Louisiana Law Review

Volume 73 | Number 4
Summer 2013

The Nature of the Form: Legal and Regulatory Issues Surrounding the Bitcoin Digital Currency System

Joshua J. Doguet

The Nature of the Form: Legal and Regulatory Issues Surrounding the Bitcoin Digital Currency System

We are at the beginning of a mighty struggle for control of the Internet—the web links everything and very soon it will mediate most human activity—because the Internet has fashioned a new and complicated environment for an age-old dilemma that pits the demands of security with the desire for freedom.[1]

INTRODUCTION

Technology experts have described Bitcoin as a "masterpiece of technology"—a work of genius on par with the Mona Lisa.[2] Its beauty, though, is not outwardly apparent but instead lies at the heart of its design. Bitcoin is a digital currency system created to facilitate Internet commerce. It does this by using digital signatures and peer-to-peer technology to curtail the system's need for trusted third parties, such as financial intermediaries and central banks.[3] Bitcoin's architecture gives it several advantages over alternative payment systems: transaction costs are lower, privacy is enhanced, and inflationary pressures within the system should be reduced.[4]

"Currency . . . is exactly like religion. It's based entirely on faith."[5] This is especially the case with Bitcoin; no government, corporation, or commodity (like gold) backs the digital currency.[6] Practically, however, it is not very different from established fiat

---

1. Presentation, Misha Glenny, *Hire the Hackers!*, TED (Sept. 2011), *available at* http://threatpost.com/en_us/blogs/ted-global-misha-glenny-says-hire-hackers-091511.

2. Ari Altstedter, *Bitcoins Create Truly Democratic Policy, Followers Say*, CANADA.COM (Jul. 22, 2011) (on file with author) (quoting IT consultant, Bruce Wagner) (internal quotation marks omitted).

3. Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, BITCOIN.ORG, 1–2, 4 (2008), http://bitcoin.org/bitcoin.pdf. *See* discussion *infra* Part I.B.1–2.

4. *Id.* at 1, 6; Andy Greenberg, *Crypto Currency*, FORBES (May 9, 2011), http://www.forbes.com/forbes/2011/0509/technology-psilocybin-bitcoins-gavin-andresen-crypto-currency.html. *See* discussion *infra* Part I.B.2.

5. Matthew Yeomans, *The Quest for a Global E-Currency*, CNN (Sept. 28, 1999), http://articles.cnn.com/1999-09-28/tech/9909_28_global.e.currency.idg_1_credit-card-debit-global-internet-project/3 (quoting Jack Weatherford, author of THE HISTORY OF MONEY).

6. Video, *Bitcoin & the End of State-Controlled Money: Q&A with Jerry Brito*, REASON.COM, http://reason.tv/video/show/jerry-brito-on-bitcoin (last visited Oct. 5, 2011).

currencies.[7] Bitcoin's value fluctuates with respect to the value of other currencies, and Bitcoins can be spent anywhere a merchant is willing to accept them.[8]

In 2008, an enigmatic programmer, known only as Satoshi Nakamoto, first proposed the idea for Bitcoin on a cryptography email list.[9] Early the following year, he published the open-source software that implemented his system online.[10] Since then, a growing community of developers has maintained the software, which has been downloaded hundreds of thousands of times by individuals all over the world.[11] At one point, Bitcoin attained a circulation worth approximately $100 million.[12]

Bitcoin's positive attributes should make it attractive to consumers and merchants.[13] If it attains a critical mass with both groups, it could one day become a mainstream currency.[14] In fact, as a result of the increased access our society has to networked technology, some have intimated that the use of private, digital

---

7. "Fiat money . . . [is] not redeemable for any commodity; its status as money is conferred initially by the government but eventually by common experience." WILLIAM A. MCEACHERN, ECONOMICS: A CONTEMPORARY INTRODUCTION 732 (6th ed. 2003).

8. Paul Krugman, *Golden Cyberfetters*, N.Y. TIMES (Sept. 7, 2011, 12:20 AM), http://krugman.blogs.nytimes.com/2011/09/07/golden-cyberfetters; *Bitcoin Has Got Geeks Excited. What About Economists?*, THE ECONOMIST, Jun. 18, 2011, at 83, *available at* http://www.economist.com/node/18836780. This aspect of Bitcoin gives it an advantage over digital, community currencies that can only be used within the community that created them, such as Second Life's Linden Dollars, Facebook Credits, and World of Warcraft Gold. Reuben Grinberg, *Bitcoin: An Innovative Digital Currency*, 4 HASTINGS SCI. & TECH. L.J. 159, 171–72 (2012). *See* discussion *infra* Part III.A.

9. It is likely that the programmer's name is actually a pseudonym. Tom Simonite, *What Bitcoin Is, and Why It Matters*, MIT TECHNOLOGY REVIEW (May 25, 2011), http://www.technologyreview.com/computing/37619. The idea at the core of the Bitcoin system actually comes from "a concept called crypto-currency, which was first described in 1998 by Wei Dai." *About Bitcoin*, BITCOIN.ORG, http://bitcoin.org/about.html (last visited Sept. 20, 2011).

10. Simonite, *supra* note 9.

11. *About Bitcoin*, *supra* note 9 (listing developers that have contributed to the Bitcoin software); *Download Statistics: Bitcoin*, SOURCEFORGE, http://sourceforge.net/projects/bitcoin/files/Bitcoin/stats/timeline?dates=2010-09-22+to+2011-09-22 (last visited Sept. 20, 2011).

12. Thomas Lowenthal, *Bitcoin: Inside the Encrypted, Peer-to-Peer Digital Currency*, ARS TECHNICA, http://arstechnica.com/tech-policy/news/2011/06/bitcoin-inside-the-encrypted-peer-to-peer-currency.ars (last visited Sept. 23, 2011). As of April 10, 2013, "the value of all outstanding Bitcoins is a bit less than $3 billion." Timothy B. Lee, *Nobody Knows If There's a Bitcoin Bubble*, FORBES (Apr. 10, 2013, 12:09 PM), http://www.forbes.com/sites/timothylee/2013/04/10/nobody-knows-if-bitcoin-is-a-bubble.

13. Grinberg, *supra* note 8, at 160. *See* discussion *infra* Part I.B.2.

14. Altstedter, *supra* note 2.

currencies may prove to be the norm in the future. Even their limited success could have a substantial impact on the fate of more traditional currencies.[15]

The Bitcoin system itself is still in the early stages of development.[16] Its massive growth in a relatively short timeframe may predominantly be credited to the excitement it has given geeks and libertarians.[17] The partial anonymity provided by the system, however, has led to a concern that the currency will be increasingly used for criminal purposes.[18] Additionally, Bitcoin's lack of government oversight also gives way to another troublesome aspect of the system: a lack of consumer safeguards.[19] As one might conclude, where large sums of money flow, legal consequences are sure to follow.[20]

While Bitcoin is certainly not the first digital currency to gain traction online,[21] its innovative architecture is sure to make direct regulation impractical.[22] Even though Bitcoin raises a number of concerns that its community cannot fully address, a complete prohibition on its use would be a rash and ineffective response.[23] Ultimately, regulatory efforts directed at Bitcoin exchanges would best serve the interests of lawmakers.[24] However, due to the international nature of both the system and its actors, such controls may only be successful at the domestic level.[25]

---

15. Jennifer L. Schenker, *The Future of Money*, INFORMILO (Jan. 23, 2012), http://www.informilo.com/20120123/future-money-488; Simonite, *supra* note 9.

16. Scott Thill, *Bitcoin: A New Kind of Money That's Beyond the Reach of Bankers, Wall St., and Regulators?*, GUERNICA (Aug. 2, 2011), http://www.guernicamag.com/blog/2941/scott_thill_bitcoin_a_new_kind.

17. Schenker, *supra* note 15. *See* discussion *infra* Part III.A.

18. Cindy Cohn, *EFF and Bitcoin*, ELECTRONIC FRONTIER FOUNDATION (Jun. 20, 2011), https://www.eff.org/deeplinks/2011/06/eff-and-bitcoin. *See* discussion *infra* Part III.A.

19. *Id. See* discussion *infra* Part III.B.

20. F. Gregory Lastowka & Dan Hunter, *The Laws of the Virtual Worlds*, 92 CAL. L. REV. 1, 8 (2004).

21. WebMoney, E-Gold, Pecunix, and Liberty Reserve are digital currencies that are based on, or backed by, the price of gold. Peter C. Tucker, *The Digital Currency Doppelganger: Regulatory Challenge or Harbinger of the New Economy?*, 17 CARDOZO J. INT'L & COMP. L. 589, 598 (2009). Flooz and Beenz were corporate-backed digital currencies that failed during the "dot-com bust" due to lack of consumer interest. Mark W. Vigoroso, *Beenz.com Closes Internet Currency Business*, E-COMMERCE TIMES (Aug. 17, 2001, 6:39 PM), http://www.ecommercetimes.com/story/12892.html.

22. *See* discussion *infra* Part IV.

23. *See* discussion *infra* Part IV.A, C.

24. *See* discussion *infra* Part IV.B.

25. *Id.*

Part I of this Comment looks at the specific shortcomings of the current financial system, which prompted Bitcoin's development. It then explains how Bitcoin's architecture enables it to overcome these shortcomings. Part II reviews the legal barriers that private currencies face and analyze how they might apply to Bitcoin. Part III provides an overview of the Bitcoin economy by examining its participants and discussing the hurdles it must overcome if it is ever to become a mainstream currency. Part IV evaluates the motivations behind, and the merits of, three regulatory regimes, and also considers the Bitcoin community's likely response.[26]

I. THE FUTURE OF COMMERCE?

A. The Costs of Trust

Between his self-published whitepaper and forum posts describing the Bitcoin system's technical underpinnings, Nakamoto made his motivations for creating the currency clear: the removal of trusted third parties.[27] While third parties, like central banks and financial intermediaries, often perform valuable services in regulating and transferring currency, their presence in the system increases the cost of using it.[28]

Central banks are government institutions that, among other things, are responsible for their nations' money supply.[29] In effect,

---

26. While this Comment's primary focus is the Bitcoin system, its applicability is not so limited in scope. Taking into account the daily volatility of the Bitcoin economy, in addition to the recent security vulnerabilities that have troubled major market participants, the currency could go belly-up at any moment. Such a development, however, is of little concern to this Comment's analysis; the regulatory issues discussed herein are just as important to Bitcoin's progeny as they are to the Bitcoin system itself. Its two-and-a-half-year history has at least demonstrated that decentralized currencies are technologically feasible and likely here to stay. Noam Cohen, *Speed Bumps on the Road to Virtual Cash*, N.Y. TIMES (Jul. 3, 2011), http://www.nytimes.com/2011/07/04/business/media/04link.html; Daniel Lyons, *The Web's Secret Cash*, THE DAILY BEAST (Jun. 19, 2011), http://www.thedailybeast.com/newsweek/2011/06/19/the-web-s-secret-cash.html.

27. Nakamoto, *supra* note 3, at 1; Satoshi Nakamoto, *Bitcoin Open Source Implementation of P2P Currency*, P2P FOUNDATION (Feb. 11, 2009, 10:27 PM), http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source.

28. Nakamoto, *supra* note 3, at 1, 4. In this context, *cost* is used in a broad sense not only to include the increased financial expense of the system, but also the inconvenience and uncertainty that it entails. Additionally, many of the motivations behind Bitcoin's creation were also at work in bringing about the development of its digital currency predecessors.

29. That is, the quantity of money that circulates in the economy. FREDERIC S. MISHKIN, THE ECONOMICS OF MONEY, BANKING, AND FINANCIAL MARKETS 248, G-7 (8th ed. 2007).

the populace places a significant amount of trust in these institutions to make sound policy decisions that are detached from political influence and provide for stable economic growth.[30] Their track records, however, are not perfect.

Central banks' decisions to engage in overly expansionary monetary policy run the risk of creating high levels of inflation, thereby decreasing the nations' spending power.[31] While the United States' own central bank, the Federal Reserve (the Fed), may take this action to redistribute wealth, reduce unemployment, or finance deficits, "virtually no limit exists with respect to what [it] can do with the nation's money supply."[32] In fact, history is replete with examples of monetary policy spiraling out of control, often at the will of governments that would rather finance their expenditures by printing money, instead of, for instance, raising taxes.[33] Furthermore, central banks often rely on economic indicators and principles to guide their policy decisions; a misinterpretation of—or rigid reliance upon—either of the two can have particularly disastrous consequences.[34]

In addition to central banks, the market relies on financial intermediaries, such as banks, credit card companies, and electronic payment processors, to serve as trusted third parties between the participants in an online transaction.[35] The cost of using these

---

30. Michael D. Bordo, *A Brief History of Central Banks*, FED. RESERVE BANK OF CLEVELAND (Dec. 1, 2007), http://www.clevelandfed.org/research/commentary/2007/12.cfm.

31. MISHKIN, *supra* note 29, at 393; MURRAY N. ROTHBARD, AMERICA'S GREAT DEPRESSION 7 (5th ed. 2000), *available at* http://mises.org/rothbard/agd.pdf.

32. Lewis D. Solomon, *Local Currency: A Legal & Policy Analysis*, 5 KAN. J.L. & PUB. POL'Y 59, 65–66 (1996). Some scholars have argued that the Federal Reserve's misuse of monetary policy has contributed to the current financial crisis. John B. Taylor, *The Fed and the Crisis: A Reply to Ben Bernanke*, WALL STREET J. (Jan. 10, 2010), http://online.wsj.com/article/SB10001424052748703481004574646100272016422.html.

33. Germany experienced massive hyperinflation in the years following World War I, the rate of which ultimately exceeded one million percent and led to the collapse of its currency. Though not nearly as severe, the Latin American countries of Peru, Brazil, and Argentina each underwent a period of rapid inflation between 1980 and 1990. More recently, Zimbabwe's own problems with hyperinflation necessitated the production of banknotes with face values of $100 trillion. Their currency, too, was eventually abandoned. MISHKIN, *supra* note 29, at 614–15; Chris Bowlby, *The Fear of Printing Too Much Money*, BBC NEWS (Mar. 5, 2009), http://news.bbc.co.uk/2/hi/business/7925981.stm.

34. MISHKIN, *supra* note 29, at 408; Bordo, *supra* note 30. Bordo argues that the Federal Reserve's own strict adherence to the real bills doctrine in the 1920s led to the stock market crash of 1929, and eventually—after the Federal Reserve failed to act as a lender of last resort—to the onset of the Great Depression. Bordo, *supra* note 30.

35. Nakamoto, *supra* note 3, at 3.

intermediaries comes in the form of transaction fees, which must be borne by the buyer, the seller, or both parties, depending on the particular intermediary and the nature of the exchange.[36] Not only do the presence of these fees reduce the seller's profit margin, but they also limit the minimum practical size of the transaction to a few dollars, cutting off the possibility of smaller value transactions such as micropayments.[37]

Minimizing the risks associated with these transactions is a primary purpose of third party intermediaries.[38] The most pressing of these risks is the threat of fraud, such as when buyers attempt to reverse the charges to their account after receiving a good or service.[39] (The process of payment reversal, fraudulent or otherwise, is known as a charge-back).[40] When these allegations arise, intermediaries are unable to avoid mediating the ensuing dispute, an

---

36. David D. Friedman & Kerry L. Macintosh, *The Cash of the Twenty-First Century*, 17 SANTA CLARA COMPUTER & HIGH TECH L.J. 273, 277 (2001). Merchants typically must pay between 2% and 6% of the total purchase price to both the merchant bank and credit card company. Tucker, *supra* note 21, at 604. The popular online payment website, PayPal, charges sellers a 1.9% to 2.9% + $0.30 fee. For personal transfers funded by credit or debit cards, a 2.9% + $0.30 fee is assessed, with the sender having the option of which party will cover the cost. *Fees*, PAYPAL, https://www.paypal.com/cgi-bin/webscr?cmd=_display-fees-outside (last visited Sept. 27, 2011).

37. Friedman & Macintosh, *supra* note 36, at 277; Nakamoto, *supra* note 3, at 1; MARGARET JANE RADIN ET AL., INTERNET COMMERCE: THE EMERGING LEGAL FRAMEWORK 1194 n.9 (2nd ed. 2006); Nakamoto, *Bitcoin Open Source Implementation of P2P Currency*, *supra* note 27. A micropayment is

> a financial payment in an amount that is small relative to the transaction costs that would be incurred in making the payment using traditional payment mechanisms. . . .
>
> In the late 1990s micropayments were heralded as a breakthrough payment technology for Internet commerce, one that would make possible a broad array of new business models. Micropayments seemed to be the ideal way to sell low-value digital products for small amounts of money, amounting to a large revenue stream in the aggregate. But micropayments never caught on.

RADIN ET AL., *supra* note 37, at 1194 (footnote omitted). While their past failure may be attributed to their impracticality, other theories exist as to why they were unsuccessful. *Id.* at 1177. *See*, *e.g.*, Clay Shirky, *The Case Against Micropayments*, P2P FOUNDATION (Dec. 19, 2000), http://openp2p.com/lpt/a//p2p/2000/12/19/micropayments.html (arguing that micropayments failed "because they are a bad idea").

38. Kenneth N. Kuttner & James J. McAndrews, *Personal On-Line Payments*, 7 ECON. POL'Y REV. 35, 41 (2001).

39. *Id.*; Friedman & Macintosh, *supra* note 36, at 277. These payment reversals are both costly and inconvenient for merchants, and also unavoidable when conducted using any medium other than physical currency. Nakamoto, *supra* note 3, at 1.

40. Kuttner & McAndrews, *supra* note 38.

act that increases their overhead, the fees they impose on their customers, and, thus, the transaction costs of the entire system.[41] Because certain types of businesses tend to create higher rates of charge-backs than others, some intermediaries may even prevent their customers from patronizing them altogether, thus diminishing freedom in the market.[42] Finally, these intermediaries often retain a large quantity of the parties' personal data to decrease the number of times it is transmitted over the Internet.[43] Thus, they must also be trusted to store this information safely, keeping the parties' purchase histories private and their sensitive account information secure from the dangers of identity theft.[44]

In the Section that follows, the underlying architecture of the Bitcoin system is explored, in addition to the ways that this architecture attempts to do away with many of the costs imposed by this "trust-based model."

B. Replacing Trust with Cryptography

1. System Architecture

The Bitcoin system is comprised of a decentralized peer-to-peer network of connected computers, also known as nodes, each running a version of the Bitcoin client software.[45] In addition to providing other functions, the client serves as the user's digital wallet, which holds his supply of Bitcoins.[46]

When the client is initially run, the application generates a set of cryptographic keys that are mathematically related to one another.[47] One key is private and remains concealed on the user's computer.[48]

---

41. Tucker, *supra* note 21, at 605.

42. The best examples of these businesses are those that provide online access to either adult content or gambling; individuals who purchase adult content, or lose money through online gambling websites, often dispute the charges with their credit card company. In some cases, financial intermediaries prevent their customers from patronizing these businesses because they are illegal in the customer's jurisdiction. RADIN ET AL., *supra* note 37, at 21–22.

43. Kuttner & McAndrews, *supra* note 38, at 41.

44. Nakamoto, *Bitcoin Open Source Implementation of P2P Currency*, *supra* note 27.

45. Simonite, *supra* note 9; Lowenthal, *supra* note 12. The latest version of the Bitcoin client can be found at http://bitcoin.org.

46. J.P., *Virtual Currency*, THE ECONOMIST (Jun. 13, 2011, 8:30 PM) http://www.economist.com/blogs/babbage/2011/06/virtual-currency.

47. These keys are stored as a part of the user's wallet file and "can be transferred to another computer, for example, if [the user] upgrades." Simonite, *supra* note 9.

48. *Id.*

The other key, often referred to as a Bitcoin address, is made public; it is used to accept Bitcoin payments from other users.[49] Together, these keys serve as the user's digital signature.[50]

The client is also responsible for downloading a log of all transactions that have ever taken place on the network.[51] Because Bitcoin transactions are organized into successive groups, called blocks, this log is aptly named the blockchain.[52] The blockchain records the path of every Bitcoin as it changes hands through the network, thereby functioning as the definitive public ledger of every user's account balance.[53]

The mechanics of the Bitcoin system are best understood through the context of a transaction as it propagates through the network. When a sender initiates a transfer of Bitcoins, the amount of the transaction is encoded with the recipient's public key.[54] "By exploiting the mathematical relationship between his public and private keys," the recipient is able to prove his identity and accept the transfer.[55] The sender, meanwhile, acknowledges the transfer of these coins by signing the same transaction with his private key, thereby informing the network that the Bitcoins formerly located in his account now have a new owner.[56] The results of the exchange are then broadcast to all of the nodes connected to the Bitcoin network.[57]

However, for the network to approve the transaction, and add it to the newest block at the end of the chain, it must undergo a complex verification process that utilizes hashing and forced work.[58]

---

49. *Id.* Bitcoin addresses generally look something like this: 1LhksUu1AcqoUdehhhY99oRDPNynCszymB.

50. Nakamoto, *supra* note 3, at 2.

51. If the user's client is not connected to the Bitcoin network for an extended period of time, upon rejoining, it will download the newest blocks that were added while it was offline. Nakamoto, *supra* note 3, at 1.

52. J.P., *supra* note 46; Thill, *supra* note 16; Altstedter, *supra* note 2.

53. Danny O'Brien, *Imagine Your Computer As a Wallet Full of Bitcoins*, IRISH TIMES (Nov. 26, 2010), http://www.irishtimes.com/newspaper/finance/2010/1126/1224284180416.html (on file with author). The blockchain can be viewed online at http://blockexplorer.com.

54. J.P., *supra* note 46; Simonite, *supra* note 9.

55. J.P., *supra* note 46; Simonite, *supra* note 9. A critical aspect of this process is that "it is practically impossible—even with the most powerful supercomputer—to work out someone's private key from their public key." This ensures that an attacker may not fraudulently accept Bitcoins by masquerading as the intended recipient. Simonite, *supra* note 9.

56. Simonite, *supra* note 9; Lowenthal, *supra* note 12.

57. Altstedter, *supra* note 2.

58. Simonite, *supra* note 9. J.P. provides a simple explanation of hashing:

> A hashing algorithm converts a message into a number called a hash value . . . . If this number is big enough, it provides a unique representation of the

Using a hash value of the new and previously valid transactions, nodes race to determine the solution to a cryptographic puzzle that can only be found through extensive trial and error.[59] Once the solution is discovered, it is forwarded to the other nodes so that its accuracy can be verified.[60] If they are satisfied with the result, the new transactions are approved, and each node adds the block containing them to the end of their chain.[61] The process then begins again to confirm all Bitcoin transactions that have occurred in the interim while the nodes were solving the previous block.[62]

To incentivize users to participate in the computationally intensive task of verifying the network's transactions, the first node to discover the solution to each block is rewarded with 50 Bitcoins.[63] However, this amount is halved for every 210,000 blocks that are found, up to a total issuance of approximately 21 million

---

> original . . . . [I]t is impossible to reconstruct the original on the basis of the [hash value] alone . . . [n]or is it possible to predict what the [hash value] would be for even a slightly tweaked version of the original message . . . . As a result, hashing is . . . an irreversible process.

J.P., *supra* note 46.

59. J.P., *supra* note 46; Altstedter, *supra* note 2. Because many solutions to the puzzle exist, the chance of finding one is dependent upon the number of nodes searching and the amount of computing power they dedicate to the process. To ensure that solutions are found at a steady rate as these inputs change, a variable is correspondingly adjusted that makes it either easier or more difficult to find a solution. Lowenthal, *supra* note 12. By making the task of solution discovery "prohibitively costly to . . . individual [nodes], but relatively cheap for the network as a whole," users are effectively prevented from attempting to include forged transactions into the blockchain. J.P., *supra* note 46.

60. Simonite, *supra* note 9.

61. Altstedter, *supra* note 2. As Nakamoto explains:

> Nodes always consider the longest chain to be the correct one and will keep working on extending it. If two nodes broadcast different versions of the next block simultaneously, some nodes may receive one or the other first. In that case, they work on the first one they received, but save the other branch in case it becomes longer. The tie will be broken when the next [block] is found and one branch becomes longer; the nodes that were working on the other branch will then switch to the longer one.

Nakamoto, *supra* note 3, at 3.

62. Lowenthal, *supra* note 12.

63. The winning nodes are not only rewarded with newly minted Bitcoins. Users are encouraged to include with their payments a minimal, self-imposed transaction fee, which operates to prioritize it in the verification process. When the block is solved, the winning node also receives the sum of all transaction fees included with it. In this way, as the rate of coins that are minted decreases, the system is still able to provide participation incentives. Nakamoto, *supra* note 3, at 4; Simonite, *supra* note 9.

Bitcoins.[64] This process is known as mining, because it is meant to imitate the act of prospecting for precious minerals.[65]

2. Design Implications

Even in the abstract, the Bitcoin system is quite complex, but necessarily so. Its architecture provides it with a number of advantages over the trust-based model previously discussed, the first of which is its novel approach to counterfeit prevention.[66]

All currencies must address the problem of counterfeiting; in the context of digital currencies, it is known as the double-spending problem.[67] Because these coins are essentially nothing more than bits of data, the same coin may be copied and used multiple times.[68] While this is not a problem for other types of computer files, the ability to arbitrarily create and spend the same coin erodes one of the facets that makes money valuable: scarcity.[69]

Instead of introducing into the system a trusted intermediary to guarantee that the parties do not attempt to double-spend their coins, Bitcoin solves this problem through the use of its blockchain.[70] Because all transactions are broadcast to each node in the network and eventually find their way into this public ledger, each node has incontestable proof of the ownership and transactional history of each Bitcoin.[71] The sheer computational force required to alter the blockchain ensures that transactions cannot be undone and that the same coin cannot be spent twice.[72]

---

64. Vitalik Buterin, *Block Reward Halving: A Guide*, BITCOIN MAGAZINE (Nov. 27, 2012), http://bitcoinmagazine.com/block-reward-halving-a-guide. At the current rate of block discovery, this will occur roughly once every four years. J.P., *supra* note 46. *See* discussion *infra* Part I.B.2.

65. J.P., *supra* note 46. "The steady addition of a constant . . . amount of new coins is analogous to gold miners expending resources to add gold to circulation. In [the case of Bitcoin], it is CPU time and electricity that is expended." Nakamoto, *supra* note 3, at 4.

66. Thill, *supra* note 16.

67. BARBARA A. GOOD, PRIVATE MONEY: EVERYTHING OLD IS NEW AGAIN, FED. RESERVE BANK OF CLEVELAND (1998), *available at* http://www.clevelandfed.org/research/commentary/1998/0401.pdf; Lowenthal, *supra* note 12.

68. Lowenthal, *supra* note 12.

69. *Id.*

70. *Id.*

71. *Id.*

72. Because the verification of each block requires the hash of the previously valid blocks, an attacker would be forced to redo the work of each of the blocks after the one that involved the transaction he sought to reverse or change. Thus, he would have to eventually outpace the work of all other "honest" nodes on the network to ensure that his doctored blockchain would become the accepted standard. After each new "honest" block is added to the chain after the attack

Bitcoin also manages to provide a certain degree of privacy to its users.[73] Despite each node's access to the blockchain, transactions are kept partially anonymous because only the users' Bitcoin addresses (that is, their public keys) are published within it.[74] As no personally identifying information is tied to this address, viewers are only able to discern that one party sent a certain amount of Bitcoins to another.[75] Functionally, this is similar to the way information is released at stock exchanges: trade sizes and times are published without revealing the identity of the party buying or selling.[76] Nevertheless, the public nature of the blockchain means that transactional anonymity is not foolproof, especially if users fail to take additional precautions to maintain their privacy.[77]

---

begins, it becomes exponentially more improbable that he could accomplish this goal. Nakamoto, *supra* note 3, at 4. Nevertheless, if the attacker were able to amass a majority of the computing power on the network, his goal would become feasible. The chance of this occurring is unlikely because "[t]he combined power of the network is currently equal to one of the most powerful supercomputers in the world," and would thus prove to be exceptionally expensive. Simonite, *supra* note 9 (quoting one of Bitcoin's core developers, Jeff Garzik); J.P., *supra* note 46. Regardless, a successful attack would not subject the Bitcoin system to "arbitrary changes, such as creating value out of thin air or taking money that never belonged to the attacker. Nodes are not going to accept an invalid transaction as payment, and honest nodes will never accept a block containing them." Nakamoto, *supra* note 3, at 6. Furthermore, the fact that nodes are rewarded with Bitcoins for verifying new blocks provides an incentive for the attacker to stay honest. As Nakamoto explains:

> If [an] attacker [were] able to assemble more CPU power than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins. He ought to find it more profitable to play by the rules, such rules that favour him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth.

Nakamoto, *supra* note 3, at 4.

73. *Id.* at 6.

74. *Id.*

75. *Id.*

76. *Id.*

77. As many have pointed out, Bitcoin only provides pseudo-anonymity. Because users are still identified by their addresses, "sophisticated network analysis techniques [could be used by law enforcement] to parse the transaction flow and track down individual Bitcoin users." Adrian Chen, *The Underground Website Where You Can Buy Any Drug Imaginable*, GAWKER (Jun. 1, 2011), http://gawker.com/5805928/the-underground-website-where-you-can-buy-any-rug-imaginable (quoting core Bitcoin developer, Jeff Garzik). Indeed, "individuals sometimes post [their addresses] online in ways that can be connected to their online identities." Grinberg, *supra* note 8, at 179. *See* Fergal Reid & Martin Harrigan, *An Analysis of Anonymity in the Bitcoin System*, CORNELL UNIV. LIBRARY (2011), http://arxiv.org/pdf/1107.4524v1.pdf (concluding that by "using

Because the Bitcoin system is able to manage all of these functions itself, it reduces its users' reliance on financial intermediaries.[78] As a result, small value transactions are made possible, and the costs of doing business are reduced.[79] Furthermore, the impossibility of payment reversal, combined with the pseudo-anonymous nature of Bitcoin payments, allows users to transact with any merchant they see fit, regardless of the questionable nature of that merchant's business.[80]

In addition to reducing its dependency on financial intermediaries, the Bitcoin system also needs no central bank to function.[81] The initial issuance of the currency is accomplished through the process of mining, which rewards the system's early adopters in exchange for their help in securing and supporting the network.[82] The network also addresses the issue of regulating the supply of Bitcoins by setting a cap on the amount of Bitcoins that can ever be created at 21 million.[83] Because miners are compensated for validating blocks, an event calculated to occur roughly once

---

an appropriate network representation, it is possible to map many users to public keys" and that "casual users need to be aware of this, especially when sending Bitcoins to users and organizations they would prefer not to be publicly associated with"). One such precaution a user could take would be to generate a new address for each transaction. Nakamoto, *supra* note 3, at 6.

78. Fees, however, have not been completely eliminated. Users looking to trade the currency on Bitcoin exchanges and buyers seeking to protect themselves from fraudulent sellers through the use of escrow services must pay fees to the entities operating these businesses. *Bitcoin Has Got Geeks Excited. What About Economists?*, *supra* note 8; *Fees*, BTCROW, http://btcrow.com (follow the "Fees" hyperlink located at the bottom of the page) (last visited Oct. 1, 2011). *See* discussion *infra* Parts III.A, IV.A; *see also supra* note 63 and accompanying text.

79. Nakamoto, *supra* note 3, at 1.

80. There are other notable benefits to Bitcoin's reduction of financial intermediaries. First, the currency is essentially a digital cash system, a user does not need to rely on his credit history to qualify to use it, as is the case with credit cards. *Bitcoin Has Got Geeks Excited. What About Economists?*, *supra* note 8. Second, every Bitcoin transaction, regardless of where it is sent, typically clears within ten minutes, as opposed to the days it takes banks to complete international transfers. *Bitcoin for Business*, BITCOIN.ORG, http://bitcoin.org/en/bitcoin-for-businesses (last visited Apr. 10, 2013); Melvin Richardson, *Processing Time of Receiving an International Bank Wire Transfer*, EHOW, http://www.ehow.com /about_5456118_processing-international-bank-wire-transfer.html (last visited Apr. 10, 2013).

81. J.P., *supra* note 46.

82. Nakamoto, *supra* note 3, at 4.

83. J.P., *supra* note 46. Should the system survive long enough, this plateau in the supply of Bitcoins should occur around 2030. *Id.*

every ten minutes, the supply of Bitcoins increases at a steady, predictable rate.[84]

This aspect of the Bitcoin system should, *in theory*, keep inflation low and place investment and spending decisions on more solid ground.[85] In fact, as the number of Bitcoins issued begins to decline, their value will grow.[86] Slow and steady deflation like this is normally a destructive force in modern economies, primarily because it is unexpected.[87] Bitcoin, on the other hand, should not fall victim to this problem, because its users will anticipate the effect.[88]

II. BITCOIN'S LEGAL STATUS

When first introduced to Bitcoin, individuals often question its legality.[89] In other words, they wonder if someone may lawfully create a private currency like Bitcoin in the United States. In fact, both digital and tangible private currencies are nothing new, the latter having existed in this country for over two centuries.[90] Looking at the issue in its entirety requires an analysis of certain provisions of the United States Constitution, in addition to an obscure currency-related law—the Stamp Payments Act of 1862. An ultimate finding of legality should have a positive impact on the demand for Bitcoins because legal uncertainty tends to inhibit economic growth.[91]

A. The Constitution

The Constitution gives Congress the power "to coin money" and "regulate the value thereof"[92] while also prohibiting the states from

84. Interestingly, Milton Friedman, a Nobel laureate in economics, argued that automated systems to increase the money supply could replace the role of central banks, such as the Federal Reserve. *Id.*; MISHKIN, *supra* note 29, at 11.

85. J.P., *supra* note 46. *See* discussion *infra* Part III.B.

86. Simonite, *supra* note 9. Bitcoins "can be divided down to the eighth decimal place, which may prove increasingly useful [as] their value grows." Lowenthal, *supra* note 12.

87. Simonite, *supra* note 9 (quoting Russ Roberts, professor of economics at George Mason University).

88. *Id.*

89. Jacob Goldstein & David Kestenbaum, *What Is Bitcoin?*, NPR (Aug. 24, 2011), http://www.npr.org/blogs/money/2011/08/24/138673630/what-is-bitcoin; O'Brien, *supra* note 53.

90. GOOD, *supra* note 67. More recent examples include the Ithaca Hour and BerkShare. *See* discussion *infra* Part II.B; *see also infra* note 110 and accompanying text.

91. Grinberg, *supra* note 8, at 182; PENG HWA ANG, ORDERING CHAOS: REGULATING THE INTERNET 22 (2005).

92. U.S. CONST. art. I, § 8, cl. 5.

doing the same.[93] The Framers' definition of "money," though, was limited only to coins.[94] While the document also forbids the states from issuing paper money,[95] it is silent concerning the federal government's ability to do so.[96] Thus, the Constitution goes no further than establishing Congress's authority over the money of the United States to the exclusion of the states.[97] That is, it does not prohibit the private issuance of currency inasmuch as it makes no mention of the subject altogether.[98]

B. The Stamp Payments Act of 1862

In the latter half of the 19th century, Congress finally addressed the issue of private currency.[99] Its action stemmed from a concern that individuals were hoarding United States coins, because the value of their metal surpassed the face value of the coins.[100] The resulting shortage of coins led the issuance of private bank notes of small denomination.[101] Congress responded with the Stamp Payments Act of 1862, which attempted to combat the problem with criminal sanctions.[102] Though the Act has been amended multiple times over the past 150 years, section two remains substantively the same to this day.[103] It provides that:

---

93. "No state shall . . . coin money . . . ." U.S. CONST. art. I, § 10. "The Framers were concerned primarily with restricting the states from influencing monetary policy . . . ." LEWIS D. SOLOMON, RETHINKING OUR CENTRALIZED MONETARY SYSTEM: THE CASE FOR A SYSTEM OF LOCAL CURRENCIES 95–96 (1996).

94. SOLOMON, *supra* note 93, at 96.

95. "No state shall . . . emit bills of credit . . ." U.S. CONST. art. I, § 10.

96. Congress's authority to issue paper money was affirmed by the Supreme Court in *The Legal Tender Cases*, 79 U.S. 457 (1871). SOLOMON, *supra* note 93, at 96.

97. SOLOMON, *supra* note 93, at 95–96; Grinberg, *supra* note 8, at 182.

98. SOLOMON, *supra* note 93, at 95–96. Other acts from our nation's founding era (such as the Coinage Act of 1792, which established the United States Mint and regulated the nation's coins) are also silent about private currencies. *Id.* at 96–97.

99. Grinberg, *supra* note 8, at 183; SOLOMON, *supra* note 93, at 97–98.

100. Grinberg, *supra* note 8, at 183 (citing Thomas P. Vartanian et. al, *Echoes of the Past with Implications for the Future: The Stamp Payments Act of 1862 and Electronic Commerce*, 67 BANKING REP. (BNA) 464 (1996)).

101. Catherine Lee Wilson, *Banking on the Net: Extending Bank Regulation to Electronic Money and Beyond*, 30 CREIGHTON L. REV. 671, 693 (1997) (citing Thomas P. Vartanian et. al, *Echoes of the Past with Implications for the Future: The Stamp Payments Act of 1862 and Electronic Commerce*, 67 BANKING REP. (BNA) 464, 464 (1996)).

102. *Id.* at 693.

103. The Act was amended in 1873, 1909, 1948, and 1994. SOLOMON, *supra* note 93, at 98.

> 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.[104]

While Congress has paid some attention to the Act in the modern era, no published court opinions have interpreted its meaning since 1899.[105] Early case law, though limited, is able to provide at least *some* insight as to its application.

In *United States v. Van Auken*,[106] the Supreme Court recognized that in passing the Act, Congress primarily intended it "to prevent competition with the national currency."[107] Thus, it would not apply to anything with a limited circulation.[108] This determination in *Van Auken*, and in similar cases, rested on the fact that the notes were only redeemable in merchandise and that they did not physically resemble the nation's official currency.[109]

Modern, paper-based, private currencies such as the Ithaca Hour and BerkShare only circulate within particular communities and are only accepted at certain businesses.[110] Furthermore, their values are

---

104. 18 U.S.C. § 336 (2006).

105. Grinberg, *supra* note 8, at 190. *See* United States v. Roussopulous, 95 F. 977 (D. Minn. 1899).

106. United States v. Van Auken, 96 U.S. 366 (1877).

107. SOLOMON, *supra* note 93, at 97.

108. *Van Auken*, 96 U.S. at 367–68.

109. *Id.* at 367–68 ("Small notes payable in any specific articles, if issued, could have only a neighborhood circulation, and but a limited one there."); United States v. Monongahela Bridge Co., 26 F. Cas. 1292, 1292–93 (W.D. Pa. 1863) ("[T]hese tickets have no resemblance . . . to the coin of the United States . . . of which it was the design of the act to advance and protect. . . . They do not contain a promise to pay money, they are not the representatives of money, and therefore cannot be said to circulate, or be intended to circulate as money."); *Roussopulous*, 95 F. at 978 ("[T]he metal token . . . differs . . . plainly from all coins of the United States, and is not liable to be mistaken for any of them . . . . It does not purport to be a piece of money, or an obligation to pay money, and the obligation expressed is in terms solvable in merchandise. It cannot, therefore, have been intended to circulate as money, or to be received and used in lieu of lawful money, and does not come within the prohibition . . . ."); Grinberg, *supra* note 8, at 188 n.132.

110. GOOD, *supra* note 67; Jane O'Brien, *BerkShares Boost the Berkshires in Massachusetts*, BBC (Sept. 6, 2011), http://www.bbc.co.uk/news/world-us-canada-14814834; SOLOMON, *supra* note 93, at 98; Grinberg, *supra* note 8, at 182. The same can be said for the digital currencies discussed *supra*, note 8, as they may only be used to purchase goods in the virtual worlds of which they are a part. Grinberg, *supra* note 8, at 186. The Ithaca Hour is a local currency that was established in 1991 in Ithaca, New York, by a resident and self-described "community economist." The currency is denominated in Hours and notes come in various amounts; each Hour is equivalent to $10. Since its creation, approximately

tied to the U.S. dollar, and their smallest notes are denominated in values greater than one dollar.[111] As such, they have been able to escape criminal liability under the Act.[112]

Bitcoin is not geographically constricted like these currencies. Its supporters are pushing for it to be a widely accepted medium of exchange on the Internet, an aspect that could lead a court to find that Bitcoins, indeed, "circulate as money."[113] Furthermore, Bitcoin was designed to be economically superior to government-backed currencies, and those who transact in Bitcoins necessarily do so to the exclusion of the U.S. dollar.[114] In this sense, some may see Bitcoin as competing with the nation's currency.[115] Finally, because Bitcoin is able to restore the practicality of micropayments, there can be little doubt that it will be used to engage in transactions far below the Act's one-dollar threshold.[116]

There are many valid counterarguments, however, that Bitcoin would fall outside of the Act's scope. First, because Bitcoins are primarily intended for Internet transactions, they do not actually compete with the currency of the United States; it may be more accurate to say that digital currencies, like Bitcoin, compete with online payment processors, such as PayPal and Dwolla, and credit cards.[117] Second, unlike the previously mentioned community currencies, Bitcoin's value is not pegged to the dollar, but is determined by supply and demand.[118] As such, an argument can be made that Bitcoin transactions, no matter how small, are not "for a less sum than $1," because Bitcoins are not denominated in dollars.[119]

In evaluating how the Stamp Payments Act could apply to digital currencies in general, scholars have suggested that in order

---

$63,000 worth of Hours have been issued. GOOD, *supra* note 67. The BerkShare is another community currency that circulates in the BerkShare region of Massachusetts. Created in 2006, it is accepted at over 400 local businesses. The currency comes in values of 1, 5, 10, 20, and 50; each BerkShare is worth 95% of $1; that is, they represent a 5% discount. *What Are BerkShares?*, BERKSHARES, INC., http://www.berkshares.org/whatareberkshares.htm (last visited Feb. 9, 2012).

111. GOOD, *supra* note 67; O'Brien, *supra* note 110.

112. GOOD, *supra* note 67; Grinberg, *supra* note 8, at 186 (citing Ellen Graham, *Community Groups Print Local (and Legal) Currencies*, WALL STREET J., Jun. 27, 1996, at B1).

113. Grinberg, *supra* note 8, at 187; 18 U.S.C. § 336 (2006).

114. *See* discussion *supra* Part I.B.2.

115. Grinberg, *supra* note 8, at 187.

116. *Id. See* discussion *supra* Part I.B.2.

117. Grinberg, *supra* note 8, at 187.

118. *See* discussion *infra* Part III.A.

119. Grinberg, *supra* note 8, at 186; 18 U.S.C. § 336 (2006).

for something to "circulate as money," it must posses the physical characteristics of money.[120] This argument is supported in the text of the Act, which refers to "any note, check, memorandum, token, or other obligation."[121] Each of these items is a "physical manifestation of currency."[122] As a digital currency, Bitcoin is completely intangible, a fact that could exclude it from the Act's reach.[123]

Perhaps the strongest textual argument is that each of the prohibited items in the list above is an obligation, as is indicated by the final phrase "or other obligation."[124] Unlike many of the items at issue in the cases interpreting the Act, Bitcoins are not obligations because no "entity has promised to provide something in return for [them]."[125] Thus, even if an argument were made that Bitcoins are "digital tokens," they would fall outside the list's range, as they are not obligations.[126]

Finally, because the Act was passed to address a shortage of United States coins, its legislative purpose has long since vanished.[127] Although it was stylistically amended as recently as 1994, Congress did not add "digital currency" or any similar term to the list of proscribed items.[128] Their failure to do so could certainly indicate that they did not intend for the Act to apply to such things.[129] Furthermore, it is not likely that when the Act was

---

120. Brian W. Smith & Ramsey J. Wilson, *How Best to Guide the Evolution of Electronic Currency Law*, 46 AM. U. L. REV. 1105, 1110 (1997); 18 U.S.C. § 336.

121. Grinberg, *supra* note 8, at 188; 18 U.S.C. § 336.

122. Grinberg, *supra* note 8, at 188.

123. Although, "[i]f faced with an ether-based payment system . . . a court may dismiss the relevance of distinctions based on physical attributes and instead may focus on similarities arising from non-physical properties, such as the rights and obligations of the holders." Smith & Wilson, *supra* note 120, at 1110.

124. Grinberg, *supra* note 8, at 188–89 n.132; 18 U.S.C. § 336.

125. Grinberg, *supra* note 8, at 189. *See* United States v. Van Auken, 96 U.S. 366, 367 (1877) (item was an obligation from The Bangor Furnace Company that could be redeemed for 50¢ in goods at their store); United States v. Monongahela Bridge Co., 26 F.Cas. 1292, 1292 (W.D. Pa. 1863) (item was a paper ticket for one trip across the Monongahela Bridge); United States v. Roussopulous, 95 F. 977, 978 (D. Minn. 1899) (item was a metal token from Clark & Boice Lumber Company that could be redeemed for 50¢ in merchandise).

126. Grinberg, *supra* note 8, at 189.

127. Wilson, *supra* note 101, at 693.

128. Reuben Grinberg, *Bitcoin: An Innovative Digital Currency* 28–29 (Yale Law School, Working Paper, 2011) (on file with author) (later published as Grinberg, *supra* note 8).

129. *Id.* at 29. Their inaction could also "be taken as a sign that Congress intended to breathe new life into the Act, reaffirming and extending its prohibition to all twentieth century obligations—including electronic ones." Kerry Lynn Macintosh, *The New Money*, 14 BERKELEY TECH. L.J. 659, 672 n.78 (1999). Even if this were the case, Bitcoins would still side-step proscription, as they are not obligations.

originally written, lawmakers could have intended for it to encompass digital currencies, a machination of technology that would not be conceived for over 100 more years.[130]

In lieu of the continuing expansion in the number of digital currencies, the Treasury Department has requested that the Act be interpreted narrowly by the Department of Justice; some scholars have even called for its repeal.[131] Regardless of the Act's continued existence, Bitcoin is unlikely to be challenged by it, as the arguments for bringing Bitcoin within its purview are overwhelmingly outweighed by the arguments against doing so. Indeed, digital currencies have been around in some form or another for over a decade and neither their creators nor their users have yet to be prosecuted under the Act—nor should they be worried about this possibility.[132]As such, the remainder of this Comment surveys the activities occurring within the Bitcoin economy, with a focus on how regulators should respond to its more "concerning" aspects.

III. THE BITCOIN ECONOMY

A. Market Participants

In Bitcoin's short lifespan, it has amassed a base of approximately 10,000 users, including several hundred merchants that currently accept the digital currency as a method of payment.[133] However, the currency has yet to find adoption with any mainstream retailers, such as Amazon.com.[134] Despite the fact that the overwhelming majority of these merchants are small businesses that operate in the technology sector,[135] the goods and services provided by the remainder are incredibly diverse.[136] Indeed, they run the gamut from sellers of clothing, home, and car accessories, to brick-and-mortar establishments, like restaurants, hotels, and travel companies.[137]

---

130. Macintosh, *supra* note 129, at 672.
131. Wilson, *supra* note 101, at 693; Macintosh, *supra* note 129, at 672 n.78.
132. Smith & Wilson, *supra* note 120, at 1111.
133. J.P., *supra* note 46.
134. Daniel Roberts, *The Clock Is Ticking on Bitcoin*, CNN MONEY (Jun. 17, 2011), http://tech.fortune.cnn.com/2011/06/17/the-clock-is-ticking-on-bitcoin.
135. *Id.* For example, these businesses include providers of Internet services such as website design and development, virtual private and dedicated servers, domain names, VoIP, and security, in addition to software, online auctions, technical consulting, and a number of other digital products. *Trade*, BITCOIN WIKI, https://en.bitcoin.it/wiki/Trade (last visited Oct. 2, 2011) (listing online and real world businesses that currently accept Bitcoin).
136. *Trade*, *supra* note 135.
137. Goldstein & Kestenbaum, *supra* note 89; *Trade*, *supra* note 135. New York's Meze Grill, located in midtown Manhattan, has garnered significant

Three attorneys located in the United States have even offered to provide legal services in exchange for Bitcoins.[138] Furthermore, a handful of organizations (including a few nonprofits) accept donations in Bitcoins; among these is the notorious whistle-blowing website, Wikileaks, and the hacker group Lulz Security.[139]

Businesses in the financial sector also make up an important part of the Bitcoin economy. While they range from providers of escrow and online wallet services, to mobile payment systems, perhaps the most crucial of these are Bitcoin exchanges.[140] By matching buyers with sellers, these businesses facilitate the conversion of Bitcoins to (and from) at least two dozen established fiat currencies, such as the dollar, euro, and pound sterling.[141] For individuals looking to

---

attention in the news media for accepting Bitcoins. *See*, *e.g.*, Roberts, *supra* note 134.

138. *Trade*, *supra* note 135.

139. *Donation Accepting Organizations and Projects*, BITCOIN WIKI, https://en.bitcoin.it/wiki/Donation-accepting_organizations_and_projects (last visited Oct. 2, 2011) (listing notable organizations that accept Bitcoin donations); Eria Ogg, *Hackers Steal More Customer Info From Sony's Servers*, CNET NEWS (Jun. 2, 2011), http://news.cnet.com/8301-31021_3-20068414-260/hackers-steal-more-customer-info-from-sony-servers. Near the beginning of 2011, the Electronic Frontier Foundation began accepting Bitcoin donations but abandoned the practice six months later as a result of the "untested legal concerns" Bitcoin creates. Rainey Reitman, *Bitcoin: A Step Toward Censorship-Resistant Digital Currency*, ELECTRONIC FRONTIER FOUNDATION (Jan. 20, 2011), https://www.eff.org/deeplinks/2011/01/bitcoin-step-toward-censorship-resistant; Cohn, *supra* note 18. Nakamoto was undoubtedly very concerned about the negative attention Bitcoin was receiving after Wikileaks began accepting the digital currency to support its activities. Before essentially disappearing from the Internet, one of his final public posts contained the message: "WikiLeaks has kicked the hornet's nest, and the swarm is headed towards us." Satoshi Nakamoto, *Re:PC World Article on Bitcoin*, BITCOIN FORUM (Dec. 11, 2010, 11:39 PM), https://bitcointalk.org/index.php?topic=2216.msg29280#msg29280; Joe Duncko, *Who Created Bitcoins?*, WRITTEN BY JOE DUNCKO (Jun. 20, 2011), http://joeduncko.com/2011/06/20/who-created-bitcoins.

140. *Trade*, *supra* note 135. As opposed to the Bitcoin client, which stores the user's currency only on their computer, online wallet services store Bitcoins in a centralized location so that any web-connected device can have access to them. In a way, they may be thought of as Bitcoin banks, although they do not perform any traditional banking services. *FAQ*, FLEXCOIN, http://www.flexcoin.com/15.html (last visited Oct. 2, 2011); J.P., *supra* note 46.

141. *Bitcoin's Network of Exchanges Expands*, BITCOIN MONEY (Sept. 6, 2011), http://www.bitcoinmoney.com/post/9872899440/global-exchange-trading-expands. These exchanges also allow traders to engage in arbitrage opportunities. Vitalik Buterin, *BTC Trader: Bitcoin Arbitrage Made Easy*, BITCOIN MAGAZINE (Nov. 2, 2012), http://bitcoinmagazine.com/btc-trader-bitcoin-arbitrage-made-easy. *Bitcoin Arbitrage Opportunities*, NYSE-GROUP.DE, http://nyse-group.de/bitcoin-arbitrage (last visited Oct. 2, 2011).

transact in Bitcoins without having to mine for them, these exchanges provide the simplest method of obtaining the digital currency and also the easiest way to convert Bitcoins back to other fiat currencies.[142] The number of operating exchanges continues to expand and the volume of transactions that pass through them is fairly substantial.[143] For example, Mt. Gox, one of the more popular exchanges, has moved $70 million in funds in the last six months alone.[144]

As far as individual users go, those holding Bitcoins do so for a number of different reasons. Categorically, they vary from privacy, technology, and cryptography enthusiasts to speculators and government-mistrusting individuals who would rather hold their assets in a vehicle other than state-controlled fiat money.[145] One group of Bitcoin users, however, has received significantly more attention by the media than others—criminals.[146]

Due to the partial anonymity that the Bitcoin system provides,[147] many have raised the issue of its ability to facilitate a multitude of illegal activities, including money laundering, tax evasion, the sale of stolen credit cards, and the funding of online gambling (in jurisdictions where it is prohibited).[148] For the most part, the amount of criminal activity occurring with digital currencies is, at this point, mere conjecture and undoubtedly subject to the hyperbolic tendencies of the press.[149] The use of Bitcoins to purchase illegal drugs through the Internet, however, is very real.[150]

The Silk Road Marketplace is a website that allow its users to buy and sell anything, from marijuana and heroin to LSD and ecstasy.[151] This online black market operates on the anonymizing

---

142. J.P., *supra* note 46.

143. *Bitcoin's Network of Exchanges Expands*, *supra* note 141.

144. *Mt. Gox (USD)*, BITCOIN CHARTS, http://bitcoincharts.com/markets/mtgoxUSD_trades.html (last visited Oct. 2, 2011).

145. Grinberg, *supra* note 8, at 165.

146. *See*, *e.g.*, Chen, *supra* note 77; Tom Cheredar, *Forget Piracy, U.S. Government Is Going After Bitcoin*, VENTUREBEAT (Jun. 8, 2011), http://venturebeat.com/2011/06/08/government-crackdown-on-bitcoin; Jerry Brito, *Online Cash Could Challenge Governments, Banks*, TIME: TECHLAND (Apr. 16, 2011), http://techland.time.com/2011/04/16/online-cash-bitcoin-could-challenge-governments; Jack Hough, *The Bitcoin Triples Again*, SMARTMONEY (Jun. 10, 2011), http://www.smartmoney.com/invest/stocks/the-bitcoin-triples-again-1307638613180; J.P., *supra* note 46.

147. *See* discussion *supra* Part I.B.2.

148. Brito, *supra* note 146; Cohn, *supra* note 18.

149. Tucker, *supra* note 21, at 618.

150. Chen, *supra* note 77.

151. *Id.* Even this black market has limits, though. Its terms of service bans "anything who's [sic] purpose is to harm or defraud, such as stolen credit cards, assassinations, and weapons of mass destruction." *Id.*

network, Tor,[152] which allows the site to obfuscate both its location and the identity of its administrators.[153] Set up in much the same way as traditional e-commerce websites, visitors peruse the hundreds of items listed for sale, in addition to reviews that have been written about their sellers by previous buyers.[154] After adding items to their shopping carts, buyers are required to pay with the only currency the website accepts: Bitcoins.[155] Possibly, the most alarming aspect of Silk Road is that a significant amount of the market's sellers are located in the United States and Canada.[156]

In June of 2011, Senators Charles Schumer of New York and Joe Manchin of West Virginia sent a letter to United States Attorney General Eric Holder and Drug Enforcement Agency Administrator Michele Leonhart. They urged the officials to immediately shut down Silk Road.[157] In the letter, the Senators referenced the "untraceable peer-to-peer currency known as Bitcoins" as the sole method of payment accepted by the website.[158] While their description of the digital currency as "untraceable" is somewhat exaggerated,[159] it has only increased the unfavorable attention that Bitcoin has received.[160]

---

152. On the project's homepage, Tor is described as:

> free software and an open network that helps you defend against a form of network surveillance that threatens personal freedom and privacy . . . by bouncing your communications around a distributed network of relays run by volunteers all around the world: it prevents somebody watching your Internet connection from learning what sites you visit, and it prevents the sites you visit from learning your physical location.

TOR, https://www.torproject.org (last visited Oct. 4, 2011).

153. Chen, *supra* note 77.

154. *Id.*

155. The drugs are delivered through the United States Postal Service, and Silk Road encourages its merchants to disguise their shipments and vacuum seal items that could be detected through smell. *Id.*

156. *Id.*

157. Letter from Charles Schumer & Joe Manchin, United States Senators, to Eric Holder, Attorney General of the United States (Jun. 6, 2011), *available at* http://manchin.senate.gov/public/index.cfm/2011/6/manchin-urges-federal-law-enforcement-to-shut-down-online-black-market-for-illegal-drugs.

158. *Id*. Senator Schumer has also described Bitcoin as "an online form of money laundering used to disguise the source of the money and disguise who is both buying and selling the drug." Brett Wolf, *Bitcoin Exchanges Offer Anti-Money Laundering Aid*, REUTERS, Jun. 15, 2011, http://uk.reuters.com/article/2011/06/15/financial-bitcoin-idUKN1510930920110615.

159. *See* discussion *supra* Part I.B.2; *see also supra* note 77 and accompanying text.

160. *See*, *e.g.*, Keir Thomas, *Could the Wikileaks Scandal Lead to New Virtual Currency*, PC WORLD (Dec. 10, 2010), http://www.pcworld.com/businesscenter/article/213230/could_the_wikileaks_scandal_lead_to_new_virtual_currency.html; Ogg, *supra* note 139.

B. Likelihood of Success

Excepting any challenges to Bitcoin's legality,[161] however unlikely, there are a number of hurdles that the Bitcoin economy must overcome if the currency that drives it is to remain useful. The first of these hurdles involves economic stability.

In the Bitcoin economy, price volatility is still a huge problem. Both in the short and long term, the currency has been prone to significant value fluctuations, arguably the result of ideological enthusiasm and widespread speculation.[162] Such fluctuations make it difficult, if not impossible, for merchants to accurately price their products in Bitcoins.[163] This, in turn, has a negative effect on the number of businesses that are willing to accept the currency as a method of payment.[164] Indeed, the Bitcoin system's continued existence heavily depends on its ability to attract the critical mass of merchants and consumers necessary to make dealing in the currency practical.[165]

Bitcoin's incredible upward leaps in value, at times, have led to the fear that it is being used primarily to speculate; that is, individuals have been buying Bitcoins only as an investment vehicle.[166] The digital currency's approach to capping its money supply exacerbates this problem: the fact that Bitcoins are likely to be worth more in the future incentivizes hoarding, thereby

---

161. *See* discussion *supra* Part II.

162. *Bitcoin Has Got Geeks Excited. What About Economists?*, *supra* note 8; Timothy B. Lee, *The Bitcoin Bubble*, BOTTOM UP (Apr. 18, 2011), http://timothy blee.com/2011/04/18/the-bitcoin-bubble. In terms of dollars, a "Bitcoin has been worth as little as a few pennies and as much as $33, and after seeming to stabilize at around $14 over the summer [of 2011], Bitcoin's value tumbled by almost 50 percent in a matter of days in August." James Surowiecki, *Cryptocurrency*, MIT TECH. REVIEW (Aug. 23, 2011), http://www.technology review.com/computing /38392. Media coverage has had a tremendous impact on its valuation, at times, causing tenfold jumps over short time periods. *Id.*

163. Cohen, *supra* note 26.

164. Surowiecki, *supra* note 162.

165. Altstedter, *supra* note 2. This is a difficult task, because

> currencies are subject to massive network effects . . . . People who hold obscure currencies have to waste time and money converting it to a more popular currency before they can perform everyday transactions. And [those] who conduct business in multiple currencies . . . also have to worry about exchange rate risk . . . .

Lee, *supra* note 162. Undoubtedly, to get more merchants and consumers to accept the currency, Bitcoin's developers will also have to make it more user-friendly and able to be integrated with current e-commerce systems. Rick Falkvinge, *Bitcoins Four Hurdles: Part One – Usability*, FALKVINGE & CO. ON INFOPOLICY (Jun. 4, 2011), http://falkvinge.net/2011/06/04/bitcoins-four-hurdles-part-one-usability.

166. Surowiecki, *supra* note 162.

preventing their use as a medium of exchange.[167] Furthermore, because Bitcoin is not the legal tender of any country, there is no reason that its users would *need* to start spending them.[168]

Another hurdle is security. In the past few months, incidents have occurred in the Bitcoin economy that have decreased confidence in the currency. Two incidents resulted in the theft of Bitcoins,[169] while another led to a massive sell-off and subsequent price crash of the digital currency.[170] While all were allegedly the result of security breaches, a failure of the Bitcoin software itself was not directly responsible; improvements to the software, however, could have at least reduced the damage of one of the incidents.[171] Thus, Bitcoin's expansion also depends on its

---

167. *Id.* That is, the *purpose* of currencies is to facilitate transactions, not increase the wealth of its users. Krugman, *supra* note 8.

168. That is, individuals cannot hold all of their legal tender, such as their U.S. dollars, forever. Eventually bills must be paid and food must be purchased using it. This is not the case with Bitcoins. Surowiecki, *supra* note 162. Bitcoin also faces a number of other economic hurdles. For one, some critics have expressed doubt that Bitcoin could expand enough to serve the needs of a much larger economy. *See*, *e.g.*, Presentation, Dan Kaminsky, *Some Thoughts on Bitcoin*, SLIDESHARE, *available at* http://www.slideshare.net/dakami/bitcoin-8776098 (last visited Oct. 4, 2011). Others point to the fact that Bitcoin's removal of intermediaries means that there are no institutions to perform the necessary functions of borrowing and lending. Furthermore, even if there were, Bitcoin's irreversible transactions mean that there would be no guarantee the parties would get their money back. *Bitcoin Has Got Geeks Excited. What About Economists?*, *supra* note 8.

169. The first occurred when one of the most popular online wallet services, MyBitcoin.com, mysteriously went offline for a week during the summer of 2011. When it later resurfaced, the site's operator claimed that it had been broken into, and an enormous amount of Bitcoins had been stolen. At the time of the incident, the service was holding approximately $250,000 of the currency for its customers. There is some suspicion in the Bitcoin community that the security breach was a sham perpetuated by the site's operator(s) to effectively steal the Bitcoin holdings of its customers. Adrianne Jeffries, *MyBitcoin.com Is Back: A Week After Vanishing with at Least $250 K. Worth of BTC, Site Claims It Was Hacked*, BETABEAT (Aug. 5, 2011, 7:03 AM), http://www.betabeat.com/2011/08/05/mybitcoin-disappeared-with-bitcoins. The second incident was the result of an unknown hacker gaining access to the computer of a Bitcoin user and stealing his digital wallet. The wallet contained $500,000 worth of Bitcoins, based on their trading value at the incident. Cohen, *supra* note 26.

170. This incident occurred in June of 2011 at the Mt. Gox exchange. Cohen, *supra* note 26.

171. Indeed, these improvements have since been implemented. On September 23, 2011, the developers released version 0.4.0 of the Bitcoin client. The update allows users to encrypt their wallets with a passphrase. Doing so means that even if a hacker were to steal a user's wallet, he would not automatically be able to spend that user's Bitcoins without breaking through this added layer of protection. *Bitcoin Version 0.4.0 Released*, BITCOIN.ORG (Sept. 23, 2011), http://bitcoin.org/releases/2011/09/23/v0.4.0.html.

community's ability to increase protective measures and ease its users' minds.

What is left to be seen is whether Bitcoin's provision of lower fees and pseudo-anonymous transactions will be valuable to the average consumer.[172] The digital currency does not need to become mainstream in order to be successful; it could find plenty of use in niche markets, such as those that cater to technologists, providers of digital goods, and participants in virtual worlds.[173] It could also explode in popularity with those planning to use it for nefarious purposes.[174] At this point, then, its fate ultimately rests in the direction taken by those behind the wheel. For a decentralized currency like Bitcoin, that means its users.[175]

IV. ROADS TO REGULATION

Senators Schumer and Manchin's letter to officials in the Department of Justice and Drug Enforcement Agency has done nothing but draw speculation that in the future, Bitcoin will in fact be subjected to government regulation or, more drastically, prohibition.[176] Even though Bitcoin is not the first digital currency to be the target of government action,[177] many of the challenges it presents are wholly new. Its distributed nature and lack of corporate backing means that there is no central database to shut down and no company officers to hold accountable.[178] Because a community of open source developers maintains its code, if some developers were to leave the project, through choice or coercion, others would likely take up the reigns. The issues, however, go much deeper than this.

As many in the Bitcoin community are quick to remind those participating in discussions on this topic, the United States does not exercise preeminent control over the medium through which

---

172. *See* discussion *supra* Part I.B.2.

173. Surowiecki, *supra* note 162; Grinberg, *supra* note 8, at 171–72.

174. Goldstein & Kestenbaum, *supra* note 89. *See* discussion *supra* Part III.A.

175. Goldstein & Kestenbaum, *supra* note 89.

176. Cheredar, *supra* note 146; Mike Young, *Should Bitcoins Become Illegal Digital Currency?*, ATTORNEY MIKE YOUNG'S INTERNET LAW FIRM, http://mikeyounglaw.com/bitcoin-digital-currency/ (last visited Oct. 25, 2011).

177. *See infra* note 214 and accompanying text. The F.B.I. conducted an investigation into the online currency, Flooz, after they determined that international criminals were purchasing it using stolen credit cards. This, in addition to a lack of consumer interest, may have ultimately contributed to its failure. Bob Tedeschi, *E-Commerce Report: Seller of Online Currency May Have Been Victim of Fraud*, N.Y. TIMES (Aug. 27, 2001), http://www.nytimes.com/2001/08/27/business/e-commerce-report-seller-of-online-currency-may-have-been-victim-of-fraud.html.

178. *See* discussion *supra* Part I.B.

Bitcoins travel: the Internet itself.[179] Because the latter is able to cut through invisible geographic boundaries, it erodes the traditional jurisdictional notions upon which laws and their enforcement are founded.[180] As such, in dealing with an inherently elaborate and distributed system like Bitcoin, there may be no way to exercise perfect control over it. This does not mean, however, that effective control is out of the question. Even partial control over the Bitcoin system could have considerable effects.[181]

The goal of this Part is to provide insight as to what sort of regulatory regime would be most effective at addressing the concerns presented by the Bitcoin system, while also taking into account the community response they would elicit.[182] Three regimes are evaluated: self-regulation (representing the current state of the Bitcoin system), intermediary regulation, and prohibition. Each regime represents a distinct position on a regulatory scale with respect to the level that it would constrain the use of Bitcoins, and each entails a different set of benefits and costs.

A. Self-Regulation

For regulating the Internet, many believe that self-regulation is the most desirable solution.[183] That is to say, social norms[184] and market mechanisms should govern the relationships between users

---

179. fonestar, Comment to *Guest Post: What Every Libertarian Should Know About Bitcoin*, ZERO HEDGE (Apr. 1, 2013, 8:45 PM), http://www.zerohedge.com/news/2013-04-01/guest-post-what-every-libertarian-should-know-about-bitcoin; John Perry Barlow, *A Declaration of the Independence of Cyberspace* (1996), *available at* https://projects.eff.org/~barlow /Declaration-Final.html (asserting that no government exercises sovereign authority over the Internet).

180. David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1367 (1996).

181. LAWRENCE LESSIG, CODE: VERSION 2.0, 73 (2006).

182. For the remainder of this Comment, *small-scale criminal activities* are defined as the use of Bitcoins to purchase illegal items of relatively low value (such as drugs, child pornography, and other black market goods) and its use in making contributions to criminal organizations. Additionally, *large-scale criminal activities* refer to the use of Bitcoins to launder money, evade taxes, or move any other suspiciously large sums of money.

183. ANG, *supra* note 91, at 59. *See also* Barlow, *supra* note 179.

184. Social norms are the constraints on behavior that are imposed by either society as a whole or by the members within a specific community. Broadly, they may be defined as what actions are acceptable and what actions are not acceptable. Unlike sanctions for violating the law (which come from the State), in the case of norms, sanctions come from the community itself. Those who fail to abide by their community's norms could end up ostracized, filtered, or stigmatized. LESSIG, *supra* note 181, at 340–41, 124.

without the need for state intervention.[185] In practice, self-regulation via norms was sufficient during the Internet's early days when the medium was primarily used as a research tool for government agencies and academic institutions.[186] Since then, however, the Internet's landscape has transformed into one dominated by commerce.[187] In this new era, some feel that government involvement is required to enforce the rights of transacting parties.[188]

The Bitcoin system exemplifies the Internet's commercial evolution; indeed, the system is premised on the idea that software can be designed to address the shortcomings of the market.[189] However, Bitcoin's architectural constraints have, in fact, created their own problems. In turn, market mechanisms have developed to provide a solution without state intervention.

More specifically, Bitcoin transactions are practically irreversible.[190] Considering the amount of computing power that secures them, they are essentially etched in stone. While such architectural constraints are a boon to honest merchants, inasmuch as they are protected from the practices of fraudulent buyers, Bitcoin has no architectural constraints which protect honest buyers from fraudulent merchants. To provide these consumers with such protection, reputation systems and escrow services have naturally developed as a self-regulatory response.[191]

Reputation systems are an instrument through which legitimate business practices are enforced. If a merchant defrauds a buyer, then the buyer can complain about him in a public forum.[192] Thus, the community can punish the merchant by warning others of his malfeasance and encouraging them to refuse to patronize his business.[193] As a result, merchants are incentivized to protect their "reputational capital."[194] One such example of this system in

185. Jay P. Kesan & Andres A. Gallo, *Optimizing Regulation of Electronic Commerce*, 72 U. CIN. L REV. 1497, 1500–01 (2004). Self-regulation is desirable because government intervention "tends to be seen as corrupted, self-serving and cluelessly inefficient." ANG, *supra* note 91, at 59.

186. Kesan & Gallo, *surpa* note 185, at 1501.

187. *Id.*

188. *Id.*

189. *See* discussion *supra* Part I.B.2.

190. *See* discussion *supra* Part I.B.2; *see also supra* note 72.

191. Vitalik Buterin, *Webs of Trust and How to Decentralize Them*, BITCOIN WEEKLY (May 20, 2011), http://bitcoinweekly.com/articles/webs-of-trust-and-how-to-decentralize-them. *See also, e.g.*, *Fees*, *supra* note 78.

192. Buterin, *supra* note 191.

193. *Id.*

194. For an analogue of this system in farming communities, see DOUGLAS W. ALLEN & DEAN LUECK, THE NATURE OF THE FARM: CONTRACTS, RISK, AND ORGANIZATION IN AGRICULTURE 37 (2002).

practice is the Bitcoin Police, a community-run organization whose function is to identify and prevent scammers in the Bitcoin economy.[195]

This mechanism, though, has shortcomings. To be effective, it requires a small community where information is simple to collect and disseminate.[196] As the Bitcoin economy grows, complete information becomes harder to obtain and the chance of market failure increases. Furthermore, reputation systems may only protect consumers in an aggregate sense. As one of the recent fiascos in the Bitcoin economy has illustrated, a single incident of fraud can have particularly catastrophic results.[197] This problem is exacerbated because fraudsters may be able to obfuscate their identities using Bitcoin.[198]

Self-regulation could also be capable of preventing large-scale criminal activities if more Bitcoin exchanges were to employ "autonomous agents." Autonomous agents are software programs able to scan large amounts of financial transactions for irregularities; potentially, they can even halt a transaction from being processed.[199] As such, these agents represent a code-based approach to prevent the laundering of funds through Bitcoin exchanges. The incentive for these exchanges in developing and implementing autonomous agents is that it increases the legitimacy and trustworthiness of their business; effective laundering-prevention policies ensure that government authorities are less likely to shut them down and may even lead to increased business.[200] At least one Bitcoin exchange, CampBX, has already done this.[201] In fact, due to the time and

195. MrTiggr, Comment to *Welcome to BitcoinPolice.org*, BITCOIN POLICE FORUM (Nov. 16, 2012, 2:01 PM), http://bitcoinpolice.org/t29-Welcome-BitcoinPolice.org.html. The emergence of escrow services also helps to shore up consumer protection by ensuring that buyers receive the good or service they bought before their funds are released to the seller. If the escrow service itself behaves in an irresponsible or unfair manner, it is also subject to having its reputation tarnished.

196. ALLEN & LUECK, *supra* note 194, at 37.

197. *See supra* note 169 and accompanying text (explaining the questionable circumstances behind the MyBitcoin.com incident).

198. *See* discussion *supra* Part II.B.2.

199. Richard Jones, *Cybercrime and Internet Security: A Criminological Introduction*, *in* LAW AND THE INTERNET 610 (Lilian Edwards & Charlotte Waelde eds., 3rd ed. 2009). In a general sense, autonomous agents interact with the data they encounter and perform certain tasks upon it; they may even be capable of learning as they go along. *Id.*

200. Tucker, *supra* note 21 (noting that digital currencies that take a proactive approach to prevent fraud are the most popular).

201. This exchange has "hard-coded additional rules in [its] trading engine to thwart illegitimate usage of the platform." *Frequently Asked Questions*, CAMPBX,

money they have invested in developing this program, they consider it a competitive advantage.[202]

The use of these agents by a single Bitcoin exchange is not representative of the entire industry; more exchanges (in an effort to be seen as a legitimate) would have to follow in CampBX's footsteps. Furthermore, this mechanism also suffers from a lack of transparency; cooperation between Bitcoin exchanges in setting standards for how these invisible, code-based regulators operate would ensure that no single exchange has an exploitable loophole.

In the Bitcoin economy, self-regulation falls short in its inability to stop small-scale criminal activities. In tinier online communities, where the group's interests are cohesive, social norms can govern effectively, as long as the group has some kind of mechanism in place to enforce desired behaviors.[203] The Bitcoin community, however, does not. While many within it criticize those who use the currency to commit crimes, others embrace the libertarian ideals that the currency represents and have no problem using it for such purposes.[204] Bitcoin is much more than a growing community: it is a growing economy, representing a diverse collection of interests.[205] And because the Bitcoin software provides no way to punish its users or to stop them from using it criminally, state action will be necessary to prevent such uses.

An evaluation of self-regulation in the Bitcoin economy shows that some mechanisms have developed to ensure that consumers are adequately protected. Furthermore, an increase in the use of autonomous agents by Bitcoin exchanges would help to reduce the occurrence of large-scale criminal activities. Admittedly, neither of these mechanisms is perfect, but they illustrate a drive by at least some members of the community to ensure that the economy is seen as legitimate. Where self-regulation fails outright, however, is with respect to small-scale criminal activities. The community itself

---

https://campbx.com/faq.php (last visited Oct. 11, 2011) (located in the section labeled "Legal Compliance").

202. E-mail from Keyur, CampBX employee, CampBX, to author (Oct. 2, 2011, 1:03 AM) (on file with author).

203. Mark A. Lemley, *The Law and Economics of Internet Norms*, 73 CHI.-KENT L. REV. 1257, 1270 (1998).

204. Chen, *supra* note 77. *Compare, e.g.*, *Trade*, *supra* note 135 (which bans the public listing of any illegal products or services), *with* Vince, *Maintaining Anonymity While Using Bitcoin*, THE MONETARY FUTURE (Jun. 16, 2011), http://themonetaryfuture.blogspot.com/2011/07/maintaining-anonymity-while-using.html (instructing users on the steps they can take to maintain greater anonymity, beyond that of what Bitcoin provides by default, in the event they plan on using the currency to purchase drugs from Silk Road).

205. *See* discussion *supra* Part III.A.

possesses no discernable means to punish wrongdoers, and it is likely that state action is required.

B. Regulation of Market Participants

Currently, the vast majority of activity in the Bitcoin economy involves the movement of funds by investors, speculators, and traders through Bitcoin exchanges.[206] By facilitating the conversion of Bitcoins to and from more established (and stable) currencies, they are indispensable entities to the functioning of the Bitcoin economy. That is, they could best be described as valves through which the illicit earnings of any major criminal enterprise must flow. Thus, these exchanges represent a logical place to begin implementing mechanisms designed to prevent large-scale criminal activities from taking place using the currency.

In fact, these exchanges may already fall into an existing regulatory scheme—one that governs the operation of certain financial institutions known as "money service businesses." These businesses cash checks, deal in foreign exchange, and provide prepaid access or money transmission services.[207] Bitcoin exchanges would probably be categorized as the latter. Money transmitters accept "currency, funds, or other value that substitutes for currency" and transmit it "to another location or person by any means."[208] Additionally, an entity may be classified as a money transmitter based on the specific facts and circumstances that surround the operation of its business.[209]

The definition of *money transmitter* was revised in 2011. The previous version was more limited, which led to some ambiguity as to where digital currency exchanges would fit into these regulations.[210] For example, an exchange might have raised the defense that private currencies do not actually qualify as "funds."[211]

---

206. *Paul Krugman – Golden Cyberfetters [Op-Ed on Bitcoin]*, BITCOIN MONEY (Sept. 7, 2011), http://www.bitcoinmoney.com/post/9913036774/paul-krugman-bitcoin-op-ed. *See* discussion *supra* Part III.A.

207. 31 C.F.R. § 1010.100(ff) (2011). Money service businesses need not actually be "organized or licensed business concern[s]." *Id.*

208. 31 C.F.R. § 1010.100(ff)(5)(i)(A) (2011).

209. 31 C.F.R. § 1010.100(ff)(5)(ii) (2011).

210. William Hett, *Digital Currencies and the Financing of Terrorism*, 15 RICH. J.L. & TECH. 4, 24 (2008). Before the revision, a money transmitter was an entity "who engages as a business in accepting currency, or funds denominated in currency, and transmits the currency or funds, or the value of the currency or funds, by any means . . . ." 31 C.F.R. § 103.11(uu)(5)(A) (2010).

211. Tucker, *supra* note 21, at 610. The regulation's definition of *currency* does not encompass digital currencies, as the term is limited to that which is legal tender in the United States or in foreign nations. 31 C.F.R. § 1010.100(m) (2011).

Regardless of the merits of such an argument, the inclusion of "value that substitutes for currency" is sure to foreclose any doubt whether Bitcoin exchanges are covered under the revised regulations.[212]

Under these regulations (and the federal statutes they cross-reference), if Bitcoin exchanges were indeed categorized as money transmitters, they would have to comply with a number of rules governing their operation.[213] First, operators of these businesses are required to register with the Financial Crimes Enforcement Network (also known as FinCEN, a division of the Department of the Treasury).[214] They must also compile "certain reports or records [that] have a high degree of usefulness in criminal, tax, or regulatory investigations"[215] in addition to developing and implementing effective anti-money-laundering programs.[216] Finally, under the provisions of the USA PATRIOT Act, these financial institutions would also be required to verify and maintain records on the identities of their customers.[217]

There are two major advantages to ensuring that Bitcoin exchanges comply with these regulations. The first is that the rules are preexisting; in other words, no additional legislative effort is required to devise a wholly new, Bitcoin-specific framework to govern the operation of these entities. Second, the reporting standards the regulations call for were precisely designed to inhibit

---

212. Additionally, before the revision, businesses that would otherwise qualify as money transmitters were exempted if their "acceptance and transmission of funds [was] an integral part of the execution and settlement of a transaction other than the funds transmission itself (for example, in connection with a bona fide sale of securities or other property)." 31 C.F.R. § 103.11(uu)(5)(B)(ii) (2010). If Bitcoins were to be classified as securities instead of as a currency, *see, e.g.*, Grinberg, *supra* note 8, at 194–99 (discussing the merits of such a classification), exchanges would have been exempted under this provision. However, the exemption now applies only if the money transmitter "[a]ccepts and transmits funds only integral to the sale of goods or the provision of services." 31 C.F.R. § 1010.100(ff)(5)(ii)(F) (2011).

213. Tucker, *supra* note 21, at 611–12; *see also* 31 C.F.R. § 1022.200 (2012).

214. 31 U.S.C. § 5330(a) (2006); 31 C.F.R. § 1022.380(a) (2011). These businesses must also be licensed under state law, where it is required. Failure to comply with registration and licensing requirements can result in criminal sanctions. 18 U.S.C. § 1960 (2006). *See, e.g.*, United States v. E-Gold, Ltd., 550 F. Supp. 2d 82 (D.D.C. 2008) (digital currency provider was a "money transmitting business," because the definition was not limited to only businesses that engaged in actual cash transmissions).

215. 31 U.S.C. § 5311.

216. These programs "shall include provisions for . . . (A) Verifying customer identification . . . (B) Filing Reports; (C) Creating and retaining records; [and] (D) Responding to law enforcement requests." 31 C.F.R. § 1022.210 (2011).

217. 31 U.S.C. § 5318(l); Hett, *supra* note 210, at 27.

criminals from funneling their proceeds through these types of nonbank financial institutions. As such, the regulations would need no further alteration to achieve their purpose in the context of the Bitcoin economy. Thus, a definitive administrative ruling by the Treasury Department—clarifying the application of these requirements to Bitcoin exchanges and stating their intent to enforce compliance—may be all that is additionally necessary.[218]

The drawback to relying on these regulations, however, comes in the form of the limited jurisdiction of the United States. That is, measures such as this will only be effective if they are enforced on an international scale by cooperating nations.[219] Many exchanges are located abroad and would probably prefer not to undertake the substantial costs associated with registration and compliance.[220] Criminal enterprises, then, could utilize these noncompliant exchanges to increase the chance that their activities would escape governmental scrutiny.

In sum, the regulations governing the operation of money service businesses provide an existing framework for stymieing large-scale criminal activities in the Bitcoin economy. However, without enforcement abroad, they may only prove to be effective at the domestic level. Furthermore, casual transactions for contraband items would likely continue to go unnoticed.

C. Prohibition

A prohibition on the use of Bitcoins would not be unheard of. Lawmakers have, in fact, banned the use of certain technologies in the past. For example, provisions in the Digital Millennium Copyright Act criminalize the dissemination of any technology whose primary purpose is to circumvent digital copyright protections.[221] Prohibitive measures, however, are typically not taken unless the technology's harms greatly outweigh the societal benefits from its use.[222] In such

---

218. Notably, in an effort to ensure that Bitcoin continues to be seen as legitimate, some exchanges have taken a proactive approach to comply with these regulations, including Mt. Gox and CampBX. Wolf, *supra* note 158; *Frequently Asked Questions*, *supra* note 201.

219. Tucker, *supra* note 21, at 617.

220. Even if the costs of doing so were negligible, it is likely that some exchanges would refuse to comply *specifically because* they cater to customers who use Bitcoin to engage in criminal activities.

221. *See* 17 U.S.C. § 1201(a)–(b) (2006).

222. Jay P. Kesan & Rajiv C. Shah, *Shaping Code*, 18 HARV. J.L. & TECH. 319, 328 (2005).

circumstances, lawmakers tend to view prohibition as the most efficient solution.[223]

In *Sony v. Universal City Studios*, the Supreme Court was faced with deciding whether Sony, producer of the Betamax home video recorder, could be held liable for contributing to the copyright infringing activities of its customers.[224] In resolving the case in favor of Sony, the Court determined that the Betamax was "capable of substantial noninfringing uses" and, additionally, that there was no evidence that Sony encouraged infringing behavior.[225]

Admittedly, Bitcoin has nothing to do with copyright infringement. *Sony*, however, provides a useful analogy of how regulators might view the Bitcoin system: prohibitive measures will not likely be taken against the digital currency unless lawmakers find that it is being used almost exclusively for illicit purposes.[226] In other words, if average consumers were unimpressed by Bitcoin's advantages and its economy was devoid of any lawful activity, a prohibition might make sense.

A ban on Bitcoin's use could also result if it was able to sufficiently challenge the U.S. dollar.[227] Some scholars have suggested that lawmakers might respond with hostility to successful digital currencies because they could eventually undermine the government's seignorage income[228] and decrease the value of the nation's currency (if individuals preferred the digital currency to the national one).[229]

While many, if not all, of these reasons supporting prohibitive measures are valid, they are not valid *yet*. At this point, there are still too many legitimate actors in the Bitcoin economy to conclude, as Senator Schumer has, that Bitcoin is nothing other than "an online

---

223. *Id.*

224. Sony Corp. of Am. v. Universal City Studios, 464 U.S. 417 (1984).

225. *Id.* at 438.

226. Goldstein & Kestenbaum, *supra* note 89 (quoting Columbia Law School Professor Ronald Mann, who intimates that regulators will likely evaluate what Bitcoin is primarily used for when calculating how they should respond). Bitcoin's architecture could escalate such a finding because experts have stated that the most dangerous features of some digital currencies is not their ability to provide anonymity, but the irrevocable nature of their transactions. That is, criminals are less concerned with the traceability of their actions and seem to care more about frustrating the possibility of funds recovery. Ross Anderson, *Closing the Phishing Hole – Fraud, Risk, and Nonbanks*, CAMBRIDGE UNIV., 1 (Apr. 8, 2007), http://www.cl.cam.ac.uk/~rja14/Papers/nonbanks.pdf.

227. *See* discussion *supra* Part II.B.

228. Seignorage is the "revenue a government receives by issuing money." MISHKIN, *supra* note 29, at G-9.

229. Tucker, *supra* note 21, at 620; Friedman & Macintosh, *supra* note 36, at 279.

form of money laundering."[230] Furthermore, the Bitcoin economy is still too small to warrant concern that it could lead to overall economic instability. As governmental financial authorities have pointed out, "even if every person in the United States held $150 in electronic currency, the total value would amount to less than $50 billion, which is insignificant relative to the current M1 monetary aggregate of $1 trillion."[231]

Prohibitions also tend to be "economically inefficient means of regulation" for three primary reasons.[232] First, they eliminate any potential benefit conferred by the banned technology.[233] Second, they tend to stymie any future innovation that could have resulted from the technology's continued use.[234] Finally, they entail high costs with respect to enforcement.[235]

These arguments against prohibition also resonate strongly with Bitcoin. A proscription on the digital currency's use would concomitantly eliminate the financial advantages and convenience it provides to consumers and merchants. Passing a law banning the use of the digital currency would also foreclose the future advances it could bring as it continues to upend the traditional paradigm of Internet commerce.[236] Indeed, its novel approach to transaction verification has led to the development of other innovative projects, which would not have been possible in Bitcoin's absence.[237]

The effects of such a law would do little more than stop the majority of law-abiding individuals from using the digital currency out of the fear of prosecution, while "Bitcoin criminals" would not likely be deterred because they were already engaging in illegal activities. Fundamentally, this is the same problem that has troubled the entertainment industry for nearly a decade.[238] Despite the panoply of (expensive) lawsuits that the industry has filed in an

---

230. *See supra* note 158 and accompanying text.

231. Grinberg, *supra* note 8, at 182 n.97 (citing Edward W. Kelley, Jr., Member, Board of Governors of the Federal Reserve System, Remarks at the Digital Commerce Conference 4 (May 6, 1996)). M1 is one of the measures of the money supply used by the Federal Reserve; it includes the total value of currency, traveler's checks, and demand deposits. MISHKIN, *supra* note 29, at 57.

232. Kesan & Shah, *supra* note 222, at 328.

233. *Id.*

234. *Id.*

235. *Id.*

236. *See* discussion *supra* Part I.B.2.

237. *See*, *e.g.*, Namecoin, an alternative domain name system based on Bitcoin's source code. *Namecoin – A DNS Alternative Based on Bitcoin*, BLUISH CODER (May 12, 2011), http://www.bluishcoder.co.nz/2011/05/12/namecoin-a-dns-alternative-based-on-bitcoin.html.

238. *RIAA v. The People: Five Years Later*, ELECTRONIC FRONTIER FOUNDATION (Sept. 2008), https://www.eff.org/wp/riaa-v-people-years-later.

attempt to combat peer-to-peer file sharing, illegal downloading has only become more popular.[239] This analogy may be exceptionally appropriate because the architecture behind the Bitcoin system is not all that different from that which powers the BitTorrent file-sharing software.[240] While regulators could attempt to halt the flow of Bitcoins by requiring Internet Service Providers to block the digital currency's transactions, sophisticated Bitcoin users could easily respond by recalibrating the Bitcoin software to evade this technological roadblock.[241]

Considering these factors, prohibiting Bitcoin in the near future would be a rash and unnecessary response to issues that have not yet fully materialized. While the approach may ultimately protect consumers by removing them from the system altogether, it would probably not affect the behavior of individuals persistent in using the digital currency for both small and large-scale criminal activities.

CONCLUSION

In theory, the ideas that prompted the development of the Bitcoin system are sound. It is the first digital currency to solve the double-spending problem without having to introduce a third party. This reduces transaction costs for both consumers and merchants and protects Bitcoin users from having to share their transactional history with financial institutions. Furthermore, Bitcoin's self-administered money supply eliminates the need for a central authority, which could protect it from both inflation and political influence.[242]

While the system certainly presents opportunities for criminal abuse that cannot be ignored,[243] the digital currency is still too much in its infancy to have proven that its economic model is sustainable and, thus, that its facilitation of illicit activities is likely to

---

239. *Id.*

240. J.P., *supra* note 46. BitTorrent is a peer-to-peer protocol that allows users to share files with one another without the need for a centralized server. *BitTorrent*, TECHNOPEDIA, http://www.techopedia.com/definition/1865/bittorrent (last visited Nov. 7, 2011).

241. Traditionally, the entertainment industry has looked to ISPs as "chokepoints" through which the dissemination of illegally copied files could be throttled. As would be the case with Bitcoin, this task would be accomplished by the use of port scrutiny or deep packet inspection. A governmental mandate to employ such measures, however, would undoubtedly raise substantial privacy concerns. Lilian Edwards, *The Fall and Rise of Intermediary Liability Online*, *in* LAW AND THE INTERNET, *supra* note 199, at 81; Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 U. ILL. L. REV. 1417, 1492, 1468 (2009).

242. *See* discussion *supra* Part I.B.2.

243. *See* discussion *supra* Part III.A.

continue.[244] Moreover, the Bitcoin system has provided a novel method of value exchange that could potentially serve as the foundation of further innovations. Any regulatory response, then, should initially be limited and carefully measured.

Prohibition is not the answer. Owing to Bitcoin's distributed nature, even if prohibition eventually proves to be a logical choice, it would likely never come close to addressing the problems for which it was enacted.[245] More importantly though, hand-to-hand cash transactions are used just as frequently for criminal purposes, yet the efforts of lawmakers and law enforcement agencies are directed at the criminals themselves and not at the medium through which they transact. Indeed, Bitcoin's blockchain provides a record of all transactions that take place on the network.[246] Through the use of "sophisticated network analysis techniques,"[247] law enforcement agencies may be able to leverage this public ledger to ferret out any small-scale criminal actors using the digital currency for nefarious purposes.

In terms of large-scale criminal activities, government efforts should be directed at the exchanges that operate in the Bitcoin economy. The recent revision to the regulatory definitions and requirements of money service businesses seems to eliminate any doubt as to whether Bitcoin exchanges fall within the scope of these provisions. In fact, the requirements were designed to combat the same large-scale criminal activities that have been identified as a major concern in the Bitcoin economy. While ensuring that these exchanges comply with the existing statutory scheme may only achieve the desired result on a domestic level, until the direction of the Bitcoin economy is more fully realized, it represents the best solution going forward.[248]

Joshua J. Doguet *

244. *See* discussion *supra* Part III.B.
245. *See* discussion *supra* Part IV.C.
246. *See* discussion *supra* Part I.B.1.
247. *See* Chen, *supra* note 77 and accompanying text.
248. *See* discussion *supra* Parts I.B.2. & IV.B.

* J.D./D.C.L., 2013, Paul M. Hebert Law Center, Louisiana State University.