests that in the future, the blockchain will allow for a trustless transfer, without intermediaries, of digital stocks, equities, bonds, contracts, keys, and titles.[156]

In a similar vein, Jeff Garzik, one of Bitcoin's core developers, has suggested the possibility of "smart" self-executing contracts.[157] For instance, a "smart loan" could automatically adjust interest rates based on the financial performance of the borrower.[158] The contract's code could be written to include automated observation of real world metrics, which now require manual reporting, monitoring, and enforcement.[159] As discretion on the part of the lender is removed, Houman B. Shadab of New York Law School's Center for Business and Financial Law suggests a "smart contract" of this sort would greatly reduce or eliminate the need for litigation, because it removes much of the potential for parties to have a dispute.[160]

151. ANDREESSEN HOROWITZ, http://a16z.com/team/ (last visited Feb. 11, 2015).

152. *See* Brian Fung, *Marc Andreessen: In 20 years, we'll talk about Bitcoin like we talk about the Internet today*, WASH. POST (May 21, 2014), http://www.washingtonpost.com/blogs/the-switch/wp/2014/05/21/marc-andreessen-in-20-years-well-talk-about-bitcoin-like-we-talk-about-the-internet-today/.

153. Gregory Zuckerman, *Web Pioneer Keeps Faith, and Cash, in Bitcoin*, WALL ST. J. (Mar. 21, 2014), http://www.wsj.com/articles/SB10001424052702304026304579453501821936252.

154. Andreessen notes that as Bitcoin transfer is instantaneous when a customer purchases a good with Bitcoins, hackers cannot steal that customer's information during the transfer. While Hackers could still steal Bitcoins from poorly secured merchant computer systems, this does increase the risk of loss, fraud, or identity theft to consumers. *See* Andreessen, *supra* note 43.

155. Fung, *supra* note 152.

156. *Id.*

157. Everett Rosenfeld, *Forget currency, bitcoin's tech is the revolution*, CNBC.COM (Nov. 13, 2014), http://www.cnbc.com/id/102178309#.

158. *Id.*

159. *Id.*

160. *Id.*

C. A NEW THEORY OF DIGITAL PROPERTY MADE POSSIBLE BY THE BLOCKCHAIN

At the outer frontier of theorizing on the impact of the blockchain, Professor Joshua Fairfield of the Washington and Lee University School of Law has proposed that the advent of the blockchain as a trustless public ledger that allows for rivalrous digital property warrants a new theory of property as an information communication and storage system.[161] Fairfield argues that property law has managed the transition to the online ecosystem poorly compared to tort and contract law.[162] Yet, with the advent of the blockchain, true digital ownership interests are now possible and rethinking property as an information protocol will avoid placing false constraints on the extension of traditional property rules to digital assets.[163]

The blockchain can be used to implement a property system by tying real property to specific coins within the chain through tokenization.[164] Tying a legal right to a token is common in property law, with examples ranging from paper deeds for land to paper titles for a car.[165] Thus a Bitcoin, or part of a Bitcoin, could be "tokenized" to represent a real asset, such as land. This "tokenized" coin would not impact the rest of the blockchain, but whoever owned the coin would own its associated commodity, such as a home or automobile.[166] These tokenized coins would have all the aforementioned benefits of any other Bitcoin, such as rivalrousness, security, and would be easily tracked on the decentralized public ledger.[167] A tokenized public ledger would offer new solutions to old property problems, such as low cost secure transfer, easy tracing of transactions, prevention of the double spending problem, and the near impossibility of reversal or falsification.[168]

The vast bulk of owned wealth is recorded in systems that tell users who owns what, and the blockchain can decentralize this information and address what Fairfield calls "one of the great inefficiencies of modern property: its reliance on expensive, inaccurate, hard-to-access, hard-to-search, and insecure ledgers of all stripes."[169] Thus, under a new theory of

161. *See generally* Fairfield, *supra* note 11.
162. *Id.* at 8.
163. *See id.* at 9.
164. *Id.* at 24–26.
165. *Id.* at 25.
166. *Id.* at 24.
167. *See id.* at 26.
168. *Id.*
169. *Id.* at 5.

property as an information protocol, the effectiveness of a property system should be judged on how well it stores and communicates information about ownership.[170] Today property records are contained in a "hodgepodge of relatively inaccurate, sometimes insecure, and often expensive ledgers" that are "notoriously costly to search."[171]

The Mortgage Electronic Registration System ("MERS") is a timely example of a current system that could be improved through public ledger technology. MERS is a database set up by banks to facilitate the transfer of mortgages and track their ownership internally.[172] As of 2007, more than half of all home mortgage loans originated in the United States were registered on the MERS system.[173] MERS is listed as the owner in county land records.[174] Yet New York Attorney General Eric T. Schneiderman alleges that because MERS records are private, MERS has limited the public's ability to track property transfers and thus it is difficult to verify the chain of title for a loan or a current noteholder for many properties.[175] Thus during the foreclosure crisis, it became difficult for borrowers to work out exactly who owned their mortgage and to get help in working out their loans.[176] If all mortgages were recorded on the blockchain, instead of MERS, tracking the chain of ownership and mortgages would be a simple task, and defaulting homeowners could more easily determine which bank has the authority to negotiate refinancing options.

As noted above, the Bitcoin protocol rewards Bitcoin miners in Bitcoins for utilizing their computing power to maintain the blockchain. Thus, for Professor Fairfield's ideas to become a reality, Bitcoins need to be adopted by the broader public.

170. *Id.* at 9.

171. *Id.* at 12.

172. Christopher L. Peterson, *Predatory Structured Finance*, 28 CARDOZO L. REV. 2185, 2211–12 (2007).

173. *Id.* at 2212.

174. *Id.*

175. Chad Bray, *New York Sues Banks Over Mortgage Registry System*, WALL ST. J. (Feb. 3, 2012), http://online.wsj.com/articles/SB10001424052970203889904577201060859616158.

176. Gretchen Morgenson, *Mortgage Registry Muddles Foreclosures*, N.Y. TIMES (Sept. 1, 2012), http://www.nytimes.com/2012/09/02/business/fair-game-mortgage-registry-muddles-foreclosures.html.

III. THE DARKER SIDE OF BITCOIN: THE POTENTIAL FOR BLACK MARKETS, THEFT, AND TAX EVASION

Cash remains the ultimate anonymous currency. The U.S. $100 note is particularly popular for laundering the profits of illicit activities.[177] Professor Edgar Feige estimates that U.S. currency is the preferred medium for "facilitating clandestine transactions, and for storing illicit and untaxed wealth."[178] It is estimated that over 50 percent of all hard currency in most countries is used to hide transactions.[179] These illicit transactions include illegal trade in drugs, arms, and sex as well as unreported income to skirt the tax code.[180]

In many ways, Bitcoins and cash share a key property that makes them both suitable for unlawful activity: neither requires an institutional (and subpoenable) intermediary.[181] In the same way that it can be hard to track the movements of a briefcase full of $100 bills in a direct transaction between two parties, it can be difficult to track a direct exchange of Bitcoins between two parties.[182] Like cash, there is nothing inherently nefarious about Bitcoins, but the digital nature of Bitcoin introduces a new wrinkle as it can be sent electronically, rather than requiring a physical meeting to exchange.

In the popular imagination, Bitcoin is associated with online black markets, unsavory characters, and risks to consumers from hackers.[183] This view is not entirely unwarranted. Bitcoin has been used as a key

177. *See* Chris Arnold, *Should We Kill the $100 Bill?*, NPR'S PLANET MONEY (Aug. 14, 2014), http://www.npr.org/blogs/money/2014/08/14/340356790/should-we-kill-the-100-bill.

178. Edgar L. Feige, *New Estimates of U.S. Currency Abroad, the Domestic Money Supply and the Unreported Economy* 4 (Munich Personal RePEc Archive, Working Paper No. 34778, 2011), *available at* http://mpra.ub.uni-muenchen.de/34778/1/MPRA_paper_34778.pdf.

179. Kenneth Rogoff, *Costs and benefits to phasing out paper currency*, Presentation at NBER Macroeconomics Conference (April 11, 2014), *available at* http://scholar.harvard.edu/files/rogoff/files/c13431.pdf.

180. Feige, *supra* note 178, at 4.

181. A hand-to-hand cash transaction lacks an institutional middleman. Similarly there is no Bitcoin company to raid or shut down in a direct transfer. *See* Kaplanov, *supra* note 3, at 168.

182. *See* BRITO & CASTILLO, *supra* note 10, at 7–8.

183. Stephen T. Middlebrook & Sarah Jane Hughes, *Regulating Cryptocurrencies in the United States: Current Issues and Future Directions*, 40 WM. MITCHELL L. REV. 813, 818–19 (2014).

component of illegal mail order drug and firearm markets,[184] in Ponzi schemes to defraud investors,[185] and has been stolen in large quantities by hackers.[186] Protecting society from these unlawful uses and vulnerabilities is vital to Bitcoin's wider adoption by the general public, and perhaps especially with older users.[187]

This Part will examine the most famous Bitcoin black market website, the disbanded "Silk Road" and its successor Agora, as examples of unlawful activities facilitated by the use of Bitcoin. Next, it will examine the hacked Bitcoin exchange Mt. Gox where consumers lost millions of dollars, as an example of the risks to consumers from improperly secured Bitcoin exchanges. Finally, it will explore Bitcoin's potential use for tax evasion.

A. ONLINE BLACK MARKETS: THE SILK ROAD

Silk Road was a deep Web[188] black-market site in operation from February 2011 to October 2013.[189] Through the anonymizing network TOR,[190] the pseudonymous nature of Bitcoin, plus "tumbling" services such as Bitcoin Bath,[191] users could order drugs and other illicit wares by mail.[192] It is estimated that while operational, Silk Road's transactions

184. *See* Jerry Brito, *Online Cash Bitcoin Could Challenge Government, Banks,* TIME TECHLAND, (Apr. 16, 2011), http://techland.time.com/2011/04/16/online-cash-bitcoin-could-challenge-governments/2/.

185. *See infra* Section IV.C.1; Secs. & Exch. Comm'n v. Shavers, No. 4:13-CV-416, 2014 WL 4652121 at *8 (E.D. Tex. Sept. 18, 2014) (finding defendants' operation to be a "sham and a Ponzi scheme").

186. BRITO & CASTILLO, *supra* note 10, at 22.

187. In a recent survey, of Americans aware of Bitcoin, people over the age of 55 were significantly less likely to choose to invest in Bitcoin rather than gold. Melanie Flanigan, *Most Americans Still Don't Trust Bitcoin Despite Widespread Awareness, New Survey Shows,* YODLEE, (Mar. 25, 2014), http://ir.yodlee.com/releasedetail.cfm?releaseid=867331.

188. The "deep Web" refers websites on the internet that are not accessible through search engines. *See* Michael K. Bergman, *The Deep Web: Surfacing Hidden Value*, 7 J. OF ELEC. PUBL'G 1 (Aug. 2001).

189. *See* BRITO & CASTILLO, *supra* note 10, at 23.

190. The Onion Router or TOR is software that allows users to browse the Internet in complete anonymity and free from third-party tracking by constantly changing the Internet Protocol ("IP") address of a computer. With TOR, users can explore the "deepnet" and explore sites that only host anonymous users. Dion, *supra* note 56, at 166.

191. A tumbling service combines payments from multiple buyers to multiple sellers to obscure which public keys were involved in a transaction. *See What do we do*?, BITCOINBATH, http://bitcoinbath.com/ (last visited Nov. 18, 2014).

192. *See* BRITO & CASTILLO, *supra* note 10, at 23.

amounted to $1.2 million monthly, representing only 0.15% of the $770 million in Bitcoin transactions in a single month.[193]

On October 1, 2013, Federal Bureau of Investigation ("FBI") agents and federal prosecutors in New York apprehended the Silk Road's mastermind Ross Ulbricht, also known as the Dread Pirate Roberts, in a San Francisco library with his laptop open.[194] This action allowed the FBI to shut down Silk Road and seize nearly 30,000 Bitcoins.[195]

Agora, the "online bazaar for contraband," has most successfully replaced Silk Road.[196] Silk Road 2.0 was also launched in November 2013 by several of the administrators from the original Silk Road (and shut down by federal authorities in November 2014).[197] Agora's 16,137 products for sale as of September 2014 is about two hundred more listings than Silk Road 2.0 posted, and several thousand more listings than offered on the original Silk Road.[198] These listings include the perfunctory cornucopia of drugs, but unlike the original Silk Road, also include semi-automatic firearms.[199] Like the Silk Road, business on Agora is conducted in Bitcoins.[200]

B. MT. GOX AND THE RISKS OF INADEQUATE DATA SECURITY TO CONSUMERS

Another key risk to Bitcoin users is having their Bitcoins stolen by hackers due to inadequate security by Bitcoin exchanges and other

193. *Id.* at 24.

194. David Segal, *Eagle Scout. Idealist. Drug Trafficker?*, N.Y. TIMES (Jan. 18, 2014), http://www.nytimes.com/2014/01/19/business/eagle-scout-idealist-drug-trafficker.html.

195. Rachel Abrams & Sydney Ember, *U.S Prepares for Sale of Bitcoins Seized in Its Raid on Silk Road*, N.Y. TIMES (Jan. 18, 2014), http://dealbook.nytimes.com/2014/06/26/u-s-prepares-for-sale-of-bitcoins-seized-in-silk-road-raid/. These were the Bitcoins ultimately purchased by Tim Draper for use by the company Vaurum. *See supra* Section II.B.

196. *See* Andy Greenberg, *Drug Market 'Agora' Replaces the Silk Road as King of the Dark Net*, WIRED (Sept. 2, 2014), http://www.wired.com/2014/09/agora-bigger-than-silk-road/; There are a number of other online black markets with similar, but fewer, offerings. *See Darknet Marketplace Watch – Monitoring Sales of Illegal Drugs on the Darknet*, DIGITAL CITIZENS ALLIANCE, http://www.digitalcitizensalliance.org/cac/alliance/content.aspx?page=Darknet (last visited Sept. 2, 2014).

197. *See Operator of Silk Road 2.0 Website Charged in Manhattan Federal Court*, FEDERAL BUREAU OF INVESTIGATION (Nov. 6, 2014), http://www.fbi.gov/newyork/press-releases/2014/operator-of-silk-road-2.0-website-charged-in-manhattan-federal-court.

198. Greenberg, *supra* note 196.

199. *Id.*

200. *Id.*

Bitcoin-based businesses. Bitcoin-based companies and exchanges are inherently new businesses due to the recent development of the Bitcoin protocol.[201] As a result, these companies may not have the resources to fend off hackers that larger and more established institutions might.

Mt. Gox, one of the oldest Bitcoin exchanges, serves as a cautionary tale. Mt. Gox, founded in 2009 as an exchange for Magic: The Gathering cards[202] eventually became the dominant online marketplace for the purchase and sale of Bitcoins, handling 80 percent of all Bitcoin trading activity in 2013.[203] On February 25, 2014, Mt. Gox failed after hackers stole approximately 850,000 Bitcoins.[204] Mt. Gox was eventually able to recover roughly 200,000 of the stolen Bitcoins.[205] This was not the first time hackers had attacked Mt. Gox.[206] In 2011 a hacker stole $8.75 million at the contemporaneous exchange rate.[207] Mt. Gox's failure stands as a cautionary tale, not against the security of the blockchain itself, but rather against the security of the intermediaries who are not subject to the same capital holdings requirements as regular banks and stock exchanges.

C. BITCOIN AS A VEHICLE FOR TAX EVASION

Omri Marian, Assistant Professor of Law at the University of Florida Levin College of Law, proposes that cryptocurrencies such as Bitcoin will become key vehicles for tax evasion.[208] Marian believes two factors suggest that tax evaders, who have traditionally evaded taxes through offshore bank accounts in tax-haven jurisdictions, will instead use cryptocurrencies to facilitate their evasion.[209] The first factor is the increasing popularity of cryptocurrencies such as Bitcoin that function with their own free-floating

201. "The first Bitcoin specification and proof of concept was published in 2009." *Frequently asked questions*, BITCOIN.ORG, https://bitcoin.org/en/faq (last visited Feb. 11, 2015).

202. "Magic is a tradable card game (TCG) where you build your collection of cards by trading with your friends, assembling decks of cards, and battling against an opponent and their deck." *See What is Magic: The Gathering*, http://magic.wizards.com/en/what-is-magic (last visited Nov. 18, 2014). This author was particularly fond of the game between 1998–2001.

203. Trautman, *supra* note 101, at 100–01.

204. Takashi Mochizuki & Eleanor Warnock, *Mt. Gox Head Believes No More Bitcoins Will Be Found*, WALL ST. J. (June 29, 2014), http://online.wsj.com/articles/mt-gox-head-believes-no-more-bitcoin-will-be-found-1403850830.

205. *Id.*

206. *See* Dion, *supra* note 56, at 185.

207. *Id.*

208. Omri Y. Marian, *Are Cryptocurrencies Super Tax Havens?*, 112 MICH. L. REV. FIRST IMPRESSIONS 38, 39 (2013).

209. *Id.*

exchanges. Second, many governments' preferred anti-tax evasion strategy has changed from targeting tax havens that host financial intermediaries to the financial intermediaries themselves.[210]

Since the 2010 enactment of the Foreign Accounts Tax Compliance Act ("FATCA"), foreign financial institutions ("FFIs") are required to identify their U.S. account holders to the Internal Revenue Service ("IRS"), or face a 30 percent gross tax on payments received from U.S. sources.[211] This gives FFIs with substantial business in the United States the choice of either breaching their home jurisdiction's bank secrecy laws or paying a heavy tax in the United States.[212] But FATCA was enacted and negotiated with multiple intergovernmental agreements requiring foreign governments to relax their own bank secrecy laws or risk losing business with U.S. firms, thus FFIs in many jurisdictions can comply with FATCA without breaching their local bank secrecy laws.[213]

Cryptocurrencies possess a number of important advantages over traditional tax havens. First, as Bitcoins can be held in online wallets, they do not operate in a particular jurisdiction like a traditional tax haven and are not subject to taxation at the source.[214] Second, they are pseudonymous[215] and users can have as many wallets as they wish, potentially without providing any identifying information.[216] Third and most important, Bitcoin and other cryptocurrencies are not dependent on financial intermediaries such as banks.[217] Ordinarily, the IRS may compel financial institutions to produce records to be used in an investigation or trial.[218] But with Bitcoin, these financial institutions are absent and investigators would have to compel the parties to the transaction to admit their involvement.[219] Thus, Marian argues, the IRS would not have an FFI to target, and Bitcoin wallets would skirt international anti-evasion laws

210. *Id.*
211. *Id.* at 40–41.
212. *Id.* at 41.
213. *Id.*
214. *Id.* at 42.
215. *See id.; supra* Section I.B.1. Marian argues Bitcoin public key accounts are anonymous, though this Note has established that in fact these public key addresses are pseudonymous. Still, if an account holder simply made deposits in to a Bitcoin wallet and never made withdrawals, statistical analysis techniques for unmasking users would be less useful.
216. *Id.*
217. *Id.*
218. *Id.* at 41.
219. *Id.* at 42.

such as FATCA, unless they self-reported.[220] This is something a tax evader is certain not to do.

Though current U.S. bank secrecy laws[221] applied to Bitcoin exchanges could obviate this problem, more sophisticated approaches to evasion might still succeed.[222] For instance, an evader, through tax-exempt buying agents, could invest in traded securities and commodities using a Bitcoin-equity swap contract.[223] In this scenario the evader would pay the agent in Bitcoin the amount she wants to invest in a stock.[224] The agent would purchase the stock using the dollar value of the Bitcoin paid, and transfer any dividends back to the evader. As the agent is tax-exempt, he would carry no tax liability.[225] Thus tax authorities would know nothing about the involvement of the Bitcoin investor, whose income from investment would go unreported and untaxed.[226] Though this may sound convoluted, tax evasion is estimated to cost the United States between $40 to $70 billion in tax revenues each year, and is thus quite profitable to evaders.[227]

IV. ANALYSIS OF APPLICABLE LAWS, REGULATION BY GOVERNMENT AGENCIES, AND TREATMENT IN THE COURTS

This Part will describe the current regulatory landscape around Bitcoin by government agencies and how U.S. courts have dealt with cases involving Bitcoin. The first Section will examine relevant laws that may be, or are being, used to regulate Bitcoin. The second Section will examine the regulation of Bitcoin by federal agencies. The final Section will argue that U.S. courts have treated Bitcoin from a functional perspective that is best described as "you did an unlawful thing, and you are not excused because that unlawful thing was done with Bitcoin."

Statutes and regulations around Bitcoin fall into two broad categories: those that protect people who use Bitcoins (consumers, investors), and those that protect society from people who use, or might use, Bitcoins (drug dealers, terrorists, violent criminals). The first category consists of

220. *See id.* at 42.
221. This is discussed below *infra* at Section IV.A.3.
222. Marian, *supra* note 208, at 42–43.
223. *Id.*
224. *Id.* at 43.
225. *Id.*
226. *Id.*
227. *See id.* at 40 (citing JANE G. GRAVELLE, CONGRESSIONAL RESEARCH SERVICE, R40623, TAX HAVENS: INTERNATIONAL TAX AVOIDANCE AND EVASION 1 (2013)).

statutes and regulations that protect Bitcoin users from fraud and theft. The second category consists of statutes and regulations to protect society from the "Four Horsemen of the Infocalypse."[228] Notably, many of the enforcement mechanisms are directed at Bitcoin exchanges.[229] Like cash, Bitcoins sent directly to another person without an intermediary are more difficult to track than electronic transactions involving credit cards.[230] Thus, for regulators Bitcoin exchanges are the most logical institutional choke point in the Bitcoin ecosystem.

A. APPLICABLE LAWS

1. The Stamp Payments Act

As a threshold matter, it does not appear that the U.S. government is seeking to outlaw Bitcoins completely.[231] But if the government were to attempt this, many commentators believe the Stamp Payments Act of 1862 ("Stamp Payments Act") might be a potential mechanism.[232] The Stamp Payments Act was enacted when inflation caused the metal in low denomination coins to be more valuable than the face value of the coins themselves, causing people to hoard the coins and creating a shortage.[233] In order to make change for customers in the absence of these coins, companies privately issued small denominations of currencies in notes or tokens.[234] Economists and politicians feared that these private currencies were contributing to inflation and enacted the Stamp Payments Act,[235] which in relevant part states:

228. A term coined at the dawn of the information age to describe the four key threats of the information age: drugs, money laundering, child pornography, and terrorism. The Four Horsemen are used as justification for many cyber security policies and practices. Bruce Sterling, *The Cybersecurity Industrial Complex*, WIRED (Jan. 2003), http://archive.wired.com/wired/archive/11.01/view.html?pg=4.

229. *Infra* Section IV.B.1.a).

230. *See* ELWELL ET AL, *supra* note 2, at 2–3.

231. Though Senator Joe Manchin of West Virginia has called for as much. *See Manchin Demands Federal Regulators Ban Bitcoin*, JOE MANCHIN NEWSROOM (Feb. 26, 2014), http://www.manchin.senate.gov/public/index.cfm/2014/2/manchin-demands-federal-regulators-ban-bitcoin.

232. *See, e.g.*, Dion, *supra* note 56, at 174–75; Grinberg, *supra* note 6, at 186; *but see* Matthew Kien-Meng Ly, *Coining Bitcoin's "Legal Bits": Examining the Regulatory Framework for Bitcoin and Virtual Currencies*, 27 HARV. J. L. & TECH. 587, 598–99 (2014).

233. Grinberg, *supra* note 6, at 183.

234. *Id.*

235. *Id.*

> Whoever makes, issues, circulates, or pays out any note, check, memorandum, token, or other obligation for a less sum than $1, intended to circulate as money or to be received or used in lieu of lawful money of the United States, shall be fined under this title or imprisoned not more than six months, or both.[236]

Though this might appear to apply to Bitcoins, which are divisible into sums of less than one dollar, caselaw suggests that the touchstone of the Stamp Payments Act is competition with official currency.[237] Grinberg suggests that the following factors in determining whether a note or token is in competition with official currency can be derived from caselaw. Grinberg posits that the Stamp Payments Act "is unlikely to apply to anything that (1) circulates in a limited area, (2) is redeemable only in goods, (3) does not resemble official U.S. currency and is otherwise unlikely to compete with small denominations of U.S. currency, or (4) is a commercial check."[238] Though Bitcoin arguably is intended to compete with official currency, banning Bitcoin under the Stamp Payments Act would not further Congress's goal of preventing competition with U.S. coins.[239] Additionally, as the Stamp Payments Act provides criminal penalties, a court might narrowly interpret it to conclude that Congress did not anticipate Bitcoin and it is thus not within the scope of the Stamp Payments Act.[240] There have been no published court opinions interpreting the Stamp Payments Act since 1899 and it is unlikely it will be revived to outlaw Bitcoin.[241]

2. The Securities Act

The use of Bitcoin as an investment tool has brought it to the attention of the Securities and Exchange Commission ("SEC"), under the ambit of the Securities Act of 1933.[242] The Securities Act of 1933 ("Securities Act") defines securities in broad terms through a thorough list of financial instruments.[243] Courts have painted the scope of the Securities

236. 18 U.S.C. § 336 (2012).

237. *See* Grinberg, *supra* note 6, at 183–84 (citing Stettinius v. United States, 5 D.C. (5 Cranch) 573 (D.C. Cir. 1839); United States v. Monongahela Bridge Co., 26 F. Cas. 1292, 1292 (W.D. Pa. 1863) (No. 15,796)).

238. Grinberg, *supra* note 6, at 185 (citations omitted).

239. *Id.* at 187.

240. *Id.*

241. *Id.* at 190–91.

242. *See* Secs. & Exch. Comm'n v. Shavers, No. 4:13-CV-416, 2014 WL 4652121 (E.D. Tex. Sept. 18, 2014); *infra* Section IV.A.2.

243. *See* 15 U.S.C. § 77(b) (2012).

Act with a broad brush[244] and, as discussed below, have already ruled that investment schemes involving Bitcoin qualifies.[245]

Commentator Paul H. Farmer Jr. argues that Bitcoin itself could be considered a security or an investment contract, as many purchasers of Bitcoin buy the digital currency simply to speculate on its value, rather than to use it for the purchase of goods and services.[246] Yet, the SEC has not categorized the purchase of Bitcoins as buying a security or investment contract. Instead the agency has pursued people for operating Ponzi schemes[247] and selling unregistered securities[248] involving Bitcoin, not for the simple purchase of Bitcoin itself. In both these actions, the SEC was not saying that the purchase of a Bitcoin on an exchange counted as a security or investment contract, rather that schemes that involved Bitcoin in lieu of dollars were not exempt from the SEC's enforcement authority.

Commentator Derek A. Dion has argued that regulating Bitcoin exchanges under the SEC might be both logical and desirable.[249] Under this conception, Bitcoin exchanges bring together willing buyers and sellers on a virtual trading floor to, as Dion suggests, seek a future return based on the action of others.[250] Should the SEC regulate exchanges, the exchanges would have to register with the agency, file public reports (which would provide better information to purchasers and the government) and be liable for instances of fraud.[251] While these consumer protection benefits are desirable, they are inconsistent with how the SEC has chosen to frame Bitcoin: as a currency to purchase a security or investment contract, but not as the security or investment contract itself.

244. Reves v. Ernst & Young, 494 U.S. 56, 60 (1990) ("In defining the scope of the market that it wished to regulate [through the Securities Acts], Congress painted with a broad brush.").

245. *See Shavers*, 2014 WL 4652121 at *12; *infra* Section IV.C.1.

246. Paul H. Farmer Jr., *Speculative Tech: The Bitcoin Legal Quagmire & the Need for Legal Innovation*, 9 J. BUS. & TECH. L. 85, 98–104 (2014).

247. *See, e.g.*, *SEC Charges Texas Man With Running Bitcoin-Denominated Ponzi Scheme*, SECS. & EXCH. COMM'N NEWSROOM (July 23, 2013), http://www.sec.gov/News/PressRelease/Detail/PressRelease/1370539730583#.VGzeTZPF9aQ.

248. *See, e.g.*, *SEC Charges Bitcoin Entrepreneur With Offering Unregistered Securities*, SECS. & EXCH. COMM'N NEWSROOM (June 3, 2014), http://www.sec.gov/News/PressRelease/Detail/PressRelease/1370541972520#.VGzeMJPF9aQ.

249. *See* Dion, *supra* note 56, at 193–94.

250. *Id.* at 193.

251. *Id.* at 194.

3. The Electronic Funds Transfer Act

The Electronic Funds Transfer Act of 1978 ("EFTA"),[252] along with the Federal Reserve's Regulation E,[253] were enacted to establish the "rights, liabilities, and responsibilities of participants in electronic fund and remittance transfer systems" and primarily the "provision of individual consumer rights."[254] The EFTA regulates financial institutions that both hold accounts belonging to customers and perform electronic funds transfers,[255] and requires those institutions to take consumer protection measures such as reversal rights on transactions.[256]

The Bitcoin system itself does not qualify as a financial institution, as it is a decentralized program on which users may transact with each other directly.[257] Yet, Bitcoin exchanges may fall under the purview of the EFTA.[258] Imposing chargeback requirements on Bitcoin exchanges is incompatible with one of the key features and advantages of the blockchain—its irreversibility.[259] Professor Fairfield suggests that a flexible construction of the chargeback requirement through an escrow system might be enough to satisfy regulators.[260] Although such a system would not allow for formal chargebacks, an escrow system that withholds funds for a grace period would continue to serve the same consumer protection function.[261]

B. BITCOIN AND FEDERAL AGENCIES

1. Regulations to Combat the Four Horsemen: "Protecting Us From Bitcoin Users"

This Section will examine how federal agencies have enforced regulations to combat the use of Bitcoin to facilitate unlawful activities. First, it will examine the Financial Crimes Enforcement Network's ("FinCEN") regulation of Bitcoin exchanges under the Bank Secrecy Act ("BSA") to preventmoney laundering. Second, it will examine how the

252. 15 U.S.C. §§ 1601–1693 (2012).
253. 12 C.F.R. 205.1–205.20 (2012).
254. 15 U.S.C. § 1693(b).
255. 12 C.F.R. 205.1(b).
256. Reversal rights for credit card holders stem from Regulation Z of the Truth in Lending Act 12 C.F.R. §§ 226.1–226.59. Reversal rights for debit card holders come from Regulation E of the Electronic Fund Transfer Act, *supra* note 253.
257. Ly, *supra* note 1, at 599; BRITO & CASTILLO, *supra* note 10, at 36.
258. BRITO & CASTILLO, *supra* note 10, at 35–38.
259. *Id.* at 37–38.
260. *See* Fairfield, *supra* note 11, at 41–42.
261. *Id.* at 42.

FBI auctioned off some of the Bitcoins seized from the operation to shut down the Silk Road.

a) FinCEN

On March 18, 2013, the FinCEN issued guidance clarifying that certain businesses or individuals who use or make a business of exchanging, accepting, and transmitting virtual currencies were subject to the requirements of the BSA.[262] FinCEN is a bureau housed within the U.S. Department of the Treasury, in charge of enforcing the BSA, a comprehensive anti-money laundering and counter-terrorism financing statute.[263] FinCEN later amended the ruling to exempt Bitcoin miners and companies purchasing and selling virtual currency as an investment exclusively for the company's benefit from the BSA.[264]

Recently, in response to an unnamed company's actions, FinCEN ruled that Bitcoin exchanges which operate only to match sellers and buyers also qualify as money transmitters.[265] Some observers believe this administrative ruling might expand the reach of FinCEN registration requirements to Bitcoin processors which route Bitcoin from customers to merchants, creating reporting and compliance standards on essentially any company that transfers Bitcoin in commerce.[266]

As with the IRS ruling below, FinCEN's decision helps solidify the legal responsibilities associated with virtual currency, and imposes registration, reporting, and recordkeeping burdens on certain businesses. As Bitcoin and virtual currency are still in the nascent stages of their development, these requirements may be prohibitively difficult for emerging companies to adhere to. A potential solution that would allow Bitcoin startups to build enough capital to succeed while remaining

262. *FinCEN Issues Guidance on Virtual Currencies and Regulator Responsibilities*, FIN. CRIMES ENFORCEMENT NETWORK (Mar. 18, 2013), http://www.fincen.gov/news_room/nr/pdf/20130318.pdf.

263. *See What We Do*, FIN. CRIMES ENFORCEMENT NETWORK, http://www.fincen.gov/about_fincen/wwd/ (last visited Jan. 25, 2015).

264. *FinCEN Publishes Two Rulings on Virtual Currency Miners and Investors*, FIN. CRIMES ENFORCEMENT NETWORK (Jan. 30, 2014), http://www.fincen.gov/news_room/nr/pdf/20140130.pdf.

265. JAMAL EL-HINDI, FIN. CRIMES ENFORCEMENT NETWORK, REQUEST FOR ADMINISTRATIVE RULING ON THE APPLICATION OF FINCEN'S REGULATIONS TO A VIRTUAL CURRENCY PAYMENT SYSTEM 1 (Oct. 27, 2014), *available at* http://www.fincen.gov/news_room/rp/rulings/pdf/FIN-2014-R012.pdf.

266. *See, e.g.*, Pete Rizzo, *FinCEN Rules Bitcoin Payment Processors, Exchanges are Money Transmitters*, COINDESK (Oct. 27, 2014), http://www.coindesk.com/fincen-rules-bitcoin-payment-processors-exchanges-money-transmitters/.

compliant with FinCEN regulation might include exempting Bitcoin exchanges from state regulation and setting a revenue amount at which point registration is required.

b) The Federal Bureau of Investigation

In 2013, the FBI shut down Silk Road, a website that acted as a virtual black market and operated using solely Bitcoins to purchase drugs, forged documents, and even possibly assassins for hire.[267] In a dramatic arrest in the San Francisco Public Library, the Silk Road's alleged mastermind Ross Ulbricht (known online as the Dread Pirate Roberts) was captured with his laptop open.[268] Ulbricht's laptop was purportedly a hub of more than $1.2 billion worth of transactions in illicit substances and key to the FBI seizure of Ulbricht's own personal stash of Bitcoins, valued at the time at $80 million.[269]

The federal government has a responsibility to sell property seized from criminals,[270] and selling the Bitcoins at maximum value represented a unique challenge.[271] The seized Bitcoins represented a substantial percentage of the average daily trading volume of Bitcoins, and the FBI feared that dumping them all on the virtual exchanges would flood the market and depress values.[272] To prevent this, the FBI sold the Bitcoins as

267. *See* Joseph Goldstein, *Arrest in U.S. Shuts Down a Black Market for Narcotics*, N.Y. TIMES (Oct. 2, 2013), http://www.nytimes.com/2013/10/03/nyregion/operator-of-online-market-for-illegal-drugs-is-charged-fbi-says.html.

268. Segal, *supra* note 194.

269. United States v. Ulbricht, 2014 WL 901601 (S.D.N.Y. Feb. 4, 2014); Segal, *supra* note_194, (Ulbricht's computer was the command center of Silk Road); *see* infra Section IV, Part B.

270. *See Asset Forfeiture*, FED. BUREAU OF INVESTIGATION, http://www.fbi.gov/about-us/investigate/white_collar/asset-forfeiture (last visited Jan. 25, 2015).

271. *See* U.S. v. Ulbricht No. 13 Civ. 6919 (S.D.N.Y. 2014) (noting that the U.S. and Ulbricht agree that "due to the volatile market for bitcoins, the . . . Bitcoins risk losing value during the pendency of the forfeiture proceedings").

272. *See* Sydney Ember, *Another Bitcoin Auction to Be Held by U.S. Marshalls*, N.Y. TIMES (Nov. 17, 2014), http://dealbook.nytimes.com/2014/11/17/another-bitcoin-auction-to-be-held-by-u-s-marshals/.

property in a secret auction[273] with venture capitalist Tim Draper winning all 30,000 Bitcoins at issue.[274]

2. Regulations Designed for Consumer Protection: "Protecting Bitcoin Users"

The other category of government agency oversight of Bitcoins and the blockchain is focused on consumer protection. Whereas the previous Section concerned agency action to protect society from unlawful uses of Bitcoin, this Section will examine how a number of federal agencies are seeking to prevent Bitcoin users from being defrauded, manipulated, and robbed.

First this Section will examine the IRS's classification of Bitcoin as property, not currency. This is a problematic classification for the wider adoption of Bitcoin as a currency. Next it will examine the efforts of the Commodities Futures Trading Commission and Consumer Financial Protection Bureau to ensure the safety of Bitcoin related products and services to consumers. Finally it will examine the New York Department of Financial Services proposed licensing regime for companies that hold Bitcoins for customers.

a) The IRS's Classification of Bitcoin as Property is an Obstacle to the Widespread Adoption of Bitcoin as a Currency

On March 25, 2014 the IRS issued a notice stating that for federal tax purposes, the IRS would treat virtual currency as property, rather than currency.[275] The IRS will apply general tax and reporting principles that govern property transactions to those transactions involving virtual currencies such as Bitcoin.[276] This ruling is the government regulation most inapposite to the widespread adoption of Bitcoin as a currency.

---

273. The FBI arranged for an online auction for the 30,000 seized Bitcoins in a 12-hour window to submit a single sealed bid for coins broken up into lots of 3,000. The FBI was concerned with Bitcion's potential to be used for illegal activity and the agency screened potential bidders, who had to prove their identities and have at least $200,000 in cash. The FBI partially botched the sale by accidentally releasing the list of bidders. *See* Abrams & Ember, *supra* note 195.

274. Pete Rizzo, *VC Tim Draper Revealed as Silk Road Bitcoin Auction Winner*, COINDESK (July 2, 2014), http://www.coindesk.com/tim-draper-revealed-silk-road-bitcoin-auction-winner/.

275. *IRS Virtual Currency Guidance: Virtual Currency is Treated as Property for U.S. Federal Tax Purposes; General Rules for Property Transactions Apply*, INTERNAL REVENUE SERVICE (Mar. 25, 2014), http://www.irs.gov/uac/Newsroom/IRS-Virtual-Currency-Guidance.

276. *Id.*

The IRS's ruling also means that Bitcoin investors are considered stock investors, and able to take advantage of lower capital gains taxes, and certain tax write-offs, unavailable with regular property.[277] Some have praised the IRS's decision as bringing certainty to the public.[278]

Treating Bitcoin as property has profound implications for Bitcoin transactions as it creates new income tax liabilities.[279] For instance, if an individual acquired a Bitcoin for one dollar and subsequently used it to purchase a three-dollar cup of coffee, this transaction would trigger two dollars in capital gains for the purchaser of coffee (because his original investment was one dollar) and three dollars of gross income for the coffee seller.[280] Simply tracking this sort of information might be prohibitively difficult or tedious. Some commentators, such as Pamir Gelenbe, a venture partner with Hummingbird Ventures, believes this will depress adoption of Bitcoin as it requires considering capital gains when using Bitcoins to make purchases.[281] If the goal is to promote the widespread adoption of Bitcoin as a currency among the general public, the IRS's decision to treat it as property is counterproductive.

Others believe this fear is overblown. Attorney Greg Broiles, a specialist in estate planning, trust, and probate, argues only significant purchases would require these decisions.[282] For instance, it might matter if purchasing a motorcycle, but not matter if purchasing a sandwich.[283] In early 2014, Overstock.com's average order size for customers paying in Bitcoin was $226, 34 percent higher than customers paying in dollars.[284] This suggests that many people using Bitcoins to purchase goods are making purchases in between the ham sandwich and motorcycle range. Data is unavailable as to how many of these purchasers declared, or plan to declare, capital gains.

277. *See* Richard Rubin & Carter Dougherty, *Bitcoin Is Property, Not Currency, In Tax System: IRS*, BLOOMBERG.COM (Mar. 25, 2014), http://www.bloomberg.com/news/2014-03-25/bitcoin-is-property-not-currency-in-tax-system-irs-says.html.

278. *Id.*

279. *Id.*

280. *Id.*

281. *Id.*

282. Danny Bradbury, *What the IRS Bitcoin Tax Guidelines Mean For You*, COINDESK (Mar. 26, 2014), http://www.coindesk.com/irs-bitcoin-tax-guidelines-mean/.

283. *Id.*

284. Patrick Byrne, *Coinbase and Overstock.com: The Results are In!*, COINBASE BLOG (Mar. 4, 2014), http://blog.coinbase.com/post/78558321110/coinbase-and-overstock-com-the-results-are-in.

b) Commodity Futures Trading Commission

The Commodity Futures Trading Commission ("CFTC") regulates commodities futures, the markets those futures are traded on, and certain foreign exchange instruments under the Commodity Exchange Act.[285] The mission of the CFTC is to "to avoid systemic risk, and to protect the market users and their funds from fraud, manipulation, and abusive practices related to derivatives and other products that are subject to the Commodity Exchange Act."[286]

Recently, CFTC Commissioner Mark P. Wetjen stated that he believed the CFTC had the authority to regulate price manipulation in Bitcoin markets.[287] Commissioner Wetjen stated that the CFTC had this authority "because if you think of any reasonable reading of our statute, [B]itcoin classifies as a commodity."[288] To wit, the CFTC has also made the first approval of a Bitcoin derivatives trade by the firm TeraExchange.[289]

c) Consumer Financial Protection Bureau

The newly established Consumer Financial Protection Bureau's ("CFPB") mission is to "make markets for consumer financial products and services work for Americans."[290] Although the CFPB has not taken any direct action to regulate Bitcoin yet, in August 2014 the CFPB issued a consumer advisory statement warning the public of the risk of Bitcoins.[291] The advisory warned consumers about potential hackers, that Bitcoin offered fewer protections as compared to banks or debit and credit card providers, and had potentially higher costs and scams.[292] The CFPB

285. 7 U.S.C. §§ 1–27.

286. *Mission & Responsibilities*, U.S. COMMODITIES FUTURE TRADING COMM'N, http://www.cftc.gov/About/MissionResponsibilities/index.htm (last visited Nov. 29, 2014).

287. Michael J. Casey, *CFTC Commissioner Says Agency Has Authority Over Bitcoin Price Manipulation*, WALL ST. J. (Nov. 17, 2014), http://online.wsj.com/articles/cftc-commissioner-says-agency-has-authority-over-bitcoin-price-manipulation-1416265016.

288. *Id.*

289. *TeraExchange Completes First Bitcoin Derivatives Trade on Regulated Exchange*, PR NEWSWIRE (Oct. 9, 2014), http://www.prnewswire.com/news-releases/teraexchange-completes-first-bitcoin-derivatives-trade-on-regulated-exchange-278661591.html.

290. *About Us*, CFPB, http://www.consumerfinance.gov/the-bureau/ (last visited Nov. 29, 2014).

291. *See Risks to consumers posed by virtual currencies*, CFPB (Aug. 2014), http://files.consumerfinance.gov/f/201408_cfpb_consumer-advisory_virtual-currencies.pdf.

292. *Id.*

has also begun accepting complaints about virtual currency products and services, including wallets and exchanges.[293]

Most Recently, the CFPB has proposed a rule to expand consumer protections to digital wallets, potentially including digital wallets for virtual currencies.[294]

d) State Regulation of Bitcoin: New York and California

On July 17th, 2014, New York became the first state to attempt to regulate Bitcoin by introducing a proposed licensing regime to operate in the state.[295] The New York State Department of Financial Services ("NYDFS") issued proposed rules to create requirements on exchanges and companies that secure, store, or maintain custody or control of virtual currency for customers.[296] Benjamin M. Lawsky, former Superintendent of Financial Services, characterized the "BitLicense" regulatory framework requirements as a "common sense rules of the road" to further consumer protection, ensure anti-money laundering compliance, and address the unique cyber security concerns of virtual currency.[297] The regulations do not apply to virtual currency miners, software developers, or merchants and consumers who utilize virtual currency solely for the purchase or sale of goods or services, or firms chartered under the New York Banking Law to conduct exchanges with the approval of the NYDFS.[298]

The regulations were published in the New York State Register's July 23, 2014 edition to begin a forty-five-day public comment period.[299]

293. *See Submit a complaint*, CFPB, http://www.consumerfinance.gov/complaint/#money-transfer (last visited Nov. 29, 2014).

294. *See* Proposed Rule, Docket No. CFPB- 2014-0031 32–34 (Nov. 10, 2014), *available at* http://files.consumerfinance.gov/f/201411_cfpb_regulations_prepai-nprm.pdf.

295. *NY DFS Releases Proposed BitLicense Regulatory Framework for Virtual Currency Firms*, N.Y. STATE DEP'T OF FIN. SERVS. NEWS ROOM (July 17, 2014), http://www.dfs.ny.gov/about/press2014/pr1407171.html.

296. *Id.*

297. *Id.*; Former Superintendent Lawsky has specifically mentioned preventing another Mt. Gox. *See* Paul Vigna & Michael J. Casey, *BitBeat: Lawsky Outlines Changes to BitLicense*, WALL ST. J. (Oct. 14, 2014), http://blogs.wsj.com/moneybeat/2014/10/14/bitbeat-lawsky-outlines-changes-to-bitlicense/.

298. *Superintendent Lawsky Remarks on Revised Bitlicense Framework for Virtual Currency Regulation and Trends in Payments Technology*, N.Y. STATE DEP'T OF FIN. SERVS. NEWS ROOM (Dec. 18, 2014), http://www.dfs.ny.gov/about/speeches_testimony/sp1412181.htm.

299. *See NY DFS Releases Proposed BitLicense Regulatory Framework for Virtual Currency Firms*, *supra* note 295.

Perhaps in a nod to the digital nature of Bitcoin, the NYDFS also published the regulations on Reddit and Twitter.[300] Although the rules would only apply to firms doing business in the Empire State, Gil Luria, an analyst with Wedbush Securities, noted that as the state has the largest concentration of financial firms, its regulatory and enforcement framework might serve as a model for other states, or even for the SEC or Federal Reserve.[301]

Key requirements for firms to obtain a BitLicense include: capital holding requirements with a bond or trust account in US dollars, providing receipts on transactions, establishing a complaint policy, providing consumer disclosures on the risks inherent to virtual currency compared to fiat currency,[302] compiling information on transactions for anti-money laundering compliance (essentially deanonymizing the parties involved), reporting fraud or suspicious activities, maintaining cyber security programs, designating a Chief Information Security Officer and Compliance Officer, being subject to NYDFS examinations, submitting quarterly financial statements, and establishing business continuity and disaster recovery plans, with notification to NYDFS during an emergency.[303]

On December 18, 2014, Lawsky outlined revisions to the BitLicense in light of the over 3,700 public comments submitted to the original proposal.[304] In response to complaints that the cost of compliance would discourage startups and small businesses, the regulations will include a two-year transitional BitLicense for companies unable to satisfy all the requirements of a full license.[305] Additionally, companies would no longer be required to obtain the addresses and transaction data for all parties to a transaction.[306] Instead, companies would only need to obtain this type of information on their own customers and account holders.[307]

300. *Id.*

301. Cyrus Farivar, *New York state proposes sweeping Bitcoin regulations—and they're strict*, ARS TECHNICA (July 17, 2014), http://arstechnica.com/tech-policy/2014/07/new-york-state-proposes-sweeping-bitcoin-regulations-and-theyre-strict/.

302. *Fiat Currency Definition*, *supra* note 44.

303. *NY DFS Releases Proposed BitLicense Regulatory Framework for Virtual Currency Firms*, *supra* note 295.

304. *Superintendent Lawsky Remarks on Revised Bitlicense Framework for Virtual Currency Regulation and Trends in Payments Technology*, *supra* note 298.

305. *Id.*

306. *Id.*

307. *Id.*

Officials in California's Department of Business Oversight have also determined that a state law governing money transmitters may also apply to digital currencies, such as Bitcoin.[308] Spokesman Tom Dresslar indicated the requirements to obtain a California license would focus primarily on consumer protection.[309] Potential requirements include demonstrating sufficient capital to operate, having a qualified management team subject to criminal background checks, and being bonded at levels consistent with size.[310] Applicants would also have to maintain reserves equal to the amount of their outstanding money transmissions.[311] Notably, these regulations will come on the heels of a recently enacted California statute repealing a state law prohibiting the issuance of anything other than U.S. dollars in the state.[312] This statute grants Bitcoin the status of "lawful money" under state law along with rewards programs and coupons.[313]

C. BITCOIN-RELATED LITIGATION IN THE UNITED STATES

As federal and state agencies continue to tackle the regulation of Bitcoin, courts have been forced to define Bitcoin in the course of recent litigation. Below are four key cases shaping the government's stance on Bitcoins.[314]

What characterizes these cases is that judges have taken a functional view of Bitcoin and defined it on a case-by-case basis as necessary to hold defendants culpable. In the four cases below, all of the judges defined Bitcoin as money so as to subject it to the Securities Act, and state and federal money laundering statutes.

---

308. Michael B. Marois & Carter Dougherty, *California Says State Law Grants Right to Oversee Bitcoin*, BLOOMBERG.COM (Dec. 4, 2014), http://www.bloomberg.com/news/2014-12-04/california-says-state-law-grants-right-to-oversee-bitcoin.html.

309. *Id.*

310. *Id.*

311. *Id.*

312. CA A.B. 129 (2014) (repealing Section 107 of the Corporations Code).

313. Pete Rizzo, *California to Debate Bitcoin Regulation at December Meeting*, COINDESK (Dec. 5, 2014), http://www.coindesk.com/california-debate-bitcoin-regulation-december-meeting/.

314. Tanaya Macheel, *4 Court Cases Helping Shape the US Stance on Bitcoin*, COINDESK (Sept. 28, 2014), http://www.coindesk.com/4-court-cases-helping-determine-us-stance-bitcoin/.

1. SEC v. Shavers

Defendant Trendon T. Shavers founded and operated Bitcoin Savings and Trust ("BTCST"), which was subsequently declared a Ponzi scheme used to defraud investors by Magistrate Judge Amos Mazzant of the Eastern District of Texas.[315] Judge Mazzant found that Shavers used new Bitcoins received from BTCST investors to make payments on outstanding BTCST investments, while diverting investor Bitcoins for his personal use.[316] Judge Mazzant held that the investments sold by Shavers met the definition of investment contract and were thus securities, giving the court jurisdiction over the case through the Securities Act.[317]

In an earlier memorandum to establish the court's subject matter jurisdiction, Judge Mazzant declared Bitcoins to be a form of currency.[318] The Securities Act defines a "security" as "any . . . investment contract."[319] An investment contract is defined as "any contract, transaction, or scheme involving (1) an investment of money, (2) in a common enterprise, (3) with the expectation that profits will be derived from the efforts of the promoter or a third party."[320] Thus, the threshold question for the court was whether the Bitcoins invested into Shaver's Ponzi scheme qualified as an investment of money. Judge Mazzant reasoned that because Bitcoins can be used to purchase goods or services, pay for individual living expenses, and be exchanged for fiat currencies, Bitcoins constituted an investment of money.[321]

2. United States v. Faiella

In the Southern District of New York, Judge Jed Rakoff ruled in August 2014 that Bitcoins are money and were thus subject to FinCEN's regulations.[322] Defendants Robert Faiella and Charlie Shrem were accused of operating an unlicensed money transmitting business and conspiring to commit money laundering in connection with Silk Road.[323] The defendants moved to dismiss the indictment by arguing that Bitcoins did

315. *See generally* Secs. & Exch. Comm'n v. Shavers, No. 4:13-CV-416, 2014 WL 4652121 (E.D. Tex. Sept. 18, 2014).
316. *Id.* at *8.
317. *Id.*
318. Secs. & Exch. Comm'n v. Shavers, 2013 WL 4028182 at *2 (E.D. Tex. Aug. 6, 2013).
319. *Id.*
320. *Id.*
321. *Id.*
322. United States v. Faiella, 39 F. Supp. 3d 544, 545–47 (S.D.N.Y. 2014).
323. *Id.* at 545.

not qualify as "money" under racketeering laws, and that operating a Bitcoin exchange does not constitute "transmitting money" and that the defendants were therefore not "money transmitters" under 18 U.S.C. § 1960.[324]

Judge Rakoff rejected the defendants' arguments, reasoning that Bitcoin clearly qualifies as "money" or "funds" using plain meaning definitions found in the dictionary as it "can be easily purchased in exchange for ordinary currency, acts as a denominator of value, and is used to conduct financial transactions."[325] The court found this definition consistent with the legislative history of § 1960, which was passed to prevent money laundering in connection with drug dealing.[326] The court also found that Congress chose to use the term "funds" to keep up with the evolving methods of money launderers.[327] Judge Rakoff went to further define the defendant's activities as "transmitting money" and thus qualifying them as "money transmitters" and subject to FinCEN's virtual currency guidance.[328]

3. United States v. Ulbricht

The Dread Pirate Roberts, a.k.a. Ross Ulbricht[329] also challenged the applicability of money laundering laws to virtual currency.[330] Judge Katherine Forrest ruled that as an initial matter the use of Bitcoins for payment is insufficient in and of itself to state a claim for money laundering, and that anonymous transactions are not crimes.[331] Instead, the basis of the charge was the use of Bitcoin to shield unlawful activities such as narcotics trafficking and, in Ulbricht's case, computer hacking from third party discovery.[332]

Ulbricht also brought a similar argument as the defendants in *Faiella*, arguing that Bitcoins did not qualify as "funds" for the purposes of money laundering statutes.[333] Judge Forrest found Ulbricht's argument unavailing, and by using similar reasoning to Judge Rakoff, she held that "money" and "funds" were simply methods to pay for things and thus the terms covered

324. *Id.*
325. *Id.*
326. *Id.* at 545–46.
327. *Id.* at 546.
328. *Id.* at 546–47..
329. *See supra* Section IV.B.1.b).
330. United States v. Ulbricht, 31 F. Supp. 3d 540, 548 (S.D.N.Y. 2014).
331. *Id.* at 568–70..
332. *Id.*
333. *Id.*

Bitcoins.[334] Judge Forrest noted that Bitcoins' "sole raison d'etre" was to pay for things, and any other reading would be "nonsensical."[335]

4. Florida v. Espinoza

Undercover agents arrested Pascal Reid and Michell Abner Espinoza in sting operations for converting $30,000 of cash in to Bitcoin through the online marketplace LocalBitcoins.com.[336] These charges represent the first-ever state prosecution of money laundering with virtual currency.[337] The defendants were charged under Florida's anti-money laundering law, which prohibits exchanges and business transactions of over $10,000 and the state's unlicensed money transmission law which sets a yearly cap of $20,000 on payment and currency instruments.[338]

The Bitcoin Foundation has filed an amicus brief arguing that the money transmission law applies to corporations and entities qualified to do business in the state and that the Florida statute is too ambiguous on virtual currency to be enforced.[339] The defendants have also moved for dismissal invoking the IRS's guidance that Bitcoin is property, not currency.[340]

V. SUGGESTIONS FOR THE FUTURE

Two things are necessary for the wider adoption of Bitcoin: it must become easier to use as a currency, and it has to shed its negative associations to gain the trust of average consumers. Bitcoin and the blockchain can change society in many ways, but the ideas proposed in Part II of this Note all depend on wider adoption. Bitcoins must be brought into the light and seen as a useful currency, and not simply the refuge of deep web denizens.

To promote these two goals, the regulators' tasks are twofold. First, regulators must seek to create a system where Bitcoins are treated solely as a currency, allowing consumers and merchants to feel more comfortable

334. *Id.* at 570.

335. *Id.*

336. Macheel, *supra* note 314.

337. Susannah Nesmith, *Miami Bitcoin Arrests May Be First State Prosecution*, BLOOMBERG.COM (Feb. 10, 2014), http://www.bloomberg.com/news/2014-02-09/miami-bitcoin-arrests-may-be-first-state-prosecution.html.

338. Macheel, *supra* note 314.

339. Pete Rizzo, *Bitcoin Foundation Urges Court to Dismiss Charge in Florida LocalBitcoins Case*, COINDESK (Aug. 1, 2014), http://www.coindesk.com/bitcoin-foundation-urges-court-dismiss-charge-florida-localbitcoins-case/.

340. Macheel, *supra* note 314.

relying on Bitcoin as a medium of exchange. Second, regulators must de-anonymize Bitcoin to rid the currency of its (perhaps rightfully earned) negative connotations.

To accomplish the first goal, the IRS's current policy of treating Bitcoin as property must change.[341] Requiring Bitcoin users to declare capital gains taxes on all their transactions is too cumbersome. The IRS's classification is not wholly irrational given Bitcoins' current popularity as an investment device, rather than a currency. Yet subjecting Bitcoins to a capital gains tax hampers the use of Bitcoins as a means of exchange. Therefore the IRS should either set a sunset date to their current classification or some objective criteria of price stability that would reflect a change in usage of Bitcoin from an investment tool to a currency.

To accomplish the second goal, Bitcoin users should register their public key addresses to their real identities. While some of the benefits of anonymity will be lost, it is a worthwhile tradeoff to both make illicit use of Bitcoin more difficult, and to build public confidence and acceptance. This is already happening to some extent with Bank Secrecy Act registration of Bitcoin exchanges with FinCEN. While such a change may drive away some of Bitcoins' initial users in the libertarian scene, the potential of Bitcoin and the blockchain are too great to be lost in an attempt to accommodate such idiosyncratic beliefs.[342] The benefits of expanding markets and lowering transaction costs cannot be subordinated to some people's desires to maintain anonymity in transactions. For consumers who really value such anonymity, they may, as they can today, use cash. There may be no way for the government to force compliance at the individual level as users can have multiple Bitcoin wallets, and thus multiple public key addresses. But through a mix of incentives and disincentives, many users might be convinced to comply. For example, the government could create tax incentives for people to register their public key addresses with the IRS. The government could also increase punishments against defendants who used Bitcoins to facilitate the commission of a crime. There is likely no way to fully deanonymize users of the blockchain, but to the extent that it is possible, it might increase consumer confidence, and thus adoption, of Bitcoin. This would also

341. *See supra* Section IV.B.2.a).

342. Some observers already believe the libertarian community will turn away from Bitcoin as members of the community begin to understand that the blockchain is public. *See* Kim-Mai Cutler, *Marc Andreessen: "My Prediction Is That The Libertarians Will Turn on Bitcoin,"* TECHCRUNCH (Mar. 25, 2014), http://techcrunch.com/2014/03/25/marc-andreessen-my-prediction-is-that-the-libertarians-will-turn-on-bitcoin/.

allow for other benefits, such as facilitating the passing down of Bitcoins in situations of intestacy, or escheating to the state when there is no next of kin.

VI. CONCLUSION

Trust is vital to the adoption of a payment service. As Supriya Singh observes: "there is nothing inherent in a piece of paper, a plastic card or electronic information that converts it into money."[343] Ultimately Bitcoin's wider adoption, and its attendant benefits, will come down to how much consumers trust it as a stable medium of exchange and token of value.

Bitcoin's bad actors, hackers, and black markets damage this trust. Smart regulation must protect us as, and sometimes from, Bitcoin users. Unmasking actors on the blockchain will help Bitcoin shed its infamous reputation and potentially revolutionize the way we conduct business, the size of the global market, and perhaps even our conception of what ownership means.

343. Singh, *supra* note 27 at 3.4.