

# Bitcoin: An Innovative Alternative Digital Currency

by REUBEN GRINBERG\*

<b>I. Introduction</b> .....	160
<b>II. Bitcoin Primer</b> .....	162
<b>III. Bitcoin Ecosystem</b> .....	165
<b>IV. Comparing Bitcoin to its Competition</b> .....	168
A. Facilitation of e-commerce.....	168
1. Traditional e-commerce.....	168
2. Micropayments.....	170
3. Virtual World and Game-Related Commerce .....	170
B. Gold-Backed Currencies .....	172
<b>V. Is Bitcoin Sustainable?</b> .....	174
A. Iraqi Swiss Dinar .....	174
B. Confidence .....	175
1. Improper Use of Discretionary Authority.....	175
2. Superior Competing Currency .....	176
3. Government Crackdown.....	177
4. Deflationary Spiral .....	177
C. Potential Technology Failures .....	179
1. Anonymity Failure.....	179
2. Theft.....	180
3. Denial of Service.....	180
<b>VI. Legal Issues</b> .....	181

---

\* Yale Law School, J.D. 2011; University of Texas at Austin, M.S. 2007; Yale University, B.S. 2005. The author is a first-year law clerk at a law firm in New York City. The author would like to thank professor Jonathan R. Macey, professor Ronald Mann, Melanie Keene, Gavin Andresen, and members of the Bitcoin community for their helpful comments on an earlier draft of this Article. The author also thanks Assistant U.S. Attorney Jill Westmoreland Rose and Bernard von NotHaus, opposing parties in the Liberty Dollar cases who took the time to answer my questions. Finally, the author also thanks Zion Maffeo, David Simson, and other helpful editors of the Hastings Science & Technology Law Journal.

A. Federal Government’s Monopoly on Issuing Currencies .....	182
1. The Stamp Payments Act of 1862 .....	183
2. Prohibition on Coining Money and the Liberty Dollar Saga.....	191
B. Securities Regulations.....	194
1. Note or Stock .....	195
2. Investment Contract.....	196
3. Commodity .....	199
4. Currency .....	200
C. Anti-Money Laundering Laws and Regulations .....	204
<b>VII. Conclusion.....</b>	<b>206</b>

## I. Introduction

Bitcoin is a digital, decentralized, partially anonymous currency, not backed by any government or other legal entity, and not redeemable for gold or other commodity. It relies on peer-to-peer networking and cryptography to maintain its integrity.<sup>1</sup> Its proponents argue that Bitcoin has many properties that could make it an ideal currency for mainstream consumers and merchants. For example, bitcoins are highly liquid, have low transaction costs, can be used to send payments quickly across the internet, and can be used to make micropayments. This new currency could also hold the key to allowing organizations such as Wikileaks, hated by governments, to receive donations and conduct business anonymously.<sup>2</sup>

Amazingly, as of October 2011, a bitcoin (currency ticker BTC) is worth about two U.S. Dollars (USD), there are about \$20 million worth of bitcoins in existence,<sup>3</sup> there are probably around 20,000

1. See *Bitcoin*, WIKIPEDIA, <http://en.wikipedia.org/wiki/Bitcoin> (last modified Oct. 25, 2011); Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, BITCOIN PROJECT, <http://bitcoin.org/bitcoin.pdf> (last visited Oct. 25, 2011); *FAQ*, BITCOIN WIKI, <https://en.bitcoin.it/wiki/FAQ> (last modified Oct. 25, 2011).

2. See Keir Thomas, *Could the Wikileaks Scandal Lead to New Virtual Currency?*, PC WORLD: BUSINESS CENTER (Dec. 10, 2010, 4:30 PM), [http://www.pcworld.com/businesscenter/article/213230/could\\_the\\_wikileaks\\_scandal\\_lead\\_to\\_new\\_virtual\\_currency.html](http://www.pcworld.com/businesscenter/article/213230/could_the_wikileaks_scandal_lead_to_new_virtual_currency.html); Rainey Reitman, *Bitcoin – a Step Toward Censorship-Resistant Digital Currency*, ELECTRONIC FRONTIER FOUNDATION, (Jan. 20, 2011, 5:20 PM), <https://www.eff.org/deeplinks/2011/01/bitcoin-step-toward-censorship-resistant> (“Bitcoin is particularly interesting in the wake of recent events that demonstrated how financial institutions can make political decisions in whom they service, showcased by the decisions of PayPal, Visa, Mastercard and Bank of America to cut off services to Wikileaks.”).

3. See BITCOIN WATCH, <http://bitcoinwatch.com/> (last visited Oct. 21, 2011).

Bitcoin users,<sup>4</sup> and over \$300,000 worth of bitcoins are traded every day.<sup>5</sup>

Although the Bitcoin economy is flourishing, users are anxious about Bitcoin's legal status and the possibility of a government crackdown.<sup>6</sup> Some point to Bitcoin's ability, like all digital and anonymous currencies, to facilitate money laundering, tax evasion, and trade in illegal drugs and child pornography.<sup>7</sup> Indeed, the U.S. government prosecuted and shut down the creators of e-gold, a digital currency backed by gold, under state and federal laws for conspiracy to commit money laundering, and also for providing services to those involved in "child exploitation, credit card fraud, and wire (investment) fraud."<sup>8</sup> Others point to governments' purported interests in protecting their economies and monopolies on minting new money.<sup>9</sup> These individuals point to the successful prosecution and conviction of the creator of the Liberty Dollar, a paper and coin-based currency backed by gold and other precious metals.<sup>10</sup>

Part II explains how Bitcoin works and Part III describes its nascent ecosystem of websites and services. Part IV compares Bitcoin to its competition, including payment processors like PayPal and digital gold currencies. Part V explores whether Bitcoin can be a sustainable currency and why individuals would trust a currency not supported by any legal institution and not redeemable for any

---

4. See *Bitcoin Map*, BITCOIN WIKI, [https://en.bitcoin.it/wiki/Bitcoin\\_Map](https://en.bitcoin.it/wiki/Bitcoin_Map) (last modified Oct. 21, 2011).

5. See, e.g., BITCOIN WATCH, *supra* note 3 (when visited, approximately 110,000 bitcoins exchanged in previous 24 hours at an exchange rate of approximately 2.5 USD per BTC).

6. See, e.g., epii, Comment on *How long until governments outlaw bitcoin usage?*, BITCOIN FORUM (Mar. 29, 2011 8:40:41 AM), <http://bitcointalk.org/index.php?topic=5110.msg74627#msg74627> ("I think that illegalization is Bitcoin's most likely mode of failure.").

7. See, e.g., *id.* ("Considering how quickly services like Silk Road [an anonymous marketplace for illegal drugs] have sprung up, and the fact that the demographic of people who seem most interested in Bitcoin at this point tends to overlap with the demographic of likely tax evaders, I am afraid that this illegalization might just be a matter of time.").

8. See Peter C. Tucker, *The Digital Currency Doppelganger: Regulatory Challenge or Harbinger of the New Economy?*, 17 CARDOZO J. INT'L & COMP. L. 589, 590–92 (2009) (citations omitted).

9. See, e.g., Glass, Comment on *How long until governments outlaw bitcoin usage?*, BITCOIN FORUM (Mar. 29, 2011 10:46:59 AM), <http://bitcointalk.org/index.php?topic=5110.msg74713#msg74713>.

10. See, e.g., *id.*; Press Release, Department of Justice, *Defendant Convicted of Minting His Own Currency* (Mar. 18, 2011), available at <http://charlotte.fbi.gov/dojpressrel/pressrel11/ce031811.htm> [hereinafter DOJ, *Liberty Dollar Conviction Release*].

commodity. Part VI explores a few of the many legal ramifications of Bitcoin, including statutes supposedly aimed at enforcing the federal government's monopoly on issuing currency and securities regulation.

## II. Bitcoin Primer

Julian Assange was probably unsurprised when PayPal, a corporation with large market share susceptible to government pressure, stopped processing donations to his whistleblowing organization, Wikileaks, due to what Paypal deemed "illegal activity."<sup>11</sup> In the 1990s, Assange was a member of the cypherpunks mailing list, a group that disdained most government regulation and discussed achieving privacy and libertarian ideals by using cryptography. In 1998, another member of the cypherpunks proposed a digital, distributed, anonymous currency called "b-money" that would allow "untraceable pseudonymous entities to cooperate with each other more efficiently, by providing them with a medium of exchange . . ."<sup>12</sup> About ten years later, a programmer working under the pseudonym Satoshi Nakamoto figured out how to implement such a currency, publishing a description of his invention and also releasing software to make it work.<sup>13</sup>

Like the U.S. Dollar, Bitcoin is not redeemable for another type of money or for a certain amount of a commodity, such as an ounce of gold. Unlike the U.S. Dollar, Bitcoin is not backed by the U.S. Government or any other legal institution and is a digital rather than paper currency, storable on electronic media and transferable over the internet.<sup>14</sup>

Individuals who want to own or transact in Bitcoin can either run a program on their own computer that implements the Bitcoin protocol (a Bitcoin client),<sup>15</sup> or create an account on a website that

---

11. *PayPal statement regarding Wikileaks*, PAYPAL BLOG (Dec. 3, 2010), <https://www.thepaypalblog.com/2010/12/paypal-statement-regarding-wikileaks>.

12. Wei Dai, *b-money*, WEI DAI'S HOME PAGE, <http://weidai.com/bmoney.txt> (last visited Oct. 7, 2011) (the thirteenth paragraph).

13. Nakamoto, *supra* note 1.

14. See William Hett, *Digital Currencies and the Financing of Terrorism*, XV RICH. J.L. & TECH. 4, 7 (2008), available at <http://jolt.richmond.edu/v15i2/article4.pdf> (describing how digital currencies generally work).

15. The Bitcoin developers publish an "official" Bitcoin client for Windows, Mac OS X, and Linux, with an ugly, confusing, but usable graphical user interface. See *Original Bitcoin Client*, BITCOIN WIKI, [https://en.bitcoin.it/wiki/Original\\_Bitcoin\\_client](https://en.bitcoin.it/wiki/Original_Bitcoin_client) (last visited Oct. 25, 2011) (including screenshot of graphical user interface). Others are creating alternative clients, such as one written in Java, and another intended for mobile devices running the Android operating system. See *Category:Clients*, BITCOIN WIKI,

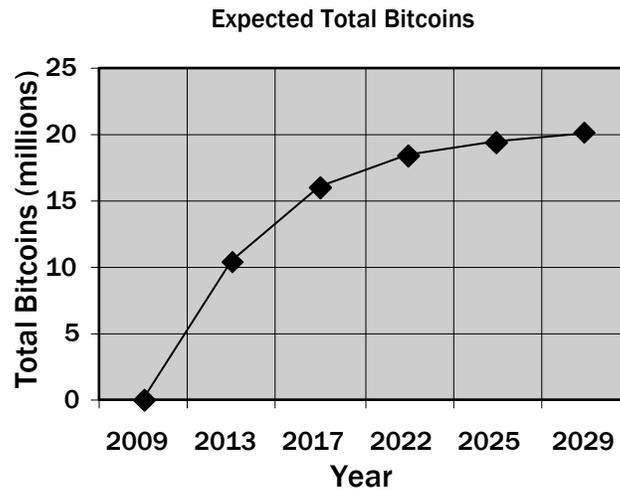
runs the Bitcoin client for its users. The Bitcoin client saves an individual's bitcoins in a file called the wallet, which the user must secure and backup. These programs connect to one another over the Internet forming peer-to-peer networks, making the system a distributed one resistant to central attack.

New bitcoins are issued to competing "miners" who use their computers to generate solutions to problems that help ensure the integrity and security of the system. As the number of miners in the network changes, the problem difficulty adjusts to ensure that bitcoins are created at a predetermined rate and not faster or slower. Currently, about 50 bitcoins are issued every ten minutes, although the rate will halve to 25 bitcoins in about two years and will halve every four years after that.<sup>16</sup> At those rates, 10.5 million bitcoins will be created in the first four years, half that amount in the next four years, and so on, approaching but never reaching a total supply of 21 million bitcoins, as illustrated in [Figure 1](#). Bitcoins are divisible to eight decimal places.

---

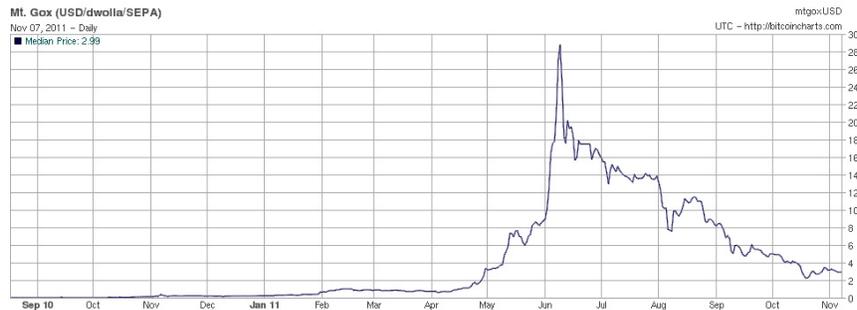
<https://en.bitcoin.it/wiki/Category:Clients> (last modified June 25, 2011); *Bitcoin Wallet*, Android Market, <https://market.android.com/details?id=de.schildbach.wallet> (last updated Oct. 5, 2011).

16. A "block" contains the solution that the mining computers are trying to solve. A block is created about once every ten minutes. According to the Bitcoin FAQ, 50 bitcoins are awarded for the first 210,000 blocks generated, and the award is halved every 210,000 blocks afterwards. It takes about 4 years to generate 210,000 blocks (10 minutes / block x 210,000 blocks / 60 / 365). As of March 8, 2011, approximately 113,000 blocks have been generated (according to my Bitcoin client), which means that in approximately two years the award will be halved to 25 bitcoins. The total supply of bitcoins will approach but never reach 21 million. *FAQ: How are new Bitcoins created?*, BITCOIN WIKI, [https://en.bitcoin.it/wiki/FAQ#How\\_are\\_new\\_Bitcoins\\_created](https://en.bitcoin.it/wiki/FAQ#How_are_new_Bitcoins_created) (last modified Oct. 25, 2011).



**Figure 1. Expected bitcoin supply over time.**

In May 2010, one bitcoin traded at half a cent. It rose steeply until it reached \$30 in June 2011 (a 600,000% increase) before crashing back to \$2 in October<sup>17</sup>, as illustrated in Figure 2.



**Figure 2. Bitcoin to USD exchange rate on the Mt. Gox exchange through October 22, 2011.**

The system is partially anonymous in that anyone can see the trail of all transactions from all accounts,<sup>18</sup> but nothing in the system ties accounts to individuals, and individuals can create unlimited

<sup>17</sup> See BITCOIN CHARTS, <http://bitcoincharts.com/charts/mtgoxUSD#tgMzm1g10zm2g25> (last visited Nov. 7, 2011).

<sup>18</sup> See, e.g., BITCOIN BLOCK EXPLORER, <http://blockexplorer.com> (allowing users to see latest Bitcoin transactions, search for transactions or accounts, and so on) (last visited Oct. 7, 2011).

accounts instantly and for free.<sup>19</sup> Individuals can send bitcoins for free, but may add optional transaction fees to ensure their transactions are quickly processed.<sup>20</sup> Furthermore, Bitcoin transactions are irreversible in the same way cash transactions are irreversible. By contrast, credit card charges can be charged back to merchants.

### III. Bitcoin Ecosystem

A growing ecosystem surrounds Bitcoin, including exchanges, transaction services providers, market information and chart providers, escrow providers, joint mining operations and so on. Absent from this ecosystem at present are futures markets and entities offering legitimate investment returns, such as fractional reserve banks, although some individuals have announced plans to build these.<sup>21</sup>

Individuals holding this currency represent a number of interests, including technology early adopters, privacy and cryptography enthusiasts, government-mistrusting “gold bugs,” criminals, and speculators.<sup>22</sup> A large number of online merchants accept bitcoins, catering to individuals with these interests, including web hosts, online casinos, illicit drug marketplaces, auction sites, technology consulting firms, and adult media and sex toy merchants.<sup>23</sup> A number of nonprofit organizations such as Wikileaks accept donations in

---

19. *Introduction*, BITCOIN WIKI, <https://en.bitcoin.it/wiki/Introduction#Anonymity> (last visited Mar. 14, 2011) (subsection “Anonymity”).

20. Although transaction fees are not generally used right now, many Bitcoin activists expect that as the volume of transactions increase, individuals will more often attach transaction fees.

21. See, e.g., Nefario, *Investors for bitcoin stock market and credit rating agency [sic], dev started!*, BITCOIN FORUM (Feb. 25, 2011 3:01:32 AM), <http://bitcointalk.org/index.php?topic=3844.0> (stock market and credit rating agency); gigabytecoin, *Where To Create Your Own Bank For Less Than \$25K???*, BITCOIN FORUM (Mar. 24, 2011 5:22:16 AM), <http://bitcointalk.org/index.php?topic=4871.0> (bank).

22. See reubgr, *Poll: Why Do You Use Bitcoin?*, BITCOIN FORUM (Mar. 14, 2011) <http://bitcointalk.org/index.php?topic=4465.0> (poll conducted by the author on the main Bitcoin forum); Tucker, *supra* note 8, at 601–08 (describing users generally interested in digital currencies); chodpaba, *What if one Bitcoin was worth the same as one share Berkshire Hathaway?*, BITCOIN FORUM (Mar. 12, 2011 12:43:29 AM), <http://bitcointalk.org/index.php?topic=4390.0> (considering whether a single Bitcoin would ever equal in worth a share of Berkshire Hathaway).

23. See *Trade*, BITCOIN WIKI, <https://en.bitcoin.it/wiki/Trade> (last modified Oct. 25, 2011) (listing merchants that accept bitcoins).

Bitcoin.<sup>24</sup> And a small handful of retail businesses accept bitcoins, although there is little indication that the amount of bitcoin-based business transacted by these retail establishments is significant.<sup>25</sup>

To accommodate growing demand several exchanges have been created, offering exchanges between Bitcoin and traditional currencies, including the U.S. Dollar, Japanese Yen, Euro, and other digital currencies, including Liberty Reserve, Pecunix, and WebMoney.<sup>26</sup> Mt. Gox, which seems to be the most popular exchange<sup>27</sup> with \$10,000 in trading volume on a particular day in March 2011,<sup>28</sup> has an easy to use website.<sup>29</sup> None of the standard exchanges allow futures trading yet, although there is a less formal over-the-counter exchange that allows individuals to list buy and sell orders involving bitcoins and any service, commodity, or currency.<sup>30</sup> Option contracts have been sold on the over-the-counter exchange.<sup>31</sup>

---

24. See *Donate*, WIKILEAKS, <http://shop.wikileaks.org/donate#dbitcoin> (last visited Oct. 25, 2011). In June 2011, the Electronic Frontier Foundation decided to no longer accept donations in bitcoins, citing unclear and complex legal issues. See Cindy Cohn, *EFF and Bitcoin*, ELECTRONIC FRONTIER FOUNDATION (June 20, 2011 5:51 PM), <https://www.eff.org/deeplinks/2011/06/eff-and-bitcoin>.

25. See Joshua Davis, *The Crypto-Currency*, THE NEW YORKER, Oct. 10, 2011, at 68 (noting that Davis, in the course of researching his article, was the first individual to use bitcoins to pay at the Howard Johnson Hotel in California).

26. See *Currency exchanges*, BITCOIN WIKI, [https://en.bitcoin.it/wiki/Trade#Currency\\_exchanges](https://en.bitcoin.it/wiki/Trade#Currency_exchanges) (last visited Oct. 25, 2011).

27. *MtGox*, BITCOIN WIKI, <https://en.bitcoin.it/wiki/MtGox> (last modified Oct. 23, 2011) (“MtGox . . . is the most widely used bitcoin currency exchange market . . . and remains the largest in terms of popularity and volume.”).

28. On the Bitcoin Charts site, trading volume on Mt. Gox on March 6, 2011 was USD \$10,000, more than ten times greater than the volume on any of the other listed exchanges.

29. See MT. GOX, <http://www.mtgox.com> (last visited Oct. 7, 2011). One can transfer money into the account by sending cash, money order or check to an individual (two percent commission) or by Paypal (seven percent commission), either of which takes several business days. Once the money appears in the Mt. Gox account, the website allows purchasing and selling Bitcoins at the prevalent exchange rate or at some particular price, with a 0.65% commission. The website also allows instantly sending funds to another individual’s Mt. Gox account or to a Bitcoin account. I was able to purchase about \$9 worth of Bitcoins on Mt. Gox. I first sent \$10 by Paypal to “Bitcoin Morpheus,” as instructed on the Mt. Gox website. That individual took a \$1 commission and added USD \$9 to the my account on Mt. Gox. I then purchased about \$9 worth of Bitcoins and then sent them to my Bitcoin account number.

30. #BITCOIN-OTC, <http://bitcoin-otc.com> (last visited Mar. 7, 2011).

31. See *Bitcoin options trading on the Bitcoin OTC marketplace*, BITCOIN MONEY (Apr. 13, 2011), <http://www.bitcoinmoney.com/post/4585101363/first-bitcoin-put-option-contract> (“The first ever bitcoin PUT option contract was just recently traded on the #bitcoin-otc marketplace. A buyer paid to a seller 1.50 BTC as the premium for a contract that gives the buyer the option to sell at a later time 100 BTC at the rate of \$0.75/BTC.”).

Several sites provide transaction services, allowing individuals to keep, send, and receive bitcoins without ever running the Bitcoin client on their own computers. Mt. Gox, for example, allows sending bitcoins through email, as does Bitcoin Mail. Instawallet provides a website that allows individuals to create Bitcoin addresses, send bitcoins to any address for free, and check balances.<sup>32</sup>

At first, individuals could quickly mine a significant number of bitcoins on their own computers. But the problem difficulty has increased so much that most computers would now take on average a year or more to mine just 50 BTC.<sup>33</sup> Several enterprising individuals have created mining collectives that have enormous computational power, collect mining rewards often, and distribute the rewards among members of the collective according to the amount of work they contributed towards finding the reward (i.e., their computational power).<sup>34</sup>

Name	Description
Bitcoin Watch <sup>35</sup>	Provides currency exchange value and volume charts for a number of Bitcoin exchanges.
Bitcoin Monitor <sup>36</sup>	Shows the most recent Bitcoin transactions, currency exchanges, and Block solutions.
Bitcoin Block Explorer <sup>37</sup>	Allows individuals to search by address and see all transactions for that address.
Bitcoin Faucet <sup>38</sup>	A service that provides 0.05 BTC for free, by one of the main developers behind Bitcoin, who “want[s] Bitcoin to be successful, [and] created this little service to give [new users] a few coins to start with.” <sup>39</sup>
Bitcoin Mail <sup>40</sup>	A site that allows individuals to send bitcoins to others by email.

32. INSTAWALLET, <https://www.instawallet.org> (last visited Oct. 24, 2011).

33. See Jered Kenna, *Remove “generate bitcoins” from standard client?*, BITCOIN FORUM (Mar. 23, 2011 1:44:37 PM), <http://bitcointalk.org/index.php?topic=4828.0> (discussing the low probability of individual miners generating bitcoins).

34. See *Pooled Mining*, BITCOIN WIKI, [https://en.bitcoin.it/wiki/Pooled\\_mining](https://en.bitcoin.it/wiki/Pooled_mining) (last modified Sept. 1, 2011).

35. BITCOIN WATCH, <http://bitcoinwatch.com> (last visited Oct. 7, 2011).

36. BITCOIN MONITOR, <http://www.bitcoinmonitor.com> (last visited Oct. 7, 2011).

37. BITCOIN BLOCK EXPLORER, <http://blockexplorer.com> (last visited Oct. 7, 2011).

38. BITCOIN FAUCET, <https://freebitcoins.appspot.com> (last visited Oct. 7, 2011).

39. Gavin Andresen, *Free Bitcoins*, <http://freebitcoins.appspot.com/> (last visited March 6, 2011) (under “What’s the catch?”).

40. BITMAIL, <http://www.bitcoinmail.com> (last visited Oct. 7, 2011).

A more comprehensive list of Bitcoin exchanges and merchants who accept Bitcoin is available on the Bitcoin Wiki.<sup>41</sup>

#### IV. Comparing Bitcoin to its Competition

Bitcoin competes with at least two classes of products: (1) products that facilitate internet-based commerce, and (2) gold-backed currencies. As described below, Bitcoin is unlikely to make significant headway in the traditional ecommerce market because consumers generally do not care about the kind of anonymity that Bitcoin provides, prefer to compare prices of most goods and services in a currency they are familiar with, and want fraud protection (which Bitcoin currently lacks). However, Bitcoin may be especially competitive in the micropayment and virtual world markets, where consumers care less about pricing in a familiar currency. Bitcoin is likely to be attractive to those who like gold-backed currencies because its value depends on the availability of a limited (albeit virtual) resource rather than discretionary actions by central bankers.

##### A. Facilitation of e-commerce

###### 1. Traditional e-commerce

The growth of the internet created demand for electronic payment systems.<sup>42</sup> PayPal has come to dominate this space, allowing users to fund accounts by credit card or bank transfers.<sup>43</sup> Companies that took the alternative approach of creating digital currencies which were convertible to and from existing currencies, such as DigiCash, GoldMoney, Pecunix, and Web-Money,<sup>44</sup> have not been as successful<sup>45</sup> due to a combination of lack of competitive advantages, managerial incompetence, and dubious legality.

---

41. *Trade*, BITCOIN WIKI, <https://en.bitcoin.it/wiki/Trade> (last modified Oct. 25, 2011).

42. Tucker, *supra* note 8, at 601; Carl Kaminski, *Online Peer-to-Peer Payments: PayPal Primes the Pump, Will Banks Follow?*, 7 N.C. BANKING INST. 375, 375 (2003).

43. Tucker, *supra* note 8, at 601–02; Kaminsky, *supra* note 42, at 378–79. PayPal handles payments for more than 100,000 websites in 18 currencies, and has more than 100 million user accounts. *Id.* Competitors abound, such as Google Checkout, Amazon Payments, and Dwolla. See Rafe Needleman, *Cash is dead, says Dwolla*, CNET NEWS (Dec. 17, 2010, 7:00 AM), [http://news.cnet.com/8301-19882\\_3-20025966-250.html](http://news.cnet.com/8301-19882_3-20025966-250.html).

44. Tucker, *supra* note 8, at 601–02.

45. See Sarah Jane Hughes et al., *Developments in the Law Concerning Stored-Value Cards and Other Electronic Payments Products*, 63 BUS. LAW. 237, 257 & n.157 (2007) (noting bankruptcy of DigiCash, one of the largest digital currency providers).

The failure of DigiCash is instructive.<sup>46</sup> Users turned out to have no qualms about entering credit card information online<sup>47</sup> (one of DigiCash's supposed advantages) and did not care about DigiCash's strong anonymity guarantees<sup>48</sup> (as is especially evident today).<sup>49</sup> Similarly, fundamental features of other digital currencies also turned out to be liabilities rather than assets. GoldMoney and Pecunix, for example, are denominated in gold rather than the U.S. Dollar, and most consumers would probably not be interested in shopping and browsing items with prices in an unfamiliar currency.<sup>50</sup>

Similarly, Bitcoin is unlikely to be particularly competitive in the traditional ecommerce market. Most consumers do not care about anonymity or centralization. They do not want to shop real goods in prices listed in Bitcoin instead of dollars. They are unafraid of inflation of the money supply by the Federal Reserve. Furthermore,

---

46. DigiCash was one of the earliest digital currencies, begun in the early 1990s, and was initially run by David Chaum, who had obtained numerous digital currency patents in the 1980s related to ensuring anonymity using cryptography. DigiCash's history, up until its bankruptcy in 1998, is one of poor management, missed opportunities, and failed deals. See Ian Grigg, *How DigiCash Blew Everything*, CRYPTOME (Feb. 10, 1999), <http://cryptome.org/jya/digicrash.htm> (translation of a Dutch online magazine article describing events leading up to DigiCash's bankruptcy); see also *Alternative History of Bitcoin*, BITCOIN FORUM (Feb. 22, 2011), <http://bitcointalk.org/index.php?topic=3755.0> (forum discussion comparing DigiCash to Bitcoin).

47. Tucker, *supra* note 8, at 593–94.

48. Steven Levy, *E-Money (That's What I Want)*, WIRED, Dec. 1994, at 174, available at <http://www.wired.com/wired/archive/2.12/emoney.html> (“David Chaum has devoted his life, or at least his life’s work, to creating cryptographic technology that liberates individuals from the spooky shadows of those who gather digital profiles. [H]e . . . advocate[s] a form of [digital currency] that fits neatly into a privacy paradigm, whereby the details of people’s lives are shielded from the prying eyes of the state, the corporation, and various unsavory elements.”).

49. Individuals give enormous amounts of data to financial companies, such as credit card companies, and social news websites, such as Facebook. These companies, in turn, whether with users’ consent—or simply without users’ complaints, sell or give this information to others. See, e.g., Josh Constine, *The Facebook Credits GetBalance API Helps Developers Dynamically Price Virtual Goods*, INSIDE FACEBOOK (Mar. 4, 2011), <http://www.insidefacebook.com/2011/03/04/facebook-credits-getbalance-api> (noting that Facebook allows companies that develop applications using Facebook Credits to see the Credits balance of its users, which would allow an application to “identify high rollers with a large balance of Credits and dynamically price virtual goods to increase purchase probability or profit margin, improving monetization.”); OFFERMATIC, <http://www.offeromatic.com> (last visited Oct 7, 2011) (website that gives individuals deals in return for sharing credit card purchase history).

50. See, e.g., SirFlibble, *BitCoin – Fee-Free Paypal Alternative?*, WHIRLPOOL FORUMS (Mar. 21, 2011 6:50 PM), <http://forums.whirlpool.net.au/forum-replies.cfm?t=1663664> (“[I]nternet currenc[ies] have never worked and never will. Paypal, Paymate etc work because they trade in money not fictional widgets.”).

Bitcoin has no built in anti-fraud capabilities, whereas companies like PayPal have invested millions of dollars in protecting customers against fraud.<sup>51</sup>

It is true that one of Bitcoin and other digital currencies' most touted benefits is low transaction costs. However, as online credit card use declines, there is no reason to think that the current payment processing market leaders will not reduce their transaction costs in response to competitive pressure.<sup>52</sup>

## 2. *Micropayments*

Another kind of ecommerce involves very small payments, called micropayments, for digital goods. Because transaction costs through existing payment processors are so large, making payments of, say, 10 cents to 30 cents over the internet is generally impractical. Payments as small as 99 cents were once considered micropayments but companies like Apple have handled 99 cent payments without a hitch using credit cards. Services involving smaller payments are generally non-existent. As credit cards become a less common way to fund online payment accounts, transaction costs are likely to fall, perhaps making micropayments from PayPal and similar processors feasible. Bitcoin could be competitive in this space because of the low transaction costs. Furthermore, the denomination in non-U.S. Dollars is probably less important in this market. YouTipIt is a "microdonation" service that allows individuals to tip websites or businesses using bitcoins.<sup>53</sup> However, a competitor that relies on traditional fiat currencies and PayPal, called Flattr, exists;<sup>54</sup> YouTipIt and similar Bitcoin services may not succeed unless they can offer something that traditional services cannot.

## 3. *Virtual World and Game-Related Commerce*

Aside from traditional ecommerce and micropayments, individuals also engage in commerce in virtual worlds or in games,

---

51. Although Bitcoin is cryptographically secure, fraud is often a result of human rather than technical failure. Scammers can use electronic currencies that do not allow chargebacks to prevent victims from getting their money back.

52. See Bill Zielke, *Why Credit Cards Are Not the Future of Online Payment*, MASHABLE (Mar. 2, 2011), <http://mashable.com/2011/03/02/credit-card-decline> ("[S]enior director of Merchant Services at PayPal" notes that use of credit cards online has declined and will continue to decline because of the inconvenience of using credit cards online and also because of high transaction fees).

53. See YOUTIPIT, <http://www.youtipit.org> (last visited Oct. 7, 2011).

54. See FLATTR, <http://flattr.com> (last visited Oct. 7, 2011).

such as buying or selling digital clothing in Second Life or buying crops in Farmville.<sup>55</sup> While alternative digital currencies failed to gain a foot-hold in real-world ecommerce, they flourish in virtual ecommerce. For example, in the virtual world Second Life, nearly all commerce is transacted in Linden Dollars, with about USD \$50 million worth of transactions monthly at the end of 2009,<sup>56</sup> and about USD \$30 million worth of Linden Dollars in existence at the end of 2010.<sup>57</sup> Facebook recently introduced Facebook Credits, and requires this currency to be used for games like Farmville which run on Facebook. Facebook then takes a commission of 30% of all purchases made with Facebook credits.<sup>58</sup>

As Facebook's huge cut indicates, virtual world and game-related currencies have the potential to be big money makers for the currency issuers. On the other hand, developing a secure virtual currency, protected from fraud, and the accompanying exchanges requires a significant investment of technical and legal expertise, not to mention time. Game-related virtual currencies present other problems too, related to centralized and discretionary control. The central game authority can decide to issue a lot of new currency, either to itself or to users. Doing so may decrease the value of the currency and particularly upset users who keep a nontrivial share of their wealth in the virtual currency, as is probably the case in Second Life. Similarly, if hackers or the government target the issuer's currency system, holders of the currency may be surprised to find their in-game wealth suddenly inaccessible.

Because Bitcoin could alleviate or eliminate a number of these problems, it has the potential to become a de facto standard for certain virtual and game-related currencies. Developers who want to focus on providing an enjoyable virtual or game experience could use Bitcoin instead of reinventing the wheel. At least one developer has already made Bitcoin the in game currency for his virtual world.<sup>59</sup>

---

55. *FarmVille*, WIKIPEDIA, <http://en.wikipedia.org/wiki/FarmVille> (last modified Oct. 25, 2011) (describing gameplay for *FarmVille*).

56. Press Release, Linden Lab, *Second Life Celebrates Major Milestones for Virtual Worlds* (Sept. 22, 2009), available at [http://lindenlab.com/press/releases/22\\_09\\_09](http://lindenlab.com/press/releases/22_09_09).

57. *The Second Life Economy in Q4 2010*, SECONDLIFE BLOGS (Jan. 26, 2011 12:30 PM), <http://community.secondlife.com/t5/Featured-News/The-Second-Life-Economy-in-Q4-2010/ba-p/674618>.

58. See Samuel Axon, *FarmVille Adds Facebook Credits Payment Option*, MASHABLE (Mar. 10, 2010), <http://mashable.com/2010/03/10/farmville-facebook-credits>.

59. See nextnonce, *Bitcoin stole my weekend!*, BITCOIN FORUM (Mar. 15, 2011 8:42:16 PM), <http://bitcointalk.org/index.php?topic=4494.msg65921#msg65921> (describing

The many implementations of Bitcoin would allow the developers to easily integrate Bitcoin functionality into the user interface of the virtual world or game. Similarly, because the company would not be the currency issuer, individuals would not have to worry about the company inflating the currency, failing, and so on. Users might also have more trust in the system knowing that even if the company supporting the game or virtual world fails or is put under legal pressure, the currency will survive.

For a certain subset of games or virtual worlds, however, Bitcoin would be inappropriate. In *World of Warcraft* (WoW), for example, players can earn WoW Gold by accomplishing various in-game tasks. Blizzard, the maker of WoW, no doubt intended for a player's in-game wealth to represent skill and time invested in the game—rather than out-of-game wealth. In this game, as in others, the creators and players may agree that individuals poor in the real world can escape reality and be rich in-game.<sup>60</sup> Thus, the End User License Agreement generally prohibits the out-of-game sale of WoW Gold. Note that this prohibition is generally unsuccessful, with significant WoW Gold traded outside the game.<sup>61</sup> For these kinds of games, Bitcoin would be inappropriate since it is easily converted into other currencies via exchanges.

## B. Gold-Backed Currencies

Certain individuals, called “gold bugs” and “perma bears” are interested in alternative currencies because of their political beliefs and investment predictions.<sup>62</sup> These individuals believe that central banking institutions that have the authority to print more money, like the Federal Reserve, corrupt the economy and therefore they do not trust government-backed fiat currencies (those unredeemable for

---

integration of Bitcoin into a “browser-based MMO (Massively Multiplayer Online) game” at <http://minethings.com>).

60. See, e.g., *Backing in-game currency with Bitcoin seems relatively easy . . .*, BITCOIN FORUM (Feb. 24, 2011), <http://bitcointalk.org/index.php?topic=3798.0> (discussing relative merits of using Bitcoin as in-game currency).

61. See Daniel Terdiman, *Virtual gaming's elusive exchange rates*, CNET NEWS (Aug. 5, 2005 7:18 AM), [http://news.cnet.com/Virtual-gamings-elusive-exchange-rates/2100-1043\\_3-5820137.html](http://news.cnet.com/Virtual-gamings-elusive-exchange-rates/2100-1043_3-5820137.html).

62. See Mike Stathis, *Fool's Gold (Part 1)*, SEEKING ALPHA (July 10, 2009), <http://seekingalpha.com/article/148106-fool-s-gold-part-1>; *Perma-Bears and Gold Bugs*, CONTINENTAL CAPITAL ADVISORS, LLC (Aug. 14, 2009), <http://www.continentalca.com/home/August-14-2009>.

commodities).<sup>63</sup> Accordingly, these individuals prefer to hold their wealth and make exchanges in currencies backed by commodities—usually gold. An analysis of this perspective is beyond the scope of this Article,<sup>64</sup> but a comparison of Bitcoin to other “gold bug” currencies is instructive.

Currencies provide individuals with “tangible medium[s] of exchange that . . . sellers will accept . . . for their goods or services.”<sup>65</sup> Historically, many currencies were “specie,” meaning they were inherently valuable, such as gold or silver coins. To alleviate the problems of carrying around heavy coins, some governments, banks, or private companies created paper money redeemable for a certain amount of gold or another commodity. (Sometimes, these backing entities kept less of the commodity, such as gold, in their reserves than would be necessary if everyone decided to redeem their notes).

In other cases, some governments created paper currencies that were not redeemable for any commodity (or simply eliminated the ability to redeem the currency for the commodity in which it was previously redeemable).<sup>66</sup> These “fiat currencies” had value simply because their backing governments identified the currency as “legal tender”—acceptable for paying legal debts, including taxes.<sup>67</sup> These governments can (and usually do) print more currency over time, increasing the supply of the currency relative to demand, which reduces the value of the currency and correspondingly increases prices in a process known as inflation.<sup>68</sup> More recently, several

---

63. See, e.g., nextnonce, *supra* note 59 (“I’m a huge fan of alternative currencies, especially considering the gross mismanagement of the USD and other fiat currencies.”).

64. The paradigmatic argument is perhaps: Ron Paul, *End the Fed* (2009). In general, most mainstream economists believe that central banks play an important and positive role in economies, and that pegging currencies to gold or other commodities can cause unnecessary economic harms. See BARRY EICHENGREEN, *GOLDEN FETTERS: THE GOLD STANDARD AND THE GREAT DEPRESSION, 1919–1939* Preface (1992); Ben Bernanke, Remarks at the Conference to Honor Milton Friedman at University of Chicago (Nov. 8, 2002), available at <http://www.federalreserve.gov/BOARDDOCS/SPEECHES/2002/20021108/default.htm>.

65. See RICHARD SCOTT CARNELL, JONATHAN R. MACEY & GEOFFREY P. MILLER, *THE LAW OF BANKING AND FINANCIAL INSTITUTIONS* 2 (4th ed. 2009).

66. See, e.g., *Nixon Shock*, WIKIPEDIA, [http://en.wikipedia.org/wiki/Nixon\\_Shock](http://en.wikipedia.org/wiki/Nixon_Shock) (last modified Oct. 25, 2011) (describing how President Nixon ended “convertibility between U.S. dollars and gold”).

67. See Julia Alpert Gladstone, *Exploring the Role of Digital Currency in the Retail Payments System*, 31 *NEW ENG. L. REV.* 1193, 1196 (1997).

68. Control over the money supply is an important lever of monetary policy for governments, which can be used to protect against recessions or depressions. On the other hand, governments can print money irresponsibly and cause hyperinflation. Zimbabwe,

private companies have created digital currencies—some to facilitate e-commerce, as discussed above, but others to serve needs of government-distrusting “gold-bugs.”<sup>69</sup>

Bitcoin is similar to the dozens of gold-backed digital currencies that already exist, such as Pecunix or GoldMoney, because it is liquid, digital, easy for end users to exchange with one another, generally anonymous, and popular among government-distrusting “gold bugs.” However, Bitcoin is different in several key ways: (1) there is no central authority that can issue new currency or defraud holders of the currency (e.g., by holding fractional reserves while promising to hold full reserves), (2) it is fiat money rather than commodity money, and (3) it may be difficult to regulate because there is no centrally controlling authority.

## V. Is Bitcoin Sustainable?

The vast majority of currencies are backed by governments (or other legal entities), commodities, or both. So who would trust Bitcoin, a currency backed by neither? But individuals apparently do trust Bitcoin, buying bitcoins at a rate sufficient to keep Bitcoins almost at parity with the dollar. This part examines whether this trust is misplaced.

### A. Iraqi Swiss Dinar

At least one currency, the Iraqi Swiss Dinar, was backed by neither government nor commodity yet held a stable value and never collapsed over a ten-year period. This fiat currency, printed with Switzerland-manufactured plates, was backed by the Iraqi government before the 1990 Gulf War. Because of sanctions imposed on Iraq during the war that prevented importing more notes, Saddam Hussein’s government disendorsed the old currency and created new “Saddam Dinars.” The Swiss Dinars continued to circulate in northern Kurdish regions of Iraq, maintaining a stable trading value. By contrast, Saddam Hussein printed an enormous amount of new

---

for example, increased its money supply by about 10,000 times in 2008 and experienced a more than 200 million percent inflation rate in 2008. *See Hyperinflataion*, WIKIPEDIA, [http://en.wikipedia.org/wiki/Zimbabwean\\_dollar#Hyperinflation](http://en.wikipedia.org/wiki/Zimbabwean_dollar#Hyperinflation) (last modified Oct. 21, 2011). On currency exchange markets, the value of a currency against other currencies is strongly influenced by predictions regarding inflation and whether a government will be able to meet its debts (as a governments struggles to pay its debts, it will be more likely to print more money, causing inflation).

69. These digital currencies have generally failed to become market leaders in e-commerce, as discussed above. *See generally* Tucker, *supra* note 8.

currency (as did counterfeiters because of the primitive technology used to print the notes), causing hyperinflation in the Saddam Dinars. After the 2003 U.S. invasion of Iraq, the U.S. central provisional authority allowed individuals to trade in Swiss Dinars for new Dinars at an exchange rate of 1 Swiss Dinar to 150 new Dinars.<sup>70</sup>

The Iraqi Swiss Dinar shows that a currency like Bitcoin, without commodity or institutional backing, may be sustainable. Nevertheless, Bitcoin may fail for a variety of reasons, and it behooves Bitcoin users and investors to understand the risks.

## B. Confidence

Like almost anything in which individuals can invest their money, Bitcoin is probably susceptible to irrational bubbles and also irrational or rational loss of confidence, which would collapse demand relative to supply. As explained in more depth below, confidence might collapse in Bitcoin because of unexpected changes in the inflation rate imposed by the software developers or others, a government crackdown, the creation of superior competing alternative currencies, or a deflationary spiral. Confidence might also collapse because of technical problems: if the anonymity of the system is compromised, if money is lost or stolen, or if hackers or governments are able to prevent any new transactions from settling.

### 1. *Improper Use of Discretionary Authority*

Some put confidence in Bitcoin because they believe that Bitcoin has no central institution with discretionary authority to increase the money supply more quickly than the inflation rate built into the software. However, either the developers<sup>71</sup> or a “convincing

---

70. See *History of the CBI*, CENTRAL BANK OF IRAQ, <http://www.cbi.iq/index.php?pid=History> (last visited Oct. 25, 2011) (sections labeled “1990–2003” and “2003–Today”); Mervyn King, *The institutions of monetary policy*—Lecture given at the American Economic Association Annual Meeting, San Diego 7–11 (Jan. 4, 2004), available at <http://www.bis.org/review/r040202b.pdf?frames=0>; *Swiss Dinar*, WIKIPEDIA, [http://en.wikipedia.org/wiki/Swiss\\_dinar](http://en.wikipedia.org/wiki/Swiss_dinar) (last visited Oct. 25, 2011).

71. Although the details of the Bitcoin Protocol, including the inflation rate, were set by Bitcoin’s creator, Satoshi Nakamoto, in 2009, a five-member development team continue to work on the software. They fix bugs, make changes, and issue new releases on the main Bitcoin website. See, e.g., eMansipater, Comment on *Counterfeiting and Loss Prevention*, BITCOIN FORUM (Feb. 25, 2011 3:12:03 AM), <http://bitcointalk.org/index.php?topic=3832.msg54809#msg54809> (describing an instance in which the development team successfully responded to a security flaw that allowed an individual to award himself 184 billion bitcoins by fixing the flaw and eliminating the offending transaction). This development team constitutes the de facto central bank of Bitcoin. If they were to decide that the inflation rate needed to be changed and updated the software,

coalition” (i.e., a group that releases a compatible version of Bitcoin with different inflation settings and convinces a majority of users to switch)<sup>72</sup> could probably exercise discretionary authority to change the inflation rate. Such an exercise of discretion, even if done with good intentions and supported by a majority of Bitcoin users, may nevertheless cause many individuals to lose confidence in Bitcoin and sell off their holdings, starting a panic. Alternatively, if the inflation rate is increased so much that Bitcoin undergoes hyperinflation, Bitcoin’s value would probably drop precipitously.

## 2. *Superior Competing Currency*

A superior competing currency could lead to a crisis of confidence causing either a collapse of Bitcoin’s value<sup>73</sup> or merely a permanent reduction of Bitcoin’s value.<sup>74</sup>

---

most users would probably use the new version of the software because of their trust in the development team. *See id.* (describing instance in which majority of Bitcoin clients switched to a new version of the software). This development team may decide to change core assumptions of the Bitcoin community either because it honestly and correctly believes doing so is in the best interest of the Bitcoin community or because the development team has been co-opted by a particular interest group. As one commentator explained:

Given the project is open-source, what would prevent central banks, governments, keynesians, and other BTC competitors/enemies to infiltrate the community of developers in order to push their own agendas ? One of the possible infiltration attacks could be to push for minting more than 21M BTC and stop the deflationary process built-in in the concept of BTC: lots of economical and political arguments could be used to support this idea in a very rational fashion. Many other infiltration attacks are possible and just up to your imagination.

Sebastiano Scrdina, Comment on *How can Bitcoin be hacked?*, QUORA FORUM (Jan. 24, 2011), <http://www.quora.com/How-can-Bitcoin-be-hacked>.

72. A coalition may take control of the Bitcoin network by convincing a majority of Bitcoin users to use a different version of the software. *See When the majority decides to change the rules*, BITCOIN FORUM (Mar. 21, 2011 4:18:48 PM), <http://bitcointalk.org/index.php?topic=4740.0>. One Bitcoin user has termed this vulnerability “mob rule.” temp1029, Comment on *Counterfeiting and Loss Prevention*, BITCOIN FORUM (Feb 24, 2011 11:06:08 PM), <http://bitcointalk.org/index.php?topic=3832.msg54605#msg54605>. Such a coalition might succeed for any number of reasons. For example, it may argue that Bitcoin is undergoing a deflationary spiral and needs a higher inflation rate to be sustainable. *See, e.g., Would you support moving to a system with controled [sic] inflation?*, BITCOIN FORUM (Mar. 25, 2011 05:06:30 PM), <http://bitcointalk.org/index.php?topic=4940.0> (asking whether a majority would support making the inflation rate constant rather than being halved every four years). Or it may appeal to prejudice, by arguing that a majority of bitcoins are unfairly owned by a disfavored ethnic group, for example, or populism, by arguing that a majority of Bitcoin-denominated debt is owed to wealthy corporations, for example.

73. As some individuals sell bitcoins to buy the new currency other individuals, in a panic, could start to sell their bitcoins at fire-sale prices, afraid of being the last ones to

### 3. *Government Crackdown*

Although Bitcoin may be difficult to shut down because of its decentralized nature, a government crackdown on Bitcoin may nevertheless cause a crisis of confidence—especially if many Bitcoin users do not want to own a currency that is associated with criminality.<sup>75</sup>

### 4. *Deflationary Spiral*

Bitcoin might undergo a deflationary spiral that causes certain individuals or industries to abandon Bitcoin,<sup>76</sup> possibly causing a panic

---

own bitcoins. In some ways, such a large-scale defection would resemble the defections from older to newer technologies where the technologies have “network effects.” For example, Friendster is a social networking site created in 2002, before Facebook. Friendster initially had the largest market share but had a number of technical problems, such as its slow website. Very quickly, Facebook overtook Friendster in the U.S. market, as participants abandoned their Friendster accounts in droves. See, e.g., Gary Rivlin, *The Wallflower at the Web Party*, N. Y. TIMES (Oct. 15, 2006), <http://www.nytimes.com/2006/10/15/business/yourmoney/15friend.html>.

74. A panic would destroy the value of bitcoins if they had value only because many merchants and service providers were willing to accept bitcoins for their goods and services. C.f. FAQ: “Where does the value of Bitcoin stem from?,” BITCOIN WIKI, [https://en.bitcoin.it/wiki/FAQ#Where\\_does\\_the\\_value\\_of\\_Bitcoin\\_stem\\_from\\_What\\_backs\\_up\\_Bitcoin](https://en.bitcoin.it/wiki/FAQ#Where_does_the_value_of_Bitcoin_stem_from_What_backs_up_Bitcoin) (last visited Mar. 26, 2011) (“Bitcoins have value if they are accepted as payment by many. . . . In a sense, you could say that Bitcoin is ‘backed up’ by the price tags of merchants—a price tag is a promise to exchange goods for a specified amount of currency.”). Yet there is another way to value them: as a currency whose supply grows much less slowly over the long term than almost any other currency in existence. Recognizing this value, investors may purchase bitcoins as others dump them in a panic—stabilizing Bitcoin’s value and ensuring its continued existence.

75. In 2006, the U.S. Mint warned consumers that use of Liberty Dollars, an alternative metal-backed currency privately issued in the U.S., is illegal. See Press Release, United States Mint, *Liberty Dollars Not Legal Tender, United States Mint Warns Consumers: Justice Determines Use of Liberty Dollar Medallions as Money is a Crime* (Sept. 14, 2006), available at [http://www.usmint.gov/pressroom/index.cfm?action=press\\_release&id=710](http://www.usmint.gov/pressroom/index.cfm?action=press_release&id=710) [hereinafter U.S. Mint, *Liberty Dollar Consumer Warning*]. Liberty Dollar’s creator complained that the U.S. Mint’s warning had a substantial “chilling effect” and eliminated demand for the currency, causing economic damage to Liberty Dollar owners. Plaintiff’s Complaint at ¶ 15, *Nothaus v. Paulson*, No. 3:07-CV-038 RLY-WGH, 2007 WL 4579959 (S.D. Ind. March 20, 2007).

76. Modern economists, following modern monetary theory, believe that deflation—the decrease in prices over time—can have deleterious effects on an economy. Deflation can lead to a deflationary spiral: prices fall, causing lower production, leading to lower wages, leading to lower demand, and further decreases in prices. Many economists believe that a deflationary spiral caused the Great Depression and other major recessions. To counteract deflation and keep inflation manageable, the U.S. central bank (the Federal Reserve, colloquially known as “the Fed”) manages both the supply and demand for money. Generally, as the supply of money decreases and demand increases, money becomes more valuable and goods cost less in that money. The most well-known tactic the Fed uses is to set the discount window interest rate—the rate at which other banks can

or just a permanent depression in Bitcoin's value. Since the upper limit of bitcoins is fixed at 21 million, bitcoins will become more valuable over time as the supply of government-backed fiat currencies continue to increase.<sup>77</sup> As prices denominated in bitcoins fall, producers may respond by lowering production, leading to lower wages, lower demand, and further decreases in prices.<sup>78</sup> The end result of such a spiral is underemployed human capital and other means of production and destruction of wealth. Thus, industries using Bitcoin<sup>79</sup> that fall into such a spiral may decide to abandon

---

borrow from it. A higher rate discourages borrowing (lowering demand for money) and a lower rate encourages borrowing (increasing demand for money).

77. Unlike the U.S. Dollar, Bitcoin has no central bank that can pull the levers of monetary policy. While the Fed will indefinitely increase the supply of the U.S. Dollar to target a low, stable inflation rate, the supply of Bitcoins is fixed: There will never be more than 21 million bitcoins in existence. Thus, as the supply of other currencies increases faster than the supply of bitcoins increases, bitcoins are likely to continually appreciate in value over time. This is not to say that bitcoins are a good investment: Bitcoin's appreciation may be much lower than investment returns than even the most riskless investments—treasury bills. Furthermore, although the supply of bitcoins will never increase beyond 21 million, demand could always fall over time. Thus, the price of goods in bitcoins will decrease over time, indicating that Bitcoin is a deflationary currency—and may be susceptible to a deflationary spiral.

78. A concern that often goes hand in hand with deflation—the scarcity of small-value currency—is not a problem for Bitcoin. Bitcoins are infinitely divisible, eliminating concerns about the feasibility of sub-“bitpenny” transactions. Newcomers to the Bitcoin community have worried that the fixed number of bitcoins will inhibit Bitcoin's reach because “[there's] not a lot of bitcoins to go round.” Dai, Comment on *When the majority decides to change the rules*, BITCOIN FORUM (Mar. 22, 2011 08:07:01 PM), <http://bitcointalk.org/index.php?topic=4740.msg69876#msg69876>. Although it would be difficult to have transactions in amounts less than one cent, transactions of, say, 0.0004 bitcoins would be simple for programs to handle because bitcoins are infinitely divisible. See, e.g., chodpaba, Comment on *Labor costs and prices in an economy using bitcoin exclusively*, BITCOIN FORUM (Mar. 22, 2011 04:55:50 PM), <http://bitcointalk.org/index.php?topic=4724.msg69762#msg69762> (comparing the feasibility of transactions in “\$.000000001” to transactions of “.000000001 BTC”). Bitcoin users might create new names for certain small amounts of bitcoins to facilitate communication. 0.0004 bitcoins might be referred to as, say, ‘four millibitcoins.’ See, e.g., Meni Rosenfeld, Comment on *If Bitcoins catch on, will people get used to having so few?*, BITCOIN FORUM (Mar. 7, 2011, 1:00:55 PM), <http://bitcointalk.org/index.php?topic=4234.msg61491#msg61491> (suggesting using “mBTC, uBTC and nBTC” for small amounts of bitcoins).

79. See Gavin Andresen, Comment on *Labor costs and prices in an economy using bitcoin exclusively*, BITCOIN FORUM (Mar. 21, 2011 12:37:04 PM), <http://bitcointalk.org/index.php?topic=4724.msg69032#msg69032> (“I think there is a strong possibility bitcoins will end up being used for something none of us is thinking about. Maybe big multinational corporations will use them to pay their international supply chains in industries that are used to constant deflation.”).

Bitcoin. Even the possibility of such a spiral may limit Bitcoin's reach.<sup>80</sup>

### C. Potential Technology Failures

Technology failures could also prevent individuals from transacting in bitcoins or cause a crisis of confidence,<sup>81</sup> as the following three examples illustrate.

#### 1. Anonymity Failure

All Bitcoin transactions are public, but are considered anonymous because nothing ties individuals or organizations to the accounts that are identified in the transactions. However, individuals sometimes post account numbers online in ways that can be connected to their online identities.<sup>82</sup> It might be possible, using statistical techniques and some identified accounts, to undo the anonymity of the system.<sup>83</sup> Such unexpected and sudden exposure would obviously be deleterious to Bitcoin's value.<sup>84</sup>

---

80. epii, Comment on *Would you support moving to a system with controlled [sic] inflation?*, BITCOIN FORUM (Mar. 25, 2011 6:01:05 PM), <http://bitcointalk.org/index.php?topic=4940.msg72218#msg72218> (“The economic future of Bitcoin is still unclear, in no small part because it is treading new economic ground. Though I'm not pessimistic personally, most people will stick with systems like the ones they know until they understand enough such that making the change is something they can do with confidence.”).

81. See *Weaknesses*, BITCOIN WIKI, <https://en.bitcoin.it/wiki/Weaknesses> (last visited Mar. 26, 2011) (listing a number of potential technological vulnerabilities).

82. Many participants in the Bitcoin Forums post a Bitcoin account number to receive a tip for a good quality post. See, e.g., Bitcoiner, Comment on *Anonymity*, BITCOIN FORUM (July 7, 2010 11:20:49 pm), <http://bitcointalk.org/index.php?topic=241.msg2044#msg2044> (user signature of “Want to thank me for this post? Donate here! Flip your coins over to: 13Cq8AmdrqewatRxEyU2xNuMvegbaLCvEe”).

83. See *Anonymity*, BITCOIN WIKI, <https://en.bitcoin.it/wiki/Anonymity> (last visited Mar. 26, 2011); see also theymos, *Anonymity*, BITCOIN FORUM (July 07, 2010 4:54:44 PM), <http://bitcointalk.org/index.php?topic=241.0>.

84. Anonymity is an important feature to many current Bitcoin users. See, e.g., nimmul, Comment on *Anonymity*, BITCOIN FORUM (Aug. 12, 2011 11:52:38 AM) <http://bitcointalk.org/index.php?topic=241.msg8874#msg8874> (“For me, anonymity is the only feature I need”); *Why do you use Bitcoin?*, BITCOIN FORUM (Mar. 14, 2011), <http://bitcointalk.org/index.php?topic=4465.0> (several comments indicating that individuals use Bitcoin because of the anonymity it provides). Similarly, mainstream consumers generally prefer that their transactions remain between them, their financial intermediaries (e.g., credit card companies), and merchants. See, e.g., Ryan Anderson, *Facebook, Beacon, and Privacy*, THE NEW PR (Nov. 26, 2007), <http://www.ryananderson.ca/2007/11/26/facebook-beacon-and-privacy/> (recounting story of Facebook user who bought an engagement ring from overstock.com and was horrified to

## 2. *Theft*

Like cash, bitcoins can be lost or stolen.<sup>85</sup> Keeping bitcoins on one's computer can be as dangerous as keeping large sums of cash in one's physical wallet, and each user should take care to backup and secure his Bitcoin wallet.<sup>86</sup> A large-scale theft of bitcoins from many users could create a confidence crisis.<sup>87</sup> Such theft could occur by a virus or trojan horse that installs itself on a Bitcoin user's computer and sends the wallet file to the criminal who wrote the software.<sup>88</sup>

## 3. *Denial of Service*

Although Bitcoin is decentralized and generally has no single point of failure, it is nevertheless susceptible to a form of denial of service attack.<sup>89</sup> Individuals with a majority of the computational power in the Bitcoin mining network can effectively preclude any transaction from being processed. Such a sustained attack might significantly depress the exchange rate and lead to a collapse of

---

find that the surprise was ruined when the purchase was posted, without his consent, in his newsfeed for his girlfriend and friends to see).

85. Bitcoins are generally stored in a "wallet." Individuals may store the wallet on their own computers or with an ewallet service.

86. See, e.g., *FAQ: How do I backup my wallet?*, BITCOIN WIKI, [http://en.bitcoin.it/wiki/FAQ#How\\_do\\_I\\_backup\\_my\\_wallet](http://en.bitcoin.it/wiki/FAQ#How_do_I_backup_my_wallet) (last visited Mar. 26, 2011).

87. But see Heather C. Alston, Comment, *Will That Be Cash, Credit, or E-Money*, 1 N.C. BANKING INST. 225, 253 (1997) ("[C]ustomers . . . want to know what will be done in the event that their hard drive crashes with stored e-money . . ."). Although few individuals backed up in 1997, since then, regularly backing up has become customary for mainstream computer users.

88. Bitcoin trojan horses already exist. See Matt Corallo, *The case of the Russian Scammer*, BITCOIN FORUM (Feb. 19, 2011 5:21:35 PM), <http://bitcointalk.org/index.php?topic=3628.msg51389#msg51389>; see also Matt Corallo, Comment on *A simple application to backup your wallet in Dropbox and Gmail [scam]*, BITCOIN FORUM (Feb. 19, 2011 5:01:22 PM), <http://bitcointalk.org/index.php?topic=3596.20>. A scammer created a program that purported to backup a user's wallet file but instead emailed the file to the creator of the software and deleted the wallet from the user's computer. *Id.* Using this program, the scammer was able to steal more than 150 bitcoins from a number of users. *Id.* Because the Bitcoin wallet is not encrypted, such theft is fairly simple. See Bruce Wagner, "Automatic Encrytion [sic] and Password Protection of wallet.dat File?", BITCOIN FORUM (Nov. 19, 2010 11:19:15 PM), <http://bitcointalk.org/index.php?topic=1852.msg22948#msg22948>. These problems can be mitigated to some extent by making the Bitcoin software secure. However, using an online wallet service that secures, backups, and guarantees users' bitcoins may be a more secure option—but only if reliable and legally accountable. See Cryptoman, *Lost money on MyBitcoin.com? Report it here. [UPDATE: funds recovered]*, BITCOIN FORUM (Feb. 18, 2011 4:46:08 PM), <http://bitcointalk.org/index.php?topic=3597.0> (some individuals questioning the reliability of some popular ewallet providers)).

89. See, e.g., Sebastiano Scrofina, Comment on *How can Bitcoin be hacked?*, QUORA FORUM (Jan. 24, 2011), <http://www.quora.com/How-can-Bitcoin-be-hacked>.

confidence. Obtaining the necessary computational power is easy, if expensive.<sup>90</sup> Although some question why anyone would do such a thing,<sup>91</sup> several parties might have sufficient interest: governments who want to shut Bitcoin down,<sup>92</sup> individuals with future liabilities in bitcoins,<sup>93</sup> or hackers who want to blackmail a business that relies on bitcoins.

As the Iraqi Swiss Dinar illustrates, Bitcoin's lack of commodity or government backing alone does not doom Bitcoin to failure. However, potential users should be aware that it is still a young and developing currency, and could potentially fail in many ways.

## VI. Legal Issues

Although Bitcoin may be more resistant to government attack because of its decentralized nature, many Bitcoin users, including

---

90. Gaining control of the network in order to prevent transactions from settling would cost, in March 2011, on the order of a million dollars, plus electricity costs. The total power in the Bitcoin mining network is currently about 500 Giga-hashes per second. A specialized processor called a GPU that can calculate at approximately 600 Mega-hashes per second costs approximately \$600. Thus, the current network has a power of about 1000 of these GPUs. An individual would need to spend around \$600,000 (plus costs for supporting infrastructure) to control a majority of the processing power on the network. See ripper234, *Can you retort/refute this attack on Bitcoin?*, BITCOIN FORUM (Mar. 28, 2011 8:37:17 AM), <http://bitcointalk.org/index.php?topic=5048.0>.

Incredible computational power can be purchased from cloud computing providers over the internet. See, e.g., *Amazon Elastic Compute Cloud*, WIKIPEDIA, [http://en.wikipedia.org/wiki/Amazon\\_Elastic\\_Compute\\_Cloud](http://en.wikipedia.org/wiki/Amazon_Elastic_Compute_Cloud) (last visited Oct. 25, 2011). Hackers control and sell use of huge networks of computers called "botnets," see *Botnet*, WIKIPEDIA, <http://en.wikipedia.org/wiki/Botnet> (last visited Oct. 25, 2011). And government agencies such as the CIA and NSA likely have significant computational power at their disposal.

91. One user notes that even if an individual dominates the network, that entity will never earn more than fifty bitcoins every ten minutes. See Nhdb, Comment on *What stops people with capable of [sic] massive amounts of cpu power . . . from mining all of the remaining bitcoins?*, REDDIT (Mar. 24, 2011), [http://www.reddit.com/r/Bitcoin/comments/gam37/what\\_stops\\_people\\_with\\_capable\\_of\\_massive\\_amounts/c1m73fv](http://www.reddit.com/r/Bitcoin/comments/gam37/what_stops_people_with_capable_of_massive_amounts/c1m73fv).

However, this amounts to substantial gross revenues of approximately USD \$2.4 million per year. (Bitcoin only awards 50 bitcoins every 10 minutes; 0.9 USD / bitcoin \* 50 bitcoins / 10 minutes x 60 minutes / hour x 24 hours / day x 365 days / year = USD \$2.4 million). Although gaining control of a majority of the mining network would cost on the order of \$1 million, see *supra* note 90, electricity and other infrastructure costs would eat into this profit significantly.

92. Governments may have an interest in shutting Bitcoin down because it is anonymous and consequently might facilitate illegal drug dealing, child pornography, and money laundering.

93. Individuals who have future liabilities in bitcoins, such as a borrower or a futures contract party, have significant incentive to reduce their future liabilities by generally wreaking havoc in the system to collapse the value of the currency.

both consumers and businesses, are anxious about its legal status. That it may exist in a legal grey area may significantly hamper demand for bitcoins. This Part examines just a few of the many relevant legal issues.

#### A. Federal Government's Monopoly on Issuing Currencies

Commentators often write that the federal government has an “exclusive right to issue currency”<sup>94</sup> because of the Constitution’s assignment of control over currency to Congress to the exclusion of states<sup>95</sup> and the Federal Reserve’s control over the money supply. To those taking the federal government’s monopoly at face value, the recent conviction of a creator of a private currency called the Liberty Dollar comes as no surprise. The Department of Justice, in a press release noting the conviction, stated “It is a violation of federal law . . . to create private coin or currency systems to compete with the official coinage and currency of the United States.”<sup>96</sup>

However, organizations have been issuing a certain type of private currency—community currencies meant to circulate only within a particular community—in the U.S. for decades. Government officials have known about these currencies and have commented that they seem to pose no threat.<sup>97</sup> Thus, the government’s supposed monopoly is more limited than it may seem at first.

The Constitution has nothing to say about private parties creating money.<sup>98</sup> Instead, two sets of federal statutes affect private

---

94. See, e.g., Brian W. Smith & Ramsey J. Wilson, *How Best to Guide the Evolution of Electronic Currency Law*, 46 AM. U. L. REV. 1105, 1111 (1996–1997).

95. The Constitution gives Congress the power to “To coin Money” and “regulate the Value thereof,” U.S. Const. art I § 8, and prohibits states from “coin[ing] money.” U.S. Const art I § 10.

96. DOJ, *Liberty Dollar Conviction Release*, *supra* note 10.

97. See Barbara A. Good, *Private Money: Everything Old is New Again*, ECONOMIC COMMENTARY (Fed. Reserve Bank of Cleveland), Apr. 1, 1998, available at <http://www.clevelandfed.org/research/commentary/1998/0401.pdf> (discussing Ithaca Hours and other local, private currencies and noting that “Private money is not prohibited if it complies with certain government regulations”); Smith & Wilson, *supra* note 94, at 1115 n.55 (comments by Federal Reserve Chairman Alan Greenspan that “some of the recent speculation about risks to monetary policy . . . has been a bit alarmist;” remarks by Edward W. Kelley, Jr., Member, Board of Governors of the Federal Reserve System, that “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.”).

98. LEWIS D. SOLOMON, RETHINKING OUR CENTRALIZED MONETARY SYSTEM: THE CASE FOR A SYSTEM OF LOCAL CURRENCIES 95–96 (1996).

parties' abilities to create currencies: The Stamp Payments Act of 1862 and federal counterfeiting statutes.

1. *The Stamp Payments Act of 1862*

In the nineteenth century, inflation caused the metal in small-value official coins to become more valuable than the face value of the coins themselves. People hoarded these coins, causing a shortage. In order to make change for customers, companies used privately issued currencies in the form of notes or tokens in small denominations.<sup>99</sup>

Economists and politicians argued that these private currencies were endangering the economy and contributing to inflation. About a dozen states prohibited private issue of notes and tokens in values less than \$5. Congress, deciding that a federal response was prudent, adopted the substance of these state laws as section 2 of the Stamp Payments Act, and in section 1, allowed U.S. postage stamps to be used for government debts less than \$5, later amended to \$1. Section 1 was quickly repealed, but Section 2 is still in effect.

Section 2 of the Stamp Payments Act of 1862 states:

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.<sup>100</sup>

Judicial interpretations of the Act and its precursors indicate that the touchstone of the Act is competition with official currency. In a 1938 case the Supreme Court reversed a conviction of a Railroad worker who had been convicted of violating a statute very similar to the 1862 Act for giving privately issued \$1 notes as change to travelers who purchased their tickets with \$5 notes. The indictments were insufficient as a matter of law because the notes were not averred to be "paper currency," or "paper medium evidently intended for common circulation."<sup>101</sup> Importantly, the legislative history for a recodification of the Act interpreted this case as meaning that

---

99. Thomas P. Vartanian, et al, *Echoes of the Past With Implications for the Future: The Stamp Payments Act of 1862 and Electronic Commerce*, BNA's Banking Report (Sept. 23, 1996).

100. 18 U.S.C. § 336.

101. *Stettinius v. United States*, 22 F. Cas. 1322, 1334 (C.C.D.D.C. 1839) (No. 13387) (quoting Act July 7, 1838, § 1, 5 Stat. 297).

commercial instruments, such as checks, for small amounts were not prohibited.<sup>102</sup>

In *Monongahela Bridge Co*, the District Court for the Western District of Pennsylvania rejected a conviction against a bridge company based on “issuing paper tickets to be received for toll.”<sup>103</sup> The tickets had printed on their face “Monongahela Bridge—good for one trip.” The judge found that unlike tokens issued by merchants that were prohibited by the Act, these tickets did not resemble U.S. coins or stamps “in shape, design or material” and “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.”<sup>104</sup> According to the judge, the Act was designed to promote the “free and untrammelled circulation” of U.S. coins and postage.<sup>105</sup> Further, the Judge expounded that money is a universal medium of exchange, “the one thing acceptable to all men, and in exchange for which they will give any commodity they possess.”<sup>106</sup> Sovereign governments have the power to make money and may punish infringements on its power.<sup>107</sup>

In the Supreme Court case *United States v. Van Auken*, the defendant was indicted for circulating 50-cent store gift certificates with the imprint “The Bangor Furnace Company will pay the bearer, on demand, fifty cents, in goods, at their store, in Bangor, Mich.”<sup>108</sup> The Supreme Court first made a purpose-based analysis of the Act. The Supreme Court, like the Pennsylvania District Court, found that the goal was to “secure, as far as possible, the field for [official small value currency], without competition from any quarter.”<sup>109</sup> Certificates payable in specific goods would only circulate locally and would not compete with official currency, the Supreme Court held, and Congress could not have intended to prohibit such certificates.<sup>110</sup>

Next, the Supreme Court referred to the Act’s text. It found that the reference to notes and checks, which are instruments of money,

---

102. Vartanian, *supra* note 99, at nn. 24–25 and accompanying text.

103. *United States v. Monongahela Bridge Co.*, 26 F. Cas. 1292, 1292 (W.D. Pa. 1863) (No. 15796).

104. *Id.* at 1293–93.

105. *Id.* at 1292.

106. *Id.* at 1293.

107. *Id.*

108. *United States v. Van Auken*, 96 U.S. 366, 368 (U.S. 1878).

109. *Id.* at 367.

110. *Id.* at 368.

limited the reach of the remaining words to notes for money.<sup>111</sup> In other words, the Act only applies to things “measurable by the pecuniary standard” and not to anything measured, for example, “by the pound, the gallon, the yard.” It found further support for this interpretation in a dictionary definition of “sum,” which was “quantity of money or currency.”<sup>112</sup> Thus, the statute’s inclusion of “obligation[s] for a less sum than \$1” meant the same thing as “for a less sum of money than one dollar.”<sup>113</sup> Therefore, a certificate payable in goods at a specific store—even for a specific dollar value of goods—was not “for a less sum than \$1” because it was not an obligation payable in money or currency.<sup>114</sup>

In *United States v. Roussopulous*, the District Court of the District of Minnesota cited *Van Auken* in rejecting an indictment against a defendant for issuing metal tokens that were redeemable for 50 cents worth of goods at a particular store.<sup>115</sup> First, because the tokens were payable in goods, they were not payable in money, as required by the statute.<sup>116</sup> Second, the Court found that the form of the token was so different from all official coinage that the token “does not purport to be a piece of money,” and “cannot, therefore, have been intended to circulate as money.”<sup>117</sup>

From these cases, the following factors in determining competition with official currency can be derived. The Act is unlikely to apply to anything that (1) circulates in a limited area,<sup>118</sup> (2) is redeemable only in goods, (3) does not resemble official U.S. currency and is otherwise unlikely to compete with small-denominations of U.S. currency,<sup>119</sup> or (4) is a commercial check (such as a customer might make out to a store to buy something worth less than \$1).<sup>120</sup>

---

111. *Id.*

112. *Id.*

113. *Id.*

114. *Id.* at 368–69.

115. 95 F. 977, 978 (D. Minn. 1899).

116. *Id.*

117. *Id.*

118. *See United States v. Van Auken*, 96 U.S. 366, 368 (U.S. 1878).

119. Vartanian, *supra* note 99 (citing *Van Auken*; *United States v. Monongahela Bridge Co.*, 26 F. Cas. 1292 (W.D. Pa. 1863) (No. 15796); *United States v. Roussopulous*, 95 F. 977 (D. Minn. 1899)).

120. *See Stettinius v. United States*, 22 F. Cas. 1322, 1324 (C.C.D.D.C. 1839) (No. 13387).

Although the motivations behind the Stamp Payments Act have long since passed, the law has not been repealed, and has been stylistically amended a number of times without consideration of its present day application.<sup>121</sup>

A number of existing “community currencies,” such as Ithaca Dollars, Berkshares, and LETS, have avoided any legal attack under the Act by creating notes only in values greater than \$1.<sup>122</sup> These currencies may also fall outside the Act’s reach because they are intended to circulate only locally, and because their scrip is often denominated in “hours” rather than dollars.<sup>123</sup> Although the case against Liberty Dollars might have been straightforward under the Act, Liberty Dollar coins and paper currency were never created in denominations smaller than \$1.<sup>124</sup>

Virtual world currencies, such as Linden Dollars or World of Warcraft Gold, likely fall outside the Act’s reach because these currencies are not “intended to circulate as money or to be received or used in lieu of lawful money of the United States.” These currencies can generally only be used to purchase *virtual* goods in a particular virtual environment, and, like currencies redeemable only in goods or that only circulate in a limited area, are unlikely to compete with official coinage.<sup>125</sup>

One view is that Bitcoin, like most digital currencies, is different from community currencies, virtual world currencies, and gift certificates in ways that make Bitcoin more likely to fall within the Act. First, unlike community currencies, Bitcoin does not limit transactions to those worth more than \$1.<sup>126</sup> Second, several factors

---

121. Vartanian, *supra* note 99.

122. See, e.g., Ellen Graham, *Community Groups Print Local (and Legal) Currencies*, WALL ST. J., June 27, 1996, at B1; Paul Glover, *Creating Community Economics with Local Currency*, <http://www.paulglover.org/hourintro.html> (last visited Oct. 25, 2011) (noting that Ithaca Hours are legal, among other reasons, because “denominations are at least \$1.00 value”); Good, *supra* note 97 (noting that community currencies are legal if, inter alia, they are “issued in denominations valued at a minimum of \$1”).

123. See, e.g., Paul Glover, *The Ithaca HOUR Family*, <http://www.paulglover.org/hourcurrency.html> (last visited Oct. 25, 2011) (indicating denominations of “One HOUR,” “Half HOUR,” “Quarter HOUR,” “Eighth HOUR,” and “Two HOURS”).

124. See Susan Headley, *What are NORFED Liberty Dollar Coins?: U.S. Mint Warns About NORFED Liberty Dollar U.S. Coin Lookalikes!*, ABOUT.COM, <http://coins.about.com/od/coinbuyingadvice/qt/libertydollars.htm> (last visited Apr. 2, 2011) (noting denominations of Liberty Dollars that are all \$1 or greater). Additionally, punishment under the Stamps Payment Act is limited to six month imprisonment—much less than under the statutes by which von NotHaus was ultimately convicted.

125. See *United States v. Van Auken*, 96 U.S. 366, 368 (U.S. 1878).

126. See Vartanian, *supra* note 99.

indicate that Bitcoin is intended to compete with official currency. Bitcoin supporters proselytize its acceptance by merchants and individuals in parallel with or in lieu of dollars, and many merchants, offering many different kinds of goods and services, accept bitcoins as payment. Bitcoins are not limited to a particular geographic area but instead are used everywhere in the U.S. (and the world) where dollars could be used—i.e., where there is Internet access. Thus, one might argue that Bitcoin is a “token . . . 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,” violating the Stamp Payments Act.

However, using the Supreme Court’s approach in *Van Auken*—analyzing the Act’s purpose and closely reading its text—the better reading is that Bitcoin does not fall within the Act. First, banning Bitcoin would not promote Congress’s goal in passing the Act of preventing competition with U.S. coins. Bitcoin is mainly used over the Internet and therefore competes with credit cards, PayPal, and checks rather than U.S. coins. Today, Bitcoin is rarely used in face-to-face transactions in which it would compete with U.S. coins.

Second, because the Act provides criminal penalties, a court may narrowly interpret it and conclude that because a nineteenth-century Congress could not have conceived of digital currencies, they cannot be within the scope of the Act.<sup>127</sup> For example, in *United States v. Gellman*, the court warned that early money-related laws providing criminal penalties should be cautiously applied to new technologies.<sup>128</sup> In that case, the defendants were charged with violating counterfeiting statutes by manufacturing inexpensive metal coins in the size and shape of U.S. coins that were meant to fool vending machines, jukeboxes, parking meters, and so on. The standard courts had used in applying these counterfeiting statutes was whether the coins would “deceive a person using ordinary caution,”<sup>129</sup> but the coins in *Gellman* would not deceive a person because they contained the inscriptions “No Cash Value” and “Good for Amusement Only” and had no numbers inscribed on them. The Court rejected the prosecution’s request for a new “mechanical test” that would apply to these new coins. The court concluded that:

---

127. *Id.*

128. *United States v. Gellman*, 44 F. Supp. 360, 365–66 (D. Minn. 1942).

129. *Id.* at 363 (quoting *United States v. Bogart*, 24 F. Cas. 1185 (N.D.N.Y. 1878) (No. 14,617)).

The difficulty is that this indictment seeks to charge the defendants with an offense under statutes which were enacted over one hundred years ago when vending machines probably did not exist. They were never framed to embrace the use of metal tokens as a substitution for money in the limited sense referred to. While the Court is not unmindful that there should be some curb on the fraud that is being perpetrated by the use of these slugs or tokens, relief must be sought from Congress and not from the courts. . . . A criminal statute must be strictly construed, and to apply these statutes to the factual situation disclosed by this evidence would be entirely unwarranted.<sup>130</sup>

A close reading of the text supports these purpose-based arguments. Although digital currencies are often described as “digital tokens,” a “note, check, memorandum, token, or other obligation” in the statute are all physical manifestations of currency, indicating that the statute was only meant to extend to physical instruments and not to digital currencies.<sup>131</sup> Although the phrase “other obligation” may be general enough to refer to something that is not physical, the principle of *ejusdem generis* indicates that it should be interpreted as only referring to physically manifested things.

On the other hand, one could argue that Congress did not need to conceive of digital currencies to create a statute that would prohibit them if they fell within the clear meaning of the text and aim of the statute.<sup>132</sup> Thus, the better textual argument is that bitcoins are

---

130. *Id.* at 365–66.

131. *Id.*

132. Two other arguments can be made in favor of Bitcoin that suffer the same flaw as the “physical manifestation theory.” Aside from this argument about Bitcoin not being an obligation, just as the Supreme Court found in *Van Auken* that scrip redeemable in goods is not “for a less sum than \$1,” *United States v. Van Auken*, 96 U.S. 366 (U.S. 1878), a court may find that a bitcoin, which is not redeemable for any particular thing and is not pegged to the dollar, is not “for a less sum than \$1.” See Vartanian, *supra* note 99. One could also argue that while Bitcoin users intend for bitcoins to circulate as money, they do not do so within the meaning of the Act because the word “circulate” in the phrase “circulate as money” refers to *physical* circulation or because “money” refers to physical manifestations of money, (although such an interpretation seems overly formalistic.) Such an argument was made by a former General Counsel for the Office of the Comptroller of the Currency and also MasterCard. See Smith & Wilson, *supra* note 94, at 1110 (“The SPA may be inapplicable to all forms of electronic currency, because such currencies lack the physical characteristics of U.S. currency. Instruments that do not have the physical characteristics of U.S. coins or paper currency cannot be ‘intended to circulate as money.’”). *But see id.* (“If faced with an ether-based payment system, however, 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.”).

not “obligations” and therefore fall outside the list.<sup>133</sup> Each of the items in the list of things proscribed by the Act is an obligation, as confirmed by the last phrase, “or other obligation.” Most of the cases brought under the Act dealt with “obligations,” such as a paper ticket that obligated the issuer to provide passage across a bridge or scrip that obligated the issuer to provide 50 cents in merchandise. A bitcoin, however, is not an obligation—it has value only because other individuals are willing to ascribe it value and not because any entity has promised to provide something in return for a bitcoin. Thus, a bitcoin may not be a “token” within the statute’s meaning because it is not an obligation.

In personal correspondence, Professor Ronald Mann of Columbia Law School, who conducts research on payment systems and electronic commerce among other topics, disagreed with using the word “obligations” to narrow the scope the statute. According to Mann, “[T]hat reading can’t prevail, I think, because the statute plainly would cover a private coin that was valued based solely on its metallic content (and thus was not an ‘obligation’). Because I think Bitcoin is pretty clearly a ‘token,’ albeit an electronic one, I would argue it is covered.”

However, the evidence against Professor Mann’s interpretation is strong. The only evidence for his view is the word “token,” which colloquially may describe any metal coins used as currency. However, Webster’s Dictionary defines “token,” in relevant part, as “[a] piece of metal intended for currency, and issued by a private party, usually bearing the name of the issuer, and redeemable in lawful money . . .”<sup>134</sup> The first part of this definition describes something that is *redeemable*—that is, an obligation—rather than a coin that is valued based solely on its metallic content (i.e., “specie”). Thus, mere use of the word “token” does not bring specie within the statute.

Furthermore, no evidence indicates that the statute was aimed at specie. Money in nineteenth-century America before the passage of the Stamp Payments Act consisted mostly of bank notes.<sup>135</sup> Although specie was probably the most trusted store of value, it was chronically

---

133. *C.f.* Kerry Lynn Macintosh, *The New Money*, 14 BERKELEY TECH. L.J. 659, 672 n.78 (1999) (“An argument can be made that ‘obligation’ was never intended to include electronic money . . .”).

134. WEBSTER’S THIRD INTERNATIONAL DICTIONARY OF THE ENGLISH LANGUAGE UNABRIDGED 2404 (Philip B. Grove et al., eds., 3rd ed. 1993) (Token definition seven is cited.).

135. CARNELL, MACEY & MILLER, *supra* note 65, at 7.

scarce.<sup>136</sup> It was extremely unlikely that businesses wanting to make change would use extremely valuable specie to do so. As the legislative history indicates, the Act was instead aimed at “shinplasters,”<sup>137</sup> a derogatory term for worthless privately issued notes and tokens.<sup>138</sup> Underscoring that the target of the Act was worthless obligations, the Treasury Secretary wrote in a letter to Congress in support of the Act that “The depreciation of [official] currency, result[s], in great measure, from the unrestricted issues of *non-specie-paying banks* and unauthorized associations and persons . . . .”<sup>139</sup>

Perhaps the best argument against the application of the Act to Bitcoin is pragmatic. It is a 150-year-old statute that has outlived its usefulness. Courts began limiting its application almost immediately after it was passed.<sup>140</sup> Although many academic works have noted that the Stamp Payments Act may be a problem for digital currencies,<sup>141</sup> and digital currencies have existed for more than a decade, there has been no published court opinion interpreting the Act since 1899.<sup>142</sup> And the comparatively lenient punishments available for violations of the Act (fine and maximum six month imprisonment) and availability of more fitting statutes under which to

---

136. *Id.* at 2, 5, 7.

137. CONG. GLOBE, 37th Cong., 2d Sess. 3405 (1862), available at <http://memory.loc.gov/cgi-bin/ampage?collId=llcg&fileName=061/llcg061.db&recNum=526> (Congressman Phelps, speaking in opposition to the Act on Constitutional grounds stated that “I am as much in favor as any member on the floor of this House of preventing the circulation of shinplasters.”).

138. See Vartanian, *supra* note 99.

139. CONG. GLOBE, 37th Cong., 2d Sess. 3405 (1862) (emphasis added).

140. The initial Act was passed in response to private issuers creating small-denomination tokens or scrip, often redeemable only in merchandise from the issuer. Thus, the court’s finding in *Van Auken* that scrip redeemable only for goods was not prohibited by the Act is questionable. Furthermore, although one may argue that a single issuer’s scrip circulating in a limited area may not compete with official U.S. currency, there is no question that many such private currencies circulating would, taken together, challenge the monopoly of official stamps and coins. Thus, the court limited the Act by interpreting it more narrowly than the text and intentions of Congress would indicate it should have been.

141. See, e.g., Vartanian, *supra* note 99; Smith & Wilson, *supra* note 94; Macintosh, *supra* note 133, at 671–72.

142. See *United States v. Roussopolous*, 95 F. 977 (D. Minn. 1899). A search of Google Scholar and Westlaw has found no case interpreting Section 2 of the Stamp Payments Act since *Roussopolous*.

attack Bitcoin, as described *infra*, are likely to dissuade prosecutors from trying to breathe new life into the Stamps Payment Act.<sup>143</sup>

## 2. *Prohibition on Coining Current Money and the Liberty Dollar Saga*

Bernard von NotHaus started printing and distributing metallic and paper currency called Liberty Dollars in 1998.<sup>144</sup> The currency was backed by gold, silver, or other precious metals, and was intended to be inflation-proof, unlike the U.S. Dollar.<sup>145</sup> The U.S. Mint warned consumers about the Liberty Dollar in 2006,<sup>146</sup> NotHaus's offices were raided by the FBI and Secret Service in 2007,<sup>147</sup> and NotHaus was indicted in 2009<sup>148</sup> and convicted in March 2011.<sup>149</sup> In press releases related to the indictment and conviction, the Department of Justice made several statements that seemed extremely hostile to private currencies, going as far as referring to NotHaus as a "domestic terrorist."<sup>150</sup> NotHaus himself believes that his indictment and

---

143. Nevertheless, the Act, having outlived its usefulness and perhaps impeding the development of digital currencies, should be repealed. See Macintosh, *supra* note 133, at 671–73.

144. Indictment at ¶¶ 1, 13–15, 19, *United States v. NotHaus*, 5:09CR27, (W.D.N.C. May 19, 2009).

145. *Id.* at ¶¶ 14, 15, 19.

146. U.S. Mint, *Liberty Dollar Consumer Warning*, *supra* note 75.

147. *Frontal Assault on Freedom: FBI Raids Liberty Dollar*, THE RABID QUILL (Nov. 15, 2007), available at <http://replay.waybackmachine.org/20080117060339/http://www.rabidquill.com/2007/11/15/frontal-assault-on-freedom-fbi-raids-liberty-dollar> (including text of e-mail message from Bernard von NotHaus describing the raid); *Liberty Dollar Office Raided*, EVANSVILLE COURIER & PRESS (Nov. 15, 2007 1:42 PM), <http://www.courierpress.com/news/2007/nov/15/liberty-dollar-office-raided>.

148. Press Release, United States Attorney's Office, Western District of North Carolina, *Four Defendants Indicted in Unlawful Coin Operation* (June 3, 2009), available at <http://charlotte.fbi.gov/dojpressrel/pressrel09/ce060309.htm> [hereinafter DOJ, *Liberty Dollar Indictment Release*].

149. DOJ, *Liberty Dollar Conviction Release*, *supra* note 10.

150. In noting the indictment, the DOJ press release quoted an FBI special agent: "People understand that there is only one legal currency in the United States. When groups try to replace the U.S. dollar with coins and bills that don't hold the same value, it affects the economy." DOJ, *Liberty Dollar Indictment Release*, *supra* note 148. The press release noting the conviction stated: "Along with the power to coin money, Congress has the concurrent power to restrain the circulation of money which is not issued under its own authority in order to protect and preserve the constitutional currency for the benefit of all citizens of the nation. It is a violation of federal law for individuals, such as von NotHaus, or organizations, such as NORFED, to create private coin or currency systems to compete with the official coinage and currency of the United States." DOJ, *Liberty Dollar Conviction Release*, *supra* note 10. Furthermore, the release quoted a U.S. Attorney as saying: "Attempts to undermine the legitimate currency of this country are simply a unique form of domestic terrorism . . ." *Id.*

conviction were “political,”<sup>151</sup> ostensibly because the federal government is hostile to private currencies.

As a threshold matter, the statutes under which NotHaus was convicted, 18 U.S.C. §§ 485 and 486, are inapplicable to Bitcoin because they only deal with metal coins or coins or bars that resemble official U.S. or foreign currency.<sup>152</sup> Nevertheless, some have mused that the attack on Liberty Dollar indicate that Bitcoin will be next. Such fears are magnified by the political overlap between NotHaus and Liberty Dollar users, on the one hand, and some Bitcoin users on the other: gold-bugs who believe that the Federal Reserve does harm to the economy and that the existence of an inflation resistant currency would benefit the economy.<sup>153</sup>

However, the Liberty Dollar government action is best understood as an attack on counterfeiting and fraud rather than as the first salvo in a war against private currencies,<sup>154</sup> as confirmed by Assistant U.S. Attorney (AUSA) Jill Westmoreland Rose, who successfully prosecuted NotHaus.<sup>155</sup> In a 2006 U.S. Mint press

---

151. NotHaus told me that his conviction was “political.” Telephone Interview with Bernard von NotHaus (Apr. 12, 2011) [hereinafter NotHaus Interview]. When I asked him why he believed so, he told me “it’s a fact, not a belief.” *Id.*

152. Section 485 is titled “Coins or bars,” and is clearly limited to “coins” or “bars” that are counterfeit and resemble official U.S. or foreign currency. Section 486, titled “Uttering coins of gold, silver or other metal,” only deals with “coins of . . . metal.” A Bitcoin is a digital token rather than a coin or a bar and does not resemble any official currency.

153. Reached after his conviction, NotHaus told me that that U.S. Dollars are “fiat pieces of shit.” NotHaus Interview, *supra* note 151. He also said, “I suggest you get hip to the monetary system. Wake up and smell the stench.” *Id.*

154. *C.f.* Seth Lipsky, Op-Ed., *When Private Money Becomes a Felony Offense: The Popular Revolt Against a Declining Dollar Leads to a Curious Conviction*, WALL ST. J. (Mar. 31, 2011), <http://online.wsj.com/article/SB10001424052748704425804576220383673608952.html> (noting the apparent mismatch between theories of counterfeit used in the trial, on the one hand, and language in the conviction press release indicating that private currencies are illegal).

155. Telephone Interview with Jill Westmoreland Rose, Assistant U.S. Attorney, Western District of North Carolina (Apr. 7, 2011) [hereinafter Rose Interview]. Ms. Rose said that the case “is not about private voluntary barter or currency systems. This is a case about fraud and counterfeiting.” I presented Ms. Rose with a hypothetical of an alternative coin-based currency system, not priced in dollars, that presented no risk of fraud or counterfeiting but was intended to be circulated and generally accepted. Rose said that although one could make an argument that such a currency would be prohibited by 18 U.S.C. § 486 because it was “intended for use as current money,” prosecutions based on such a theory would be very unlikely unless there are victims who make consumer complaints.

release,<sup>156</sup> the 2009 indictment, and 2011 trial, the government focused on the similarity of Liberty Dollars to official U.S. currency and potential to confuse consumers.<sup>157</sup> These materials noted that NotHaus tried to spend Liberty Dollars into regular circulation, encouraged other Liberty Dollar users to do the same, and encouraged businesses to give Liberty Dollars as change to unsuspecting customers.<sup>158</sup> NotHaus and his organization profited from their fraud because the face value of Liberty Dollar metal currencies was set higher than the value of their metal content.<sup>159</sup>

---

156. In 2006, the U.S. Mint published a press release notifying consumers that Liberty Dollars are “not genuine United States Mint bullion coins,” “not legal tender,” and “are neither backed by, nor affiliated with, the United States Government.” U.S. Mint, *Liberty Dollar Consumer Warning*, *supra* note 75. The release warned consumers that Liberty Dollar medallions might be confused with official U.S. currency because they had similar wording and images. *Id.* It also warned that “[a]ccording to the NORFED website, ‘Liberty merchants’ are encouraged to accept NORFED ‘Liberty Dollar’ medallions and offer them as change in sales transactions of merchandise or services.” *Id.*

157. United States’ Response in Opposition to Defendant’s Motions Under Rules 29, 33 and 34 of the Fed.R.Crim.Proc. at 4–5, *United States v. NotHaus*, 5:09CR27-V, (W.D.N.C. Apr. 7, 2011) (“The government presented substantial evidence at trial on each element of the charges for which Defendant was convicted. Ultimately, the evidence presented at trial showed that Defendant (1) designed and created counterfeit coins (Liberty Dollars) that resembled genuine coins of the United States; (2) instructed individuals on methods to inject the Liberty Dollar coins into the flow of current money by misleading people to believe that the coins were genuine U.S. coins; and (3) defrauded people by minting the Liberty Dollar coins with a dollar value that was in excess of the true inherent value of the silver contained in the coins . . . Defendant engages in a wholly irrelevant discussion of ‘private currency barter systems’ and contends that the government sought to paint a picture that private currency systems were illegal. . . . Defendant was not operating a ‘private currency barter system,’ rather, he was counterfeiting United States coins and using deceptive means to inject them into the flow of current money to defraud the public.”) (citations omitted).

158. Adam Jefferson Kirby, *The Strange Case of The Liberty Dollar*, SILVER MONTHLY, <http://www.silvermonthly.com/1459/the-strange-case-of-the-liberty-dollar> (last visited Apr. 4, 2011) (“It was common practice for Von Nothaus [sic] and his associates to present Liberty Dollars to merchants unfamiliar with his product without offering the explanation that they were not U.S. legal tender currency, but rather, a voluntary barter currency, one which could not be redeemed at face value for Federal Reserve Notes in any U.S. commercial bank. A video exposé posted originally on the Liberty Dollar website . . . features Von Nothaus [sic] personally buying sandwiches with a \$10 Liberty Dollar coin, declaring it to be a ‘new ten dollar silver piece’ as he handed it to the bewildered vendor.”).

159. One of the prosecutors, Jill Westmoreland Rose, told me: “If you’re giving someone a \$10 coin and tell them that it’s legal, but it only has \$4 worth of silver, you’re defrauding people.” Rose Interview, *supra*.note 155. (These profits—those accruing to a currency issuer because excess of face value of currency over the cost of its creation—are called “seigniorage” and are often reserved to governments). Kerry Lynn Macintosh, *How to Encourage Global Electronic Commerce: The Case for Private Currencies On the Internet*, 11 HARV. J.L. & TECH. 733, 747 n.50 (1998).

NotHaus contested these characterizations and argued that he only encouraged individuals to enter into knowing and voluntary exchanges.<sup>160</sup> However, a jury disagreed, finding him to have violated all three counterfeiting counts of the indictment.<sup>161</sup>

From this perspective, the U.S. Attorney's characterization of NotHaus as a domestic terrorist is more understandable. He attempted to create a paper and metal currency denominated in dollars that directly competed with U.S. greenbacks in representing official government-backed money. He is like a counterfeiter who prints greenbacks to pawn off on unsuspecting individuals and customers. Although some believe that metal-backed Liberty Dollars are worth more than greenbacks, that is no reason for unsuspecting individuals to be involuntarily stuck with Liberty Dollars instead of greenbacks.<sup>162</sup>

### B. Securities Regulations

Federal law subjects "securities" to a panoply of regulations, making the determination of whether bitcoins are "securities" extremely important.<sup>163</sup> "Security" is defined broadly in the Securities Act of 1933 § 2(a)(1) as including "any note, stock, . . . , transferable share, [or] investment contract," and about thirty other things. Other securities laws, such as section 3(a)(10) of the Securities and Exchange Act of 1934, contain substantially identical language. These laws also contain lists of "exempted securities," which are

---

160. For example, in a case that von NotHaus filed against the U.S. Mint (that was later dismissed), he argued that neither he nor "individuals in the Liberty Dollar organization have . . . represented the Liberty Dollar as legal tender or 'current money.' Liberty Dollar has encouraged persons who utilize the barter currency to offer it to merchants as barter payment for goods and services but not as 'legal tender' or 'current money'." Complaint at ¶ 14, *NotHaus v. Paulson*, No. 3:07-CV-038 RLY-WGH, 2007 WL 4579959 (S.D. Ind. Mar. 20, 2007). When I spoke to him after his conviction, he argued that the government had not proven the counterfeiting charges against him and asked why the government did not produce witnesses who had been defrauded or misled. NotHaus interview, *supra* note 151. He said that he was convicted because the prosecution, which he described as "lying pieces of shit," had "lied." *Id.*

161. Verdict Form, *United States v. von NotHaus*, 5:09CR27-V (W.D.N.C. Mar. 18, 2011).

162. See Kirby, *supra* note 158 (arguing that Von Nothaus's tactics were illegitimate). Individuals printing currency that purports to be "dollars" theoretically interfere with the Federal Reserve's control over monetary policy (although the amount in circulation—approximately \$20 million in the case of Liberty Dollars—is so small that there could be no practical effect). Smith & Wilson, *supra* note 94, at 1115 & n.55.

163. *C.f.* SOLOMON, *supra* note 98, at 109–10 (noting the importance of determining whether private, local currencies are securities under the federal securities laws).

exempt from registration and disclosure laws but are still subject to antifraud and civil suit provisions.

At least one commentator has concluded that digital currencies are unlikely to be regulated as securities.<sup>164</sup> Bitcoin supporters may similarly argue, as elaborated below, that bitcoins do not look like securities or investments, especially because there is no money-making enterprise that is attempting to raise money, and that bitcoins are instead like commodities or currencies, which are generally not regulated under the federal securities laws. Furthermore, although bitcoins may resemble “investment contracts,” they ultimately do not fall within that definition as described in more detail below.<sup>165</sup>

### *I. Note or Stock*

A bitcoin is not “stock” within the meaning of these statutes because it lacks important characteristics of stock, such as conferring the “right to receive dividends contingent upon an apportionment of profits” and “voting rights in proportion to the number of shares owned.”<sup>166</sup> Similarly, a bitcoin is not a “note” within the meaning of the statutes because it lacks the essential characteristics of a note.<sup>167</sup>

---

164. Macintosh, *supra* note 159, at 746 n.49.

165. In an earlier draft of this article, I concluded that bitcoins likely were investment contracts but as explained below, events that took place in the Bitcoin world after that draft was published have changed my mind.

166. See *Landreth Timber Co. v. Landreth*, 471 U.S. 681, 686 (1985) (citing *United Housing Foundation, Inc. v. Forman*, 421 U.S. 837, 851 (1975)) (noting that something is a “stock” and therefore a “security” within the 1933 Act if it has “significant characteristics typically associated with stock” such as “(i) the right to receive dividends contingent upon an apportionment of profits; (ii) negotiability; (iii) the ability to be pledged or hypothecated; (iv) the conferring of voting rights in proportion to the number of shares owned; and (v) the capacity to appreciate in value.” (citations and quotations omitted)).

167. The test for whether something is a “note” within the securities laws “begins with a presumption that any note with a term of more than nine months is a ‘security’” but allows “an issuer to rebut the presumption that a note is a security if it can show that the note in question bear[s] a strong family resemblance to an item on the judicially crafted list of exceptions” of notes that “are obviously not securities.” *Reves v. Ernst & Young*, 494 U.S. 56, 63–65 (1990) (citations and quotations omitted). On first glance, this definition seems circular because it requires a court to determine whether something is a “note” before applying a test to determine whether it is a “note” under the securities laws. However, it is clear that the Supreme Court is using the word “note” in two different ways: first, whether it is an instrument commonly considered a “note” within the commercial world; and second, if it is such an instrument, whether it should fall within the definition of “note” in the securities laws. See *id.* at 63 (“the phrase ‘any note’ should not be interpreted to mean literally ‘any note’ but must be understood against the backdrop of what Congress was attempting to accomplish in enacting the Securities Acts.”). If something is not a “note” in the broad commercial sense then it is not a “note” within the securities laws.

an instrument that indicates a “promise by the maker to pay a sum of money to another party.”<sup>168</sup> Although some digital currency tokens represent promises to pay,<sup>169</sup> a bitcoin instead represents a settled amount.<sup>170</sup>

## 2. *Investment Contract*

If a bitcoin is a security, it will be because it falls within the vague and broad phrase “investment contract.”<sup>171</sup> The Supreme Court, in *SEC v. W. J. Howey Co.*, has interpreted something to be an “investment contract” and therefore a “security” if it is a “contract, transaction or scheme whereby a person [1] invests his money in [2] a common enterprise and [3] is led to expect profits [4] solely from the efforts of the promoter or a third party . . .”<sup>172</sup> In that case, individuals who purchased a row of orange trees and management services in return for a share of the operation’s profits were found to have purchased “securities.” Supporters of Bitcoin like John William Nelson, a Georgia attorney, argue that Bitcoin does not meet any of the requirements of the *Howey* test,<sup>173</sup> while opponents would argue that it meets all of them. The best argument is likely somewhere between these extremes.

*Investment of Money.* Supporters may argue that no individual invests his money because bitcoins are initially awarded to those who invest computational time rather than money. However, most

---

168. See Part VI.A.1, *supra*, (arguing that a bitcoin is not an obligation); C.f. Edward Sonnenschein, Jr., *Federal Securities Law Coverage of Note Transactions: The Antifraud Provisions*, 35 BUS. LAW. 1567, 1578 (1980) (“The term[] ‘note’ [is] used in reference to a highly diverse set of instruments which are utilized in an even more diverse set of transactions. Although the Uniform Commercial Code defines the term more narrowly, the feature common to these instruments is that they embody a promise by the maker to pay a sum of money to another party, the payee. Such payment may become due either at a specified time, or upon the demand of the payee or the occurrence of some specified event, or some combination of the above.” (citation omitted)).

169. See Macintosh, *supra* note 159, at 745–46 & n.49 (giving an example of a hypothetical digital currency that is in the form of a “digital promissory note”).

170. If Jack gives Bob a note for \$10 and \$10 worth of bitcoins and later goes bankrupt, the note will trade at a discount because Jack cannot fulfill his promise to pay the full amount of the note, but the bitcoins will still be worth their full amount.

171. Securities Act of 1933 § 2(a)(1).

172. 328 U.S. 293, 298–99 (1946). See generally Thomas Lee Hazen, *Securities Regulation in a nutshell* 33–37 (10th ed. 2009) (noting the four parts of the *Howey* test).

173. John William Nelson, *Why Bitcoin Isn’t a Security Under Federal Securities Law*, LEX TECHNOLOGIAE (June 26, 2011 11:49 PM), <http://www.lextechnologiae.com/2011/06/26/why-bitcoin-isnt-a-security-under-federal-securities-law> (“Nevertheless, none of the four characteristics of an investment contract . . . really fit Bitcoin’s model.”).

individuals *do* purchase bitcoins on exchanges using money rather than mining them.

*Common Enterprise.* A Bitcoin opponent would argue that there is a common enterprise. There is “horizontal commonality: the tying of each individual investor’s fortunes to the fortunes of the other investors . . .”<sup>174</sup> As the value of Bitcoin increases, each person holding bitcoins is proportionally better off. The enterprise can be described as comprising the software developers because they ensure Bitcoin’s technical and money-supply properties, which are among the most important factors affecting Bitcoin’s value. Furthermore, although it may be true that Bitcoin seems to lack a business or entity that is trying to raise money (when individuals purchase bitcoins on an exchange, no money goes towards the developers),<sup>175</sup> this fact should not be dispositive in a regime that is primarily intended to protect investors.

Here, however, Bitcoin’s proponents’ argument is probably stronger. The individuals who choose to promote Bitcoin are independent of one another, and there is no one money-making business that seeks to raise money through investments. Further, recent events have shown that the Bitcoin developers, although important to the continued success of Bitcoin, are far from the most important players. For example, in June, Mt. Gox, the most popular exchange, was hacked.<sup>176</sup> The thief was able to steal or arbitrarily assign himself about 25,000 bitcoins—worth about \$500,000 at the time, and tried to sell them all at once. The glut of bitcoins for sale crashed the price from \$17.50 to \$0.01 within a half hour,<sup>177</sup> throwing the whole Bitcoin world into a panic. Mt. Gox responded by freezing trading, writing off the money that the hacker was actually able to withdraw from the exchange, and rolling back all accounts and trades to a pre-hack state. The move worked, restoring the trading price at where it had been before the hack and calming the markets. Mt. Gox

---

174. *Revak v. SEC Realty Corp.*, 18 F. 3d 81, 87 (2d Cir. 1994).

175. One might argue that Bitcoin’s developers do constitute the money making business. Bitcoin developers presumably own bitcoins—perhaps more than the average Bitcoin user. Thus, it is in their interest to ensure that bitcoins remain liquid and in high demand relative to supply, to maintain and increase their own wealth.

176. Jason Mick, Daily Tech, *Inside the Mega-Hack of Bitcoin: the Full Story* (June 19, 2011), <http://www.dailytech.com/Inside+the+MegaHack+of+Bitcoin+the+Full+Story/article21942.htm>; Press Release, Mt. Gox, *Clarification of Mt. Gox Compromise Accounts and Major Bitcoin Sell-Off* (June 30, 2011), available at [https://mtgox.com/press\\_release\\_20110630.html](https://mtgox.com/press_release_20110630.html).

177. *Id.*

played a similarly important role when a the third largest exchange, Bitomat.pl, incompetently lost the file that contained 25,000 bitcoins belonging to its users.<sup>178</sup> Mt. Gox bought Bitomat.pl and restored balances for all of Bitomat.pl's users in order to "restore confidence in the bitcoin economy."<sup>179</sup> Thus, Mt. Gox and other exchanges are critical parts of the Bitcoin infrastructure, indicating that the developers cannot be described as the whole Bitcoin enterprise.

*Expectation of Profits.* Proponents argue that there is no expectation of profits. Individuals hold bitcoins either for fun<sup>180</sup> or as they do other currencies, to facilitate commercial exchanges rather than in expectation of profit. Although some individuals do speculate in currencies on foreign exchange markets, with volumes reaching *trillions* of dollars per day,<sup>181</sup> it is unlikely that a court would find that U.S. dollars are generally held in expectation of profit. Similarly, even substantial speculation in bitcoins does not indicate a general expectation of profit.

However, at present, most Bitcoin users are probably investing in Bitcoin in expectation of profits. A very small number of merchants accept bitcoins (although the number is likely to grow) indicating that opportunities to use bitcoins in commercial exchanges is limited. Moreover, many Bitcoin users are motivated by a belief that Bitcoin, unlike the dollar, is inflation-resistant, indicating a profit expectation to some extent.<sup>182</sup>

*Solely From the Efforts of Another.* Bitcoin opponents may argue that an investor's returns do come solely from the efforts of

---

178. Press Release, Mt. Gox, *Mt.Gox, The World's Largest Bitcoin Exchange to Acquire Bitomat.pl, Compensate Loss Of Bitcoins* (Aug. 11, 2011), available at [https://mtgox.com/press\\_release\\_20110811.html](https://mtgox.com/press_release_20110811.html).

179. *Id.*

180. *C.f.* Alan R. Bromberg, *Commodities Law and Securities Law—Overlaps and Preemptions*, 1 J. CORP. L. 217, 224 & n.18 (1976) (citing *SEC v. Brigadoon Scotch Distrib., Ltd.*, 388 F. Supp. 1288 (S.D.N.Y. 1975)) (Noting that within the context of the *Howey* test, "[c]oins or stamps bought for a hobby probably lack a profit element . . .").

181. *See What is Foreign Exchange (Forex)?*, INTERNATIONAL BUSINESS TIMES (Feb. 11, 2009), <http://au.ibtimes.com/articles/110821/20110210/what-is-foreign-exchange-currency-conversion-financial-markets-forex-foreign-exchange-markets.htm>.

182. Bitcoin supporters might recharacterize the issue by arguing that purchasing bitcoins because of a belief of deleterious inflation in, e.g., the dollar, does not reflect an expectation of profit but instead a fear of loss from holding wealth in the U.S. Dollar. An adjudicator's decision on the "profits" issue may ultimately depend on who the parties at issue are, whether they invested for profit, and whether at the time of the dispute or the time of the facts that gave rise to the dispute the Bitcoin economy has flourished significantly to support a finding that most individuals hold bitcoins to facilitate commercial transactions.

others. Bitcoin investors have no active part to play in Bitcoin's management but do require the ongoing efforts of the Bitcoin developers.<sup>183</sup> Opponents, on the other hand, would argue that an individual who owns bitcoins does not rely on the efforts of a third party because bitcoins have inherent value, which comes from the limited supply of bitcoins and for which the developers are not needed. The issue here is a close one.

In sum, because there is likely no common enterprise, Bitcoin is unlikely to be an investment contract.

### 3. *Commodity*

Those arguing that a bitcoin is not a security may also argue that bitcoins are not within the spirit of the securities acts and do not look like or act like a "security"—instead, bitcoins are commodities, which are generally held not to be securities.<sup>184</sup>

Owning a bitcoin gives one only rights to use the bitcoin in any way one sees fit and to sell or make contracts involving that bitcoin. Similarly, one who owns, say, corn, has only the right to use the corn (by, e.g., making corn-on-the-cob or processing it into biofuel) or to sell the corn or make contracts involving that corn. Securities, on the other hand, have a feature that commodities do not have: they confer a claim on some other entity.<sup>185</sup> In these ways, Bitcoin is like corn and

---

183. Although some Bitcoin investors may choose to promote its virtues in order to increase demand, most will free-ride off the few who actively promote Bitcoin, and also rely on the efforts of the software developers maintaining the software. The minimal participation required by pyramid scheme investors has not precluded application of the securities laws. Hazen, *supra* note 172, at 35–36 (quoting SEC v. Glenn W. Turner Enterp., 474 F.2d 476 (9th Cir. 1973)). Thus, any investor involvement in Bitcoin's success will also not preclude Bitcoin from being deemed an "investment contract" and therefore a "security."

184. See Steven M. Johnson & Tyler M. Moore, *Recent Developments in Commodities Law*, 37 WASH. & LEE L. REV. 986, 989 n.22; Bromberg, *supra* note 180, at 221–22. A commodity transferred in a spot contract by way of a "naked" sale—meaning sold and actually delivered at present rather than in future, without accompanying managerial services, margin, repurchase agreements, or guarantees regarding subsequent price movements—is not a "security" within the federal securities laws. *Id.* at 221–22. Where a commodity sale is not naked and involves other services, it is more likely to be considered an "investment contract" and therefore a "security." *Id.* Where a contract is for future delivery, it is regulated by the CFTC as a commodity future rather than by the SEC as a security. Johnson & Moore, *supra*, at 988–90.

185. CARNELL, MACEY & MILLER, *supra* note 65, at 130 ("All securities represent claims against an *issuer*: i.e., against the corporation, government, or other entity that issued the securities."). Securities may confer a claim on an issuer's profits (as through dividend payments), management (e.g., through a vote on important business matters, such as a merger), or assets (e.g., in case of bankruptcy).

any other commodity. However, decisions explaining why commodities are not securities have also noted that commodities are “tangible” and have “inherent value,” unlike securities.<sup>186</sup> Bitcoins are not “tangible,” and one may argue that by design they have no inherent value because there is no government or commodity backing them. Furthermore, just as one generally cannot “use” a security—except by buying, selling, or pledging it—one cannot “use” a bitcoin except by buying, selling, or pledging. Alternatively, one may argue that bitcoins do have inherent value by dint of their promised rarity over time.

The question might come down to how much of a bitcoin’s value is “inherent” in its initial design and how much is dependent on the ongoing investment of effort by the software developers and promoters. If all software development on Bitcoin stopped, would Bitcoin retain its high value against the U.S. Dollar, for example? Probably not. One might recognize that this question is substantively the same as both the “enterprise” and “dependence” elements of the *Howey* test: is there a common enterprise that will account for Bitcoin’s success or failure and is the investor relying solely on the efforts of that enterprise to put in effort? In fact, one commentator has noted that commodities are not “investment contracts” under *Howey* principally because of the absence of a “common enterprise” and “dependence.”<sup>187</sup>

Thus, although bitcoins share many features with commodities, they also share features with securities and are unlikely to evade categorization as an “investment contract” on this ground.

Note that many states have regulations governing some or all commodities that have fraud provisions like those in the federal securities laws but may be preempted by federal laws.<sup>188</sup> An examination of these laws is beyond the scope of this Article.

#### 4. *Currency*

Under federal securities laws, currencies may not be securities<sup>189</sup>—or alternatively, they may be exempt from the

---

186. See Bromberg, *supra* note 180, at 222 (citing Ga. Sec. Comm’r, Release No. 1 (Sept. 18, 1973), 1 BLUE SKY L. REP. P 14,612, at 10,504 (“Obviously, grains, metals, and other items traded as commodities are tangible items, not securities . . .”).

187. Bromberg, *supra* note 180, at 223–24.

188. *Id.* at 223 n.15.

189. Lewis D. Lowenfels & Alan R. Bromberg, *What is a Security Under the Federal Securities Laws?*, 56 ALB. L. REV. 473, 483 (1993) (“[I]t is generally acknowledged that currency is not a security.”); *Procter & Gamble Co. v. Bankers Trust Co.*, 925 F. Supp.

registration and disclosure provisions while being subject to antifraud and civil suit provisions.<sup>190</sup> However, Bitcoin may fall outside these exemptions or exclusions, as explained below. Furthermore, currencies may generally be considered securities under some state securities laws.<sup>191</sup>

The 1933 Act exempts “[a]ny note, draft, bill of exchange, or banker’s acceptance which arises out of a current transaction or the proceeds of which have been or are to be used for current transactions, and which has a maturity at the time of issuance of not exceeding nine months . . .”<sup>192</sup> One commentator has concluded that this exemption would apply to local paper currency,<sup>193</sup> but it would probably not apply to Bitcoin, which is not a “note, draft, bill of exchange, or banker’s acceptance” as the plain text of that exemption requires.<sup>194</sup>

The 1934 Act excludes from the definition of a security “currency or any note . . . which has a maturity at the time of issuance of not exceeding nine months . . .”<sup>195</sup> Thus the 1934 Act excludes certain short term notes just like the 1933 Act exempts them, but the 1934 Act also excludes “currency.” However, each term defining security and its exclusions and exemptions is not usually interpreted literally but interpreted instead to effect Congress’s general purpose in passing the securities acts and more specific purpose in including that

---

1270, 1280 n.4 (S.D. Ohio 1996) (“foreign currency . . . is not a security as defined in the 1933 and 1934 Acts.”). The 1934 Act *excludes* from the definition of security “currency or any note, draft, bill of exchange, or banker’s acceptance which has a maturity at the time of issuance of not exceeding nine months, exclusive of days of grace, or any renewal thereof the maturity of which is likewise limited.” Securities Exchange Act of 1934 § 3(a)(10); *accord* Bellah v. First National Bank of Hereford, Texas, 495 F. 2d 1109, 1114 (5th Cir. 1974).

190. For example, the 1933 Act exempts from regulation “[a]ny note, draft, bill of exchange, or banker’s acceptance which arises out of a current transaction or the proceeds of which have been or are to be used for current transactions, and which has a maturity at the time of issuance of not exceeding nine months, exclusive of days of grace, or any renewal thereof the maturity of which is likewise limited . . .” Securities Act of 1933 § 3(a)(3). *See* SOLOMON, *supra* note 98, at 114–15 (concluding that paper-based local currencies would most likely fall under this exemption).

191. For example, Ohio’s blue sky law defines security to include “the currency of any government other than those of the United States or Canada.” Ohio Rev.Code § 1707.01(B) (1992).

192. Securities Act of 1933 § 3(a)(3).

193. *See* SOLOMON, *supra* note 98, at 113–14.

194. *See* Securities Act of 1933 § 3(a)(3).

195. Securities Exchange Act of 1934 § 3(a)(10).

term,<sup>196</sup> focusing on the economic substance rather than form of the instrument or transaction.<sup>197</sup> “Currency” is also not likely to be interpreted literally.

An examination of the legislative history of the neighboring short term note exception is instructive.<sup>198</sup> The history indicates that congress wanted to exempt commercial paper,<sup>199</sup> a particular type of short term debt, because it was used in commercial rather than investment transactions and was generally not offered to the public,<sup>200</sup> and because commercial paper was considered extremely safe, “only second to Government bonds.”<sup>201</sup> Like commercial paper, currency

---

196. See, e.g., *Reves v. Ernst & Young*, 494 U.S. 56, 63 (1990) (“[T]he phrase ‘any note’ [in the definition of ‘security’] should not be interpreted to mean literally ‘any note’ but must be understood against the backdrop of what Congress was attempting to accomplish in enacting the Securities Acts.”); *United Housing Foundation v. Forman*, 421 U.S. 837 (1975) (“any stock” not interpreted literally); *Reves*, 494 U.S. at 74 (Stevens, J., concurring) (“The Courts of Appeals have been unanimous in rejecting a literal reading of the [short term note] exclusion. They have instead concluded that when Congress spoke of notes with a maturity not exceeding nine months, it meant commercial paper, not investment securities.”).

197. *Id.* at 61 (“In discharging our duty, we are not bound by legal formalisms, but instead take account of the economics of the transaction under investigation. See, e.g., *Tcherepnin v. Knight*, 389 U.S. 332, 336 (1967) (in interpreting the term “security,” “form should be disregarded for substance and the emphasis should be on economic reality”).

198. Judge Friendly, Justice Stevens, and Professor Loss have assumed that Congress had the same intent for the 1934 Act exclusion. See *Zeller v. Bogue Electric Mfg. Corp.*, 476 F. 2d 795, 799–800 (2d Cir. 1973) (Friendly, J.) (“We have no doubt that the Commission would take the same view with respect to the exclusion in § 3(a)(10) of the Securities Exchange Act.”); *Reves*, 494 U.S. at 76 (Stevens, J., concurring) (“[T]here is no apparent reason to construe § 3(a)(10) of the 1934 Act differently” than § 3(a)(1) of the 1933 Act); 2 LOSS, SECURITIES REGULATION 796 (1961).

199. *Reves*, 494 U.S. at 73–76 (Stevens, J., concurring).

200. Securities Act Rel. No. 4412 (1961), 26 Fed. Reg. 9158, 9159 (1961) (“commercial, agricultural, or industrial transactions”) (quoting Rep. No. 47 on S. 875, 73d Cong., 1st sess. (1033), pp. 3–4); *Zeller*, 476 F. 2d at 799–800 (approving of the SEC’s reading of the legislative history).

201. *Sanders v. John Nuveen & Co.*, 463 F. 2d 1075, 1079 n.12 (7th Cir. 1972) (quoting Hearings on S. 875 Before the Senate Comm. on Banking and Currency, 73rd Cong., 1st Sess. at 94, 95 (1933)) (“The [SEC] release emphasized the prime quality of the paper intended to be exempted and stated that the exempted items are ‘composed of assets easily convertible into cash and are comparable to liquid inventories of an industrial or mercantile company.’ During the hearings on the 1933 act, commercial paper discountable by Federal Reserve banks was described as having ‘a record of safety only second to Government bonds’ and as being the basis of our currency. Hearings on S. 875 Before the Senate Comm. on Banking and Currency, 73rd Cong., 1st Sess. at 94, 95 (1933). It is significant that section 3(a) (10) of the 1934 act exempts ‘currency’ from the definition of security. 15 U.S.C. § 78c(a)(10).”). Although this legislative history refers mainly to the 1933 Act exemption (which says nothing about “currency”), Judge Friendly and Justice Stevens have assumed that Congress had the same intent for the 1934 Act exclusion. See

generally does not resemble a security, does not pose risk for the public (even if they purchase a lot of it), and is very safe and liquid.

Bitcoin may fall under the literal definition of “currency,” but it is also unlike the commercial paper that Congress exempted. Bitcoin may resemble a security, as discussed above, may pose risks for investors, and may not be safe or liquid. The Supreme Court has noted that

[T]he fundamental purpose undergirding the Securities Acts is to eliminate serious abuses in a largely unregulated securities market . . . . Congress therefore did not attempt to precisely cabin the scope of the Securities Acts. Rather, it enacted a definition of ‘security’ sufficiently broad to encompass virtually any instrument that might be sold as an investment.<sup>202</sup>

Thus, when faced with the argument that Bitcoin is a “currency” and therefore exempted, a court is likely to respond that Congress did not mean to exempt a currency that is also a security.<sup>203</sup>

A textual argument may support this purposive argument: by “currency,” Congress did not mean anything “that circulates as a medium of exchange”<sup>204</sup> but instead money that is “current” or generally accepted in some geographic or political area (i.e., “current money”).<sup>205</sup> The narrow definition would likely exclude bitcoins until

---

*Zeller*, 476 F. 2d at 799–800 (Friendly, J.) (“We have no doubt that the Commission would take the same view with respect to the exclusion in § 3(a)(10) of the Securities Exchange Act.”); *Reves*, 494 U.S. at 76 (Stevens, J., concurring) (“[T]here is no apparent reason to construe § 3(a)(10) of the 1934 Act differently” than § 3(a)(1) of the 1933 Act).

202. *Reves*, 494 U.S. at 60–61 (citations and quotations omitted).

203. *C.f. Reves*, 494 U.S. at 74 (“The Courts of Appeals have been unanimous in rejecting a literal reading of the [short term note] exclusion. They have instead concluded that when Congress spoke of notes with a maturity not exceeding nine months, it meant commercial paper, not investment securities.”) (Stevens, J., concurring); Alan R. Bromberg, *Securities Law, Fraud, SEC Rule 10b-5, § 4.6 (321)* (1971) (“Even if short term notes are effectively excluded from the definition of security, their use in connection with an investment contract or other transaction constituting a security does not immunize the transaction from the antifraud rules.”).

204. See BLACK’S LAW DICTIONARY (9th ed. 2009) (“An item (such as a coin, government note, or banknote) that circulates as a medium of exchange.”).

205. See, e.g., *State v. Quackenbush*, 98 Minn. 515, 520–21 (1906) (“‘Current money’ means money which passes from hand to hand and from person to person and circulates through the community. It is synonymous with ‘lawful money.’ Whatever is intended to, and does actually, circulate as money. Every species of coin or currency. Lawful money. ‘Current money,’ that which is generally used as a medium of exchange.” (citations omitted) (emphasis added)); Lewis D. Solomon, *Local Currency: A Legal and Policy Analysis*, 5 KAN. J.L. & PUB. POL’Y 59, 81–83 (1996) (construing the words “current money” in an anti-counterfeiting statute).

bitcoins become generally accepted in any geographical or political area.

### C. Anti-Money Laundering Laws and Regulations

Money laundering is the process by which dirty money—proceeds of illegal activities—is rendered clean, allowing the money to be used for legal activities.<sup>206</sup> Terrorist financing is similar, except that it allows clean money to be used for illegal activities,<sup>207</sup> and is often considered under the same umbrella as money laundering. Digital currencies are attractive vehicles for money laundering because they allow fast, anonymous, through-the-Internet transfers.

The indictment and later guilty plea of the owners and directors of the e-gold digital gold currency demonstrate the bifurcated approach that U.S. federal law takes to money laundering.<sup>208</sup> First, the Bank Secrecy Act (BSA), as amended and implemented by regulations passed by FinCEN,<sup>209</sup> requires a wide-swath of otherwise unregulated financial institutions to register with the government, implement anti-money laundering procedures, keep data, and report certain transactions and other data.<sup>210</sup> Similarly, D.C. law required licenses for money transmitting. E-gold, which allowed individuals to purchase e-gold using dollars, send e-gold to other e-gold account holders, and cash out using dollars or other currencies failed to register under both state and federal law, as it was required to so, violating 18 U.S.C. § 1960.

The BSA statute and regulations require that any “money services business” register with FinCEN,<sup>211</sup> with threat of civil and

---

206. Shawn Turner, *U.S. Anti-Money Laundering Regulations: An Economic Approach to Cyber-Laundering*, 54 CASE W. RES. L. REV. 1389, 1391 (2004).

207. Russell P. Leino, *The Strange Case of Amended Amendment S.A. 1107: Did Congress Miss a Golden Opportunity to Address the Money Laundering Threat Posed by Stored Value Cards in the Credit Card Act of 2009?*, 13 U. PA. J. BUS. L. 301, 310 (Fall 2010).

208. See Turner, *supra* note 206, at 1402–06.

209. The BSA gives authority to the Secretary of the Treasury to implement the BSA through regulations. The Secretary delegated that authority to a bureau of the Treasury Department called the Financial Crimes Enforcement Network (FinCEN).

210. See Turner, *supra* note 206, at 1402–05.

211. 31 U.S.C. 5330(a)(1) requires “Any person who owns or controls a money transmitting business shall register the business (whether or not the business is licensed as a money transmitting business in any State)” with Treasury (i.e., with FinCEN). The BSA gives some authority to Treasury to determine who is a “money transmitting business.” FinCEN has used its delegated authority to pass regulations that give guidance on what entities are “money transmitting businesses”, which are referred to as “money services businesses” in the regulations. FinCEN decided to use the term “money services

criminal penalties. That term is defined in regulations as “A person wherever located doing business . . . in one or more of the [following] capacities: (1) Dealer in foreign exchange . . . (2) Check cashier . . . (3) Issuer or seller of traveler’s checks or money orders . . . (4) Provider of prepaid access . . . (5) Money transmitter . . . (6) U.S. Postal Service . . . (7) Seller of prepaid access.”<sup>212</sup>

Second, the Money Laundering Control Act of 1986 (MLCA) criminalizes money laundering.<sup>213</sup> Under the MCLA, the prosecutors argued that E-gold had violated 18 U.S.C. § 1956, which, in general, applies to individuals who conduct a financial transaction involving dirty money, knowing that the money is dirty, with the intent of promoting certain kinds of illegal activities, concealing the dirty money’s origin, or avoiding a reporting requirement.<sup>214</sup>

The factual premises of both these charges were similar:

[T]he E-Gold operation provided digital currency services over the Internet through two sites: [www.e-gold.com](http://www.e-gold.com) and [www.Omnipay.com](http://www.Omnipay.com). Several characteristics of the E-Gold operation made it attractive to users engaged in criminal activity, such as not requiring users to provide their true identity, or any specific identity. The E-Gold operation continued to allow accounts to be opened without verification of user identity, despite knowing that “e-gold” was being used for criminal activity, including child exploitation, investment scams, credit card fraud and identity theft. In addition, E-Gold assigned employees with no prior relevant experience to monitor hundreds of thousands of accounts for criminal activity. They also participated in designing a system that expressly encouraged users whose criminal activity had been discovered to transfer their criminal proceeds among other “e-gold” accounts. Unlike other Internet payment systems, the E-Gold operation did not include any statement in its user agreement prohibiting the use of “e-gold” for criminal activity.<sup>215</sup>

---

businesses” instead of the statute’s term “money transmitting business” because it believed the statute’s terminology to be confusing. FinCEN, Amendment to the Bank Secrecy Act Regulations-Definitions Relating to, and Registration of, Money Services Businesses, 64 Fed. Reg. 45438-01, n.1.

212. 31 C.F.R. § 1010.100(ff).

213. Turner, *supra* note 206, at 1405.

214. See 18 U.S.C. § 1956; Turner, *supra* note 206, at 1405.

215. Press Release, Department of Justice, *Digital Currency Business E-Gold Pleads Guilty to Money Laundering and Illegal Money Transmitting Charges* (July 21, 2008), available at <http://www.justice.gov/opa/pr/2008/July/08-crm-635.html>.

Thus, certain kinds of financial businesses—even those located abroad<sup>216</sup>—must register under both federal and state law or face criminal penalties. Furthermore, if individuals or businesses knowingly process dirty money, make a profit on those transactions, and do nothing to stop processing those transactions, they may be guilty of money laundering.

Thus, there is a serious question of whether BSA and MLCA regimes impose legal risk for the Bitcoin developers, exchanges, ewallet providers, individual miners, operators of mining pools, mere Bitcoin users, and businesses that accept bitcoins. Future work should analyze these regimes more closely to determine which, if any, of these groups must register with FinCEN as money services businesses and be subject to heavy regulatory burdens. Future work should also determine if any of these groups are at danger of being considered money launderers since it is generally known that Bitcoin is used to promote illegal activities, such as the sale and purchase of illegal drugs.

## VII. Conclusion

Bitcoin is novel digital currency that has the potential to be a significant player in the micropayment and virtual world commerce markets. It is also a great alternative currency for gold bugs who prefer to hold currencies fully backed by commodities. Furthermore, because it is anonymous and decentralized, and therefore difficult to shut down, it may allow organizations hated by governments—whether these are morally commendable or detestable organizations—to be funded without risk of monetary seizure or sanctions on financial contributors.

While the history of currencies such as the Iraqi Swiss Dinar that had no backing by either commodities or government entities indicates that Bitcoin may succeed, potential users and investors

---

216. That many of these entities are located abroad does not mean that they are not subject to U.S. laws and regulations if, for example, many of their customers are located in the U.S. See Press Release, Financial Crimes Enforcement Network, *FinCEN Clarifies Money Services Businesses Definitions: Rule Includes Foreign-Located MSBs Doing Business in U.S.* at ¶ 1–2 (July 18, 2011); Dep't of the Treasury, Bank Secrecy Act Regulations; Definitions and Other Regulations Related to Money Services Businesses, 76 Fed. Reg. 43585, 43588 (2011) (“[A]n entity qualifies as an MSB based on its activity within the United States, not the physical presence of one or more of its agents, agencies, branches or officers in the United States. This proposal arose out of the recognition that the Internet and other technological advances make it increasingly possible for persons to offer MSB services in the United States from foreign locations.”).

should be aware of the many risks inherent in using such a young technology.

Most importantly, Bitcoin currently operates in a legal grey area. The federal government's supposed monopoly on issuing currency is somewhat narrow and statutes that impose that monopoly do not seem to apply to Bitcoin due to its digital nature. However, a bitcoin may be a "security" within the meaning of the federal securities laws, subjecting bitcoins to a vast regime of regulations, including general antifraud rules. Although the best argument is that a bitcoin is not a security, Bitcoin's proponents will have to await an SEC or court interpretation for certainty. Furthermore, other legal issues that have not been analyzed in this Article are probably significant, including tax evasion, banking without a charter, state escheat statutes, and money laundering.

\*\*\*