The Bitcoin Protocol as Law, and the Politics of a Stateless Currency

Sarah Jeong

> *Julian Assange: There's also a very nice little paper that I've seen in relation to Bitcoin, that... you know about Bitcoin?*
>
> *Eric Schmidt: No.*
>
> *Julian Assange: Okay, Bitcoin is something that evolved out of the cypherpunks a couple of years ago, and it is an alternative... it is a stateless currency.*
>
> *Jared Cohen: Yeah, I was reading about this just yesterday.*
>
> *Julian Assange: And very important, actually. It has a few problems. But its innovations exceed its problems.*
>
> Secret meeting between Julian Assange, Google CEO Eric Schmidt, and former Secretary of State advisor Jared Cohen, June 23, 2011[1]

Introduction

The literature is replete with competing accounts of money, and what money is: these theoretical accounts are intensely political in nature, with differing views on the role of the government. One view suggests that government and laws are essential to the nature of money, the other view suggests that currency and economic activity can arise spontaneously without centralized authority—indeed, that such centralized authority often acts as an inept meddler in an otherwise smoothly running natural order.

The creators of Bitcoin, a decentralized, peer-to-peer, stateless electronic currency, apparently espoused the latter view. The introduction to "Bitcoin: A Peer-to-Peer Electronic Cash System,"[2] the white paper that lays out the technological basis of the protocol, begins with what is essentially declaration of distrust—distrust of centralization, of financial institutions, and

[1] Transcript of secret meeting between Julian Assange and Google CEO Eric Schmidt, Jun. 23, 2011, http://wikileaks.org/Transcript-Meeting-Assange-Schmidt [hereinafter, Transcript of secret meeting].
[2] SATOSHI NAKAMOTO, BITCOIN: A PEER-TO-PEER ELECTRONIC CASH SYSTEM (2008), http://bitcoin.org/bitcoin.pdf [hereinafter NAKAMOTO, BITCOIN WHITE PAPER].

of the other transacting party. Satoshi[3] writes, “What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party.”

Bitcoin is not issued by any kind of central authority, let alone a government. No taxes are collected in Bitcoin. Because it is decentralized, no monetary policy is practiced in real-time—all monetary policy decisions have been essentially hard-coded into the protocol. Its monetary supply is so inflexible to demand that the current exchange rate to the dollar is around 1 BTC to $150 (down from $250 in early April, but up from $2 earlier this year).

This paper will discuss and evaluate these design features in relation to the libertarian and metallist philosophies that have shaped them. I will argue that Bitcoin has failed to be perfectly decentralized or particularly anonymous. Furthermore, its hyperdeflationary design features have made Bitcoin a currency dependent on outside, more stable currencies (e.g., the U.S. dollar), which serve as units of account. People are reticent to set up long-term transactions in Bitcoin as a unit of account (e.g., salaries and debts), and thus a large, relatively independent economy in Bitcoin is impossible with the current hard-coded monetary policies in place. But Bitcoin remains a useful innovation—a convenient, unregulated form of money transmission that is growing in use.

Finally, I will argue that despite the view of money taken by its creators, this supposedly stateless currency is far from apolitical in nature. Although its creators tend to espouse apolitical accounts of money, Bitcoin has been from the beginning a political project—an evolving,

[3] “Satoshi Nakamoto” is a pseudonym. Joshua Davis, *The Crypto-Currency: Bitcoin and its mysterious inventor*, THE NEW YORKER, October 10, 2011, 62–70. The writer of the white paper and the original programmer for the protocol may have not been one person, but rather a group of individuals. One possibility is that they were a group of Wall Street quantitative analysts concerned about the legal repercussions of their project. As his/their identities are still unknown, I will refer to him/them as “Satoshi”—how the Bitcoin and cypherpunk communities have commonly addressed him/them—and also use the singular masculine pronoun throughout this paper.

distributed constitutional project, with many goals, visions, and factions.[4] Those that champion Bitcoin have a political agenda: whether it is to oppose the existing state as outlaws, or to declare their allegiance to a new community rooted in technology and the Internet. Furthermore, depending on the shape of these political goals, Bitcoin's advocates may or may not have a vested interest in creating mechanisms to stabilize the currency and make it a viable unit of account.

I. Bitcoin: a primer

A. The Technology

> *1) New transactions are broadcast to all nodes.*
> *2) Each node collects new transactions into a block.*
> *3) Each node works on finding a difficult proof-of-work for its block.*
> *4) When a node finds a proof-of-work, it broadcasts the block to all nodes.*
> *5) Nodes accept the block only if all transactions in it are valid and not already spent.*
> *6) Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.*
>
> Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008[5]

Bitcoin is a currency both created and tracked through a decentralized peer-to-peer network. The Bitcoin protocol is an open source protocol available through several different clients—i.e., the basic code is nonproprietary, and allows for many different kinds of software to be created to interface with it.

Payments are made from one virtual wallet to another, using the cryptographic innovation of private/public keys to assign ownership. The 'coin' is transferred by digitally signing a hashed previous transaction with their private key and with the intended recipient's public key. The broadcast of the signature on top of the hash constitutes a transaction, which then becomes part of the decentralized accounting system created by the protocol. Because of the frequency of

[4] Much of this political project is embedded in the larger context of the cypherpunks of the 1990s, and the present-day WikiLeaks. For a more extensive account of these political movements, albeit without any mention of Bitcoin, see ANDY GREENBERG, THIS MACHINE KILLS SECRETS: HOW WIKILEAKERS, CYPHERPUNKS, AND HACKTIVISTS AIM TO FREE THE WORLD'S INFORMATION (2012).

[5] NAKAMOTO, BITCOIN WHITE PAPER, *supra* note 2, at 3.

transactions and number of nodes, not all nodes will agree on what the transaction history is at a given time; however, over time, parts of the time-stamped transaction history (called the "block chain") are "resolved" and transactions are "finalized" as nodes accept what becomes the one true transaction history—what is referred to as the "longest blockchain."

Each node (that is, a running instance of the client) "works" on the latest block of transaction history in the blockchain, repeatedly applying the cryptographic hash function SHA-256 to the data in order to come up with a desirable result, also known as "satisfying the proof-of-work." This is done by arriving at a hashed string beginning with a certain number of 0s (this number is sensitive to the rate of mining, and is automatically changed to tweak the "difficulty" of mining). The block is incrementally adjusted with a nonce, a small number of characters at the end that unpredictably changes how the hash comes out, until the target is reached. When the target is reached, it is broadcast to the entire network. The other nodes can verify that this is the correct "solution" to the "problem," and then proceed to accept this hashed block as the latest resolved block in the chain. They then move on to work on the next block of transactions, using the latest resolved block as a starting point.

The resolution of blocks within this decentralized accounting system is also the mechanism by which new bitcoins are released into the economy. Bitcoins are not released by a central authority, but are rather "mined" by individual users according to the protocol. The node (or pool of nodes) that first solves the block is rewarded with a set number of bitcoins. At the moment, the base mining reward is set at 25 BTC, with optional bounties collected from those seeking to process large transactions (which make the block larger).[6] The work to resolve blocks is computationally difficult, and takes enormous amounts of processing power. Since the reward is given to the first miner to resolve the block, the protocol has resulted in a computer processing

[6] *Transaction fees*, THE BITCOIN WIKI (last accessed: Apr. 29, 2013), https://en.bitcoin.it/wiki/Transaction_fees.

arms race that has resulted in the use of massive "mining rigs" equipped with specialized computer chips designed specifically for Bitcoin mining.[7]

The mechanism of public/private key transactions allows any node in the Bitcoin network to transact with any other node, transcending any geographic barriers. The mechanism of public broadcast of the timestamped transaction history prevents double-spending of coin in transactions. Transactions thus take 10 to 60 minutes to be "verified," if a user attempts to double-spend, one of those transactions will simply fail to go through as the blockchain becomes resolved. In order to commit fraud upon the currency ("forge" the currency, or rather, revise the transaction history), an attacker must control the majority of CPU power in the entire network. As explained in Satoshi's Bitcoin white paper:

> *The majority decision is represented by the longest chain, which has the greatest proof-of-work effort invested in it. If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains. To modify a past block, an attacker would have to redo the proof-of-work of the block and all blocks after it and then catch up with and surpass the work of the honest nodes.*[8]

The protocol contains a number of economic rules that serve as monetary policy enacted in code. These rules are "enforced collectively by the network," meaning that if the network came to a consensus about modifying the rules, these policies could change. (It is not clear to me what would happen if some nodes chose to modify these rules, but other nodes did not. Presumably there could be a fork in the blockchain, with two competing transaction histories circulating, as occurred on March 11, 2013, when a new version of a client was released that did not interact harmoniously with the older vision, though I am not sure at what point the fork would occur.) This coded monetary policy is, for the most part, directed at controlling inflation. Bitcoin has a hard limit of currency at about 21 million bitcoins. This limit is estimated to be reached in 2030. To ensure transactional ease, each bitcoin is divisible up to 8 decimal places

[7] For an example of a specialized mining rig, see http://store.avalon-asics.com/?product=avalon-asic-unit.
[8] NAKAMOTO, BITCOIN WHITE PAPER, *supra* note 2, at 3.

(incidentally, the smallest unit, 1 BTC x 10^-8 is called a satoshi in honor of Bitcoin's creator). The mining reward is reduced over time at a set rate. In previous years, the reward was 50 BTC. In 2013, according to a preset schedule, it was reduced to 25 BTC. The code controls for the rate of mining by automatically increasing or relaxing the difficulty of the proof-of-work in response to the rate of generation of blocks.

Bitcoin has the capacity to be anonymous, but in general, anonymity is not currently a prominent design feature.[9] Although it is possible to transact in a way that obscures one's identity, because the Bitcoin network necessarily broadcasts the history of all transactions ever made, analysis of this data can unveil revealing information about particular nodes and their transactional activities.

B. The Users

1. Drugs

The lack of border restrictions, the irreversibility of transactions, and the purposeful removal of government oversight makes Bitcoin, unsurprisingly, a nexus of criminal activity. A significant chunk of Bitcoin transactions occur on the Silk Road, a Tor[10] hidden online marketplace for drugs, which accepts only Bitcoin as a method of payment. Nicolas Christin at Carnegie Mellon has analyzed the Silk Road market place, noting in the August 1, 2012 version

[9] Fergal Reid & Martin Harrigan, *Bitcoin is not Anonymous*, AN ANALYSIS OF ANONYMITY IN THE BITCOIN SYSTEM, Sept. 30, 2011, http://anonymity-in-bitcoin.blogspot.com/2011/07/bitcoin-is-not-anonymous.html. Reid & Harrigan's internet posting is a summary of a part of a formal paper, Fergal Reid & Martin Harrigan, *An Analysis of Anonymity in the Bitcoin System*, May 7, 2013, *available at* http://arxiv.org/abs/1107.4524. *See also* Matthew Green, *Zerocoin: making Bitcoin anonymous*, A FEW THOUGHTS ON CRYPTOGRAPHIC ENGINEERING, Apr. 11, 2013, http://blog.cryptographyengineering.com/2013/04/zerocoin-making-bitcoin-anonymous.html (proposing an addition to Bitcoin to actually enable anonymity).

[10] Tor, short for "The Onion Routers," is an anonymity network that obsfuscates traffic analysis by distributing transactions over multiple nodes all over the internet. *See* TOR PROJECT: OVERVIEW, https://www.torproject.org/about/overview.html.en (including a diagrammed explanation provided by the Electronic Frontier Foundation). Although it is true, as Tor claims, the service is a valuable asset for whistleblowers and journalists who are "maintaining civil liberties online," it is also used for more explicitly harmful activity: for instance, the transmission of child porn. *See* Dan Goodin, *Tor operator charged for child porn transmitted over his servers*, ARS TECHNICA, Nov. 29, 2012, http://arstechnica.com/tech-policy/2012/11/tor-operator-charged-for-child-porn-transmitted-over-his-servers/.

of his paper that "the daily sales on Silk Road correspond to almost 20% of the average daily volume of USD-BTC exchanges on Mt. Gox, the largest exchange forum," but retracting the number to a more modest "4.5%-9% of all exchange trades" in a later version.[11] Christin notes that the majority of exchange trades are speculative in nature, thus even 4.5%-9% of all exchange trades may represent the bulk of transactions for real goods and services. (Incidentally, Christin estimates a 15 million USD annual revenue for the entire marketplace).

The way that Bitcoin is treated by the Silk Road, therefore, may be highly probative of its use in general. Bitcoin, it seems, is not used as a unit of account, but as a medium of exchange. A drop in BTC value (with respect to sovereign currency) is tightly correlated with price increases.[12] The Silk Road offers automatic pegging to the dollar, with an escrow mechanism to buffer sellers from changes in the exchange rate.[13]

2. Exchanges

If Silk Road is the marketplace for the most common transactions in Bitcoin for goods and services, then the exchanges are the marketplace for the most common form of Bitcoin transactions, period: speculative exchanges between sovereign currency and Bitcoin.

Although Bitcoin's most primary design feature is decentralization, most economic activity goes through these few central chokepoint.[14] There are a number of exchanges to choose from, but the market in exchanges is far from competitive, with Mt. Gox handling the vast

[11] Nicolas Christin, *Traveling the Silk Road: A measurement analysis of a large anonymous marketplace*, 22, Aug 1, 2012, http://www.andrew.cmu.edu/user/nicolasc/publications/TR-CMU-CyLab-12-018.pdf. *Cf.* Nicolas Christin, *Traveling the Silk Road: A measurement analysis of a large anonymous marketplace*, 19, Nov. 28, 2012, http://www.andrew.cmu.edu/user/nicolasc/publications/TR-CMU-CyLab-12-018.pdf.

[12] *Id.* at 16.

[13] *See id.*; Andy Greenberg, *Founder of Drug Site Silk Road Says Bitcoin Booms and Busts Won't Kill His Black Market*, FORBES.COM, Apr. 16, 2013, http://www.forbes.com/sites/andygreenberg/2013/04/16/founder-of-drug-site-silk-road-says-bitcoin-booms-and-busts-wont-kill-his-black-market/.

[14] Tyler Moore & Nicolas Christin, *Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk*, presented at the 17th International Conference on Financial Cryptography and Data Security, 2013, *available at* http://lyle.smu.edu/~tylerm/fc13.pdf.

majority of bitcoin conversions.[15] Since mining has greatly increased in difficulty, exchanges become the primary entry point for new traders in the Bitcoin economy. Furthermore, as long as marketplaces like the Silk Road gravitate towards treating Bitcoin as a medium of exchange pegged to sovereign currencies as standard units of value, the exchanges are central in these trades, since the exchanges set the going rate for Bitcoin.

3. Cultural use

It is important to note that although the bulk of economic activity seems to be in either speculation on the exchanges or in the illicit trade in drugs, there are people who use Bitcoin as money—not a mere commodity or transactional platform—for social and cultural reasons.

Bitcoins tend to fall in the hands of internet mainstays who accept Bitcoin donation—e.g., Wordpress,[16] Reddit,[17] and the Internet Archive.[18] Brewster Kahle, founder of the Internet Archive, is a particularly interesting "cultural" user of Bitcoin. The Internet Archive partially pays its employees in donated bitcoins and has convinced a nearby sushi restaurant to accept Bitcoin. An "honor based Bitcoin ATM" (the "ATM" uses an open cash drawer, as opposed to spitting out exact bills) inside the Internet Archive offices converts Bitcoin to cash and vice-versa. Kahle reports that "Bitcoin is becoming a day-to-day currency of the Internet Archive with employees using it as a way to settle small debts, like for dinner," and refers to it as "the local currency of the Internet."[19]

[15] In April 2013, Mt. Gox handled 76% of all Bitcoin trading across the globe. Adrianne Jeffries, *Barons of Bitcoin: the Tokyo-based powerhouse that controls the world's virtual money*, The Verge, Apr. 1, 2013, http://www.theverge.com/2013/4/1/4154500/mt-gox-barons-of-bitcoin.

[16] Bitcoin – Support – Wordpress, WORDPRESS, http://en.support.wordpress.com/bitcoin/.

[17] Brian Simpson, *New Gold Payment Options: Bitcoin and Credit Card*, BLOG.REDDIT, Feb. 14, 2013, http://blog.reddit.com/2013/02/new-gold-payment-options-bitcoin-and.html.

[18] "People have donated over $5000 worth of bitcoins in the last 2 years to the Internet Archive." Brewster Kahle, *Bitcoin is the "local currency" of the Internet*, BREWSTER KAHLE'S BLOG, posted Feb. 20, 2013, http://brewster.kahle.org/2013/02/20/bitcoin-is-the-local-currency-of-the-internet/.

[19] Brewster Kahle, *How the Internet Archive is having Great Time with Bitcoin*, Internet Archive Blogs, Apr. 3, 2013, http://blog.archive.org/2013/04/03/how-the-internet-archive-is-having-great-time-with-bitcoin/.

C. The History

Bitcoin is a *cryptocurrency*—a transactional system based on cryptography. It is not the first cryptocurrency. The idea of cryptocurrency has been around since at least 1985, when cryptographer and cypherpunk David Chaum published the article "Security without Identification: Transaction Systems to make Big Brother Obsolete."[20]

The historical context of Bitcoin cannot be completely understood without the Cypherpunks mailing list.[21] The list, which existed in its most active form from 1992 to 2001,[22] connected hackers, cryptographers, and privacy enthusiasts. Cypherpunks advocated the use of cryptography—which up until that point has been monopolized by governments for purposes of espionage and the protection of state secrets—for the protection of private individuals, against each other and against the government.[23] The philosophical inclinations of this group ranged from the sentiments expressed in Tim May's radical "Crypto Anarchist Manifesto" ("The State will of course try to slow or halt the spread of this technology . . . But this will not halt the spread of crypto anarchy . . . Arise, you have nothing to lose but your barbed wire fences!")[24] to Eric Hughes's milder "A Cypherpunk's Manifesto" ("Privacy is necessary for an open society in the

[20] David Chaum, *Security without Identification: Transaction Systems to make Big Brother Obsolete*, COMMUNICATIONS OF THE ASSOCIATION OF COMPUTING MACHINERY, October 1985, *available at* https://www.cosic.esat.kuleuven.be/apes/papers/p1030-chaum.pdf.gz. Julian Assange, who also subscribed to the cypherpunks mailing list, acknowledged the long history of cryptocurrency in his secret meeting with Eric Schmidt. Transcript of secret meeting, *supra* note 1 (Julian Assange: "Now there has been innovations along these lines in many different paths of digital currencies, anonymous, untraceable etc. People have been experimenting with over the past 20 years.").

[21] Founders of the list include Tim May, the writer of the "Crypto Anarchist Manifesto," and John Gilmore, a co-founder of the legal advocacy group, the Electronic Frontier Foundation. GREENBERG, supra note 4, at 81; Timothy C. May, *The Crypto Anarchist Manifesto*, Nov. 22, 1992, *available at* http://www.activism.net/cypherpunk/crypto-anarchy.html.

[22] Will Rodger, *R.I.P. Cypherpunks*, SECURITYFOCUS, Nov. 29, 2001, at http://www.securityfocus.com/news/294; GREENBERG, *supra* note 4, at 79–80.

[23] *See* GREENBERG, *supra* note 4, at 70 ("For those who understood cryptography, Big Brother could be rendered a toothless nanny.").

[24] *The Crypto Anarchist Manifesto*, *supra* note 21.

electronic age . . . . For privacy to be widespread it must be part of a social contract. People must come together deploy these systems for the common good.")[25].

The cypherpunks' anti-government, individualistic struggle was perhaps most clearly manifested in the U.S. Department of Justice's case against Philip Zimmermann, the creator of Pretty Good Privacy (PGP). [26] PGP was e-mail encryption software made available to the public, a landmark achievement of the movement for "populist privacy." It was widely shared across the internet, thus becoming a cryptographic export in violation of the International Traffic in Arms Regulations (ITAR).[27] The grand jury investigation of Philip Zimmermann (eventually dropped without explanation by the Justice Department, probably in response to public outcry) was considered a "catalyzing event"[28] for cypherpunks, a clear example of both the kind of code the cypherpunks wished to create and distribute in order to protect individual interests, and the kind of authoritarian government backlash that such code would face.

Against this background of crypto anarchy, the idea of cryptocurrency manifested itself over and over again through the years on the Cypherpunks list. David Chaum was perhaps the first, and although his eCash idea did manifest into reality, his company failed and eCash died

[25] Eric Hughes, *A Cypherpunk's Manifesto*, Mar. 9, 1993, http://www.activism.net/cypherpunk/manifesto.html.

[26] GREENBERG, supra note 3, at 75–76. Zimmermann's cause was widely championed by the cypherpunks, but Zimmermann was not a cypherpunk, and did not subscribe to founding member Tim May's philosophy of crypto anarchy. *Id.* at 85 ("Several times Zimmermann ran into May during trips to the Bay Area and pleaded with him to tone down his antigovernment rhetoric."). Although the cypherpunks "held Zimmermann up as a folk hero," *id.* at 86, Zimmermann himself "saw them as angry young men in leather jackets, without children and too much testosterone," *id.* at 85.

[27] *Id.* at 74–76.

[28] Transcript of secret meeting, *supra* note 1 (Julian Assange calls the "attack" on WikiLeaks as a "catalyzing event," and compares it to Philip Zimmermann's grand jury investigation).

alongside it.[29] In 1993, perhaps with Chaum's ideas in mind, Tim May played with the idea of an untraceable digital currency called "CryptoCredits."[30]

In 1998, Wei Dai, another member of the Cypherpunks list proposed an electronic currency he called "b-money."[31] His 1998 proposal opens with support and approval for Tim May's brand of crypto anarchy. He then posits that a crypto anarchic community is impossible without "b-money," since a "community is defined by the cooperation of its participants, and efficient cooperation requires a medium of exchange (money) and a way to enforce contracts."[32] He acknowledges that a central government has always played the role in establishing money and in enforcing contracts, but then proposes that the "b-money" system can replace the need for a government-issued currency.[33]

[29] Greenberg writes that eCash's failure was due to "what some say is bad luck and others say was Chaum's overly controlling style of doing business." GREENBERG, *supra* note 4, at 65. Chaum's ideas, however, are immortalized—so to speak—in a Dutch toll system that can "reliably charge drivers without recording any trace of their identities." *Id.* at 119.

[30] GREENBERG, *supra* note 4, at 89–91. I will return to Tim May's CryptoCredits later in this section.

[31] Wei Dai, *B-Money*, 1998, http://www.weidai.com/bmoney.txt; *B-money Proposal*, BITCOIN WIKI, https://en.bitcoin.it/wiki/B-money_Proposal (last accessed Apr. 28, 2013); Nikolei M. Kaplanov, *Nerdy Money: Bitcoin, the private digital currency, and the case against its regulation*, 25 LOY. CONSUMER L. REV. 111, 114–15; Reuben Grinberg, *Bitcoin: An Innovative Alternative Digital Currency*, 4 HASTINGS SCI. & TECH. L.J. 159, 162 (2012).

[32] Wei Dai, *supra* note 31.

[33] *Id.* The two pertinent paragraphs are reproduced in full below:

> *I am fascinated by Tim May's crypto-anarchy. Unlike the communities traditionally associated with the word "anarchy", in a crypto-anarchy the government is not temporarily destroyed but permanently forbidden and permanently unnecessary. It's a community where the threat of violence is impotent because violence is impossible, and violence is impossible because its participants cannot be linked to their true names or physical locations.*
>
> *Until now it's not clear, even theoretically, how such a community could operate. A community is defined by the cooperation of its participants, and efficient cooperation requires a medium of exchange (money) and a way to enforce contracts. Traditionally these services have been provided by the government or government sponsored institutions and only to legal entities. In this article I describe a protocol by which these services can be provided to and by untraceable entities.*

Wei Dai's "b-money" proposal shares many key technical characteristics with Bitcoin.[34] But the proposal was admittedly "impractical" and could not be implemented in practice. Bitcoin solved the problems of "b-money" with a synthesis of several cryptographic innovations. "B-money" is recognized on the official Bitcoin website (originally registered by Satoshi himself) as a precursor to Bitcoin,[35] and has been identified in law journal articles as its intellectual parent.[36]

But where Wei Dai's "b-money" was explicitly connected to the cypherpunks, and to Tim May's crypto anarchy, Bitcoin's creator never avowed such a connection. By 2008, the year that Satoshi published his white paper, the cypherpunks mailing list was past its heyday, having been declared "dead" by founding member John Gilmore in 2001.[37] The Bitcoin white paper did not appear in the Cypherpunks list, but rather the Cryptography mailing list.[38] Although cypherpunks like Julian Assange[39] readily claim Bitcoin as having "evolv[ed] out of the cypherpunks,"[40] Satoshi does not mention the cypherpunks or crypto anarchy in his internet postings.

Instead, Bitcoin was introduced to the world in the context of the 2008 financial crisis. When launching his innovation in 2009, Satoshi writes,

> *The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that*

[34] "Like the B-money proposal, bitcoin itself also uses the hashcash cost-function as the proof-of-work during coin minting." *B-money Proposal*, *supra* note 31.
[35] *About – Bitcoin*, BITCOIN.ORG (last accessed: Apr. 28, 2013), http://bitcoin.org/en/about.
[36] *See* Kaplanov, *supra* note 31, at 114–15; Grinberg, *supra* note 31, at 162.
[37] Rodger, *supra* note 22. John Gilmore hosted the mailing list at toad.com from its inception, and his ceasing to host was considered by many to be its "death." The mailing list continues to be hosted elsewhere. *Id.* ("The Cypherpunks list will continue to be hosted on other sites, but many participants agree that the ejection from its birthplace is a moribund milestone.").
[38] *See* Satoshi Nakamoto's posts to the Cryptography mailing list, http://www.mail-archive.com/search?l=cryptography@metzdowd.com&q=from:%22Satoshi+Nakamoto%22.
[39] Assange began posting to the list in 1995. GREENBERG, *supra* note 4, at 114.
[40] Transcript of secret meeting, *supra* note 1 (Julian Assange: "Okay, Bitcoin is something that evolved out of the cypherpunks a couple of years ago, and it is an alternative... it is a stateless currency.").

> *trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve.*[41]

The language used in the white paper itself is cold and apolitical, declining to even use the words "government" or "sovereign," instead setting up Bitcoin as an alternative to a system controlled by "financial institutions."[42] This careful language stands in stark contrast to Bitcoin's earlier predecessors—Chaum's proposal "to Make *Big Brother* Obsolete" (emphasis added) and Wei Dai's proposal to facilitate true crypto anarchy. In the moment of financial crisis in 2008, Satoshi instead focuses his skepticism and anger towards the banks. Indeed, the first block of Bitcoin is encoded with the following message:

> *The Times 03/Jan/2009 Chancellor on brink of second bailout for banks.*[43]

But regardless of his animosity towards the financial system and its entrenched interests, Satoshi did not seem to be interested in using Bitcoin as a weapon against the government per se, unlike the cypherpunks. In 1993, Tim May had, as an experiment, created an advertisement for BlackNet, a cryptographically secure market in government secrets that would pay leakers in an "untraceable digital currency" called "CryptoCredits."[44] BlackNet never really existed, and neither did CryptoCredits.[45] But in 2010, as the government pressured payment processors to institute the WikiLeaks financial blockade[46] (in which the flow of donations to WikiLeaks were voluntarily frozen by the third party processors), Tim May's prank seemed to have become a reality—with WikiLeaks taking the place of BlackNet, and Bitcoin taking the place of

[41] Satoshi Nakamoto, *Bitcoin open source implementation of P2P currency*, posted on Feb. 11, 2009 at 22:27, P2P Foundation, http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source?commentId=2003008%3AComment%3A9562.
[42] *See generally* NAKAMOTO, BITCOIN WHITE PAPER, *supra* note 2.
[43] Maria Bustillos, *The Bitcoin Boom*, THE NEW YORKER, Apr. 2, 2013, http://www.newyorker.com/online/blogs/elements/2013/04/the-future-of-bitcoin.html; *2.5Mb of Wikileaks Cables Embedded in the Bitcoin Blockchain*, THE BITCOIN TRADER, Apr. 23, 2013, http://www.thebitcointrader.com/2013/04/25mb-of-wikileaks-cables-embedded-in.html.
[44] GREENBERG, *supra* note 4, at 89–91.
[45] *Id.* at 90.
[46] Binoy Kampark, *Economic Blockade and WikiLeaks: Iceland and Beyond*, Scoop News, Apr. 29, 2013, http://www.scoop.co.nz/stories/WO1304/S00466/economic-blockade-and-wikileaks-iceland-and-beyond.htm.

CryptoCredits. But although Assange apparently felt an ownership in Bitcoin and a kinship to its creator, Satoshi was vehemently against connecting their two projects, feeling that Bitcoin "was still too small to take that much attention."[47] WikiLeaks abstained from taking Bitcoin donations until after Satoshi disappeared in April 2011.[48]

In June 2011, only a little while after WikiLeaks began to solicit for Bitcoin donations, Julian Assange met secretly with Google CEO Eric Schmidt and former Secretary of State advisor Jared Cohen.[49] In the meeting, Assange breezily associates Bitcoin with the cypherpunks and with WikiLeaks. He then describes new ideas that essentially use the basis of the Bitcoin protocol to create an anonymous, secure, and dependable peer-to-peer network for leaking. There is no mention of Satoshi's ambivalence towards WikiLeaks, and his lack of any substantive personal link to the cypherpunks: in this conversation, Assange glibly co-opts the Bitcoin project as being part of his own, blatantly political project.

In the same month, Bitcoin entered a new phase of legal uncertainty. The Electronic Frontier Foundation (EFF), a legal advocacy organization for digital civil liberties, co-founded by cypherpunk John Gilmore, had been accepting Bitcoin donations for some time. But then the organization publicly stopped accepting donations, writing, "While EFF is often the defender of people ensnared in legal issues arising from new technologies, we try very hard to keep EFF from becoming the actual subject of those fights or issues."[50] This move cast a stain on the

[47] Bustillos, *supra* note 43 ("Nakamoto rejected the idea [of WikiLeaks taking bitcoin donations] vehemently.").

[48] Davis, supra note 3, at 68 ("Then, in April, 2011, he sent a note to a developer saying that he had 'moved on to other things.' He has not been heard from since."); Andy Greenberg, *WikiLeaks Asks for Anonymous Bitcoin Donations*, FORBES.COM, Jun. 14, 2011, http://www.forbes.com/sites/andygreenberg/2011/06/14/wikileaks-asks-for-anonymous-bitcoin-donations/.

[49] Transcript of secret meeting, *supra* note 1.

[50] Cindy Cohn, *EFF and Bitcoin*, EFF DEEPLINKS BLOG, Jun. 20, 2011, https://www.eff.org/deeplinks/2011/06/eff-and-bitcoin (listing vectors of legal uncertainty regarding Bitcoin, including "securities law, the Stamp Payments Act, tax evasion, consumer protection and money laundering, among others"). Much of Grinberg's article on Bitcoin, published in 2012, is aimed at analyzing these legal issues; indeed, it seems likely that the portion of the

legitimacy of the currency, one that only began to fade once FinCEN released guidance specifically regarding electronic currencies.[51]

C. The Hype

The EFF's June 2011 announcement was unexpected, given that Rainey Reitman, Activism Director of the EFF, some months earlier had called Bitcoin as "a step toward censorship-resistant digital currency."[52] Reitman, also a founder of the Bradley Manning Support Network,[53] wrote optimistically on Bitcoin's ability to "re-establish privacy and autonomy."[54] In her view, if Bitcoin "were to live up to the dreams of its creators," it would "offer the kind of anonymity and freedom in the digital environment we associate with cash used in the offline world."[55]

This theme is repeated—inflated with certainty and absolutism—in the media: *Bitcoin is anonymous and untraceable*. Bitcoin has been called "a secure, private, decentralized type of money that makes possible anonymous and virtually costless transactions across borders."[56] Another journalist has claimed that "a Bitcoin has no serial number or any possible mechanism that could be used to trace it back to a buyer or seller."[57]

article dedicated to Bitcoin's legal issues is in response to the EFF's June 2011 announcement. Grinberg, *supra* note 30, at 166 n.24, 181–206.

[51] Timothy B. Lee, *US regulator: Bitcoin exchanges must comply with money-laundering laws*, ARS TECHNICA, Mar. 19, 2013, http://arstechnica.com/tech-policy/2013/03/us-regulator-bitcoin-exchanges-must-comply-with-money-laundering-laws/.

[52] Rainey Reitman, *Bitcoin – a Step Toward Censorship-Resistant Digital Currency*, EFF DEEPLINKS BLOG, Jan. 20, 2011, https://www.eff.org/deeplinks/2011/01/bitcoin-step-toward-censorship-resistant.

[53] *Rainey Reitman*, ELECTRONIC FRONTIER FOUNDATION, https://www.eff.org/about/staff/rainey-reitman. The Bradley Manning Support Network advocates "for the release of accused WikiLeaks whistleblower Pfc. Bradley Manning."

[54] Reitman, *supra* note 52.

[55] *Id.*

[56] Eric Posner, *Fool's Gold*, SLATE.COM, Apr. 11, 2013, http://www.slate.com/articles/news_and_politics/view_from_chicago/2013/04/bitcoin_is_a_ponzi_scheme_the_internet_currency_will_collapse.html.

[57] Sam Biddle, *What is Bitcoin?*, GIZMODO, Apr. 10, 2013, http://gizmodo.com/5803124/what-is-bitcoin.

Such statements are not strictly correct. They mistake the sincere hope of privacy advocates like Reitman (who noted correctly in her January 2011 post, written long before the frenzy of mainstream media interest in Bitcoin that erupted in 2013,[58] that Bitcoin's "current implementation" is not secure[59]) for actual functionality coded into Bitcoin. In truth, anonymity has never been a prominent design feature of Bitcoin,[60] even if the currency's predecessors (e.g., Chaum's eCash) were obsessed with it.

Bitcoin's most prominent design feature, rather, is its decentralization.[61] This theme is also trumpeted throughout the media,[62] and its radical challenge to the current U.S. monetary system as controlled by the Federal Reserve is recognizable, even by journalists with only a superficial understanding of the protocol. The claim to and aspiration of decentralization goes to the heart of the protocol, and to the heart of the beliefs of many Bitcoin users about monetary systems in general. These beliefs are perhaps best summed up in the following stanzas from a poem written in honor of Bitcoin's since-vanished creator:

> *In the year of the bailouts, 2008,*
> *The bankers were printing more debt for the state*
> *The dollar grew weaker, the big picture clear*
> *As they fed the hangover more Keynesian beer [. . .]*
>
> *Who's to blame, is this caused by desire for wealth?*
> *When perhaps the real problem is money itself!*

[58] *See* Felix Salmon, *The Bitcoin Bubble and the Future of Currency*, Apr. 3, 2013, https://medium.com/money-banking/2b5ef79482cb (noting the recent interest in Bitcoin, "because of the Cyprus connection, mainstream publication have a handy real-world news hook, now, with which to explain the bitcoin phenomenon"). Perhaps the biggest indicator of mainstream awareness of Bitcoin was the appearance of economist Paul Krugman's op-ed on Bitcoin, Paul Krugman, Op. Ed., *The Antisocial Network*, N.Y. TIMES, Apr. 14, 2013, *available at* http://www.nytimes.com/2013/04/15/opinion/krugman-the-antisocial-network.html.

[59] Reitman, *supra* note 52.

[60] Reid & Harrigan, *supra* note 9; Green, *supra* note 9.

[61] NAKAMOTO, BITCOIN WHITE PAPER, *supra* note 2, at 1 ("A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution.").

[62] Biddle, *supra* note 57 ("Aside from the software developers who work on new versions of the code that underpins Bitcoin, there's no Central Bitcoin Bank—no virtual Federal Reserve. Bitcoins are backed by no one and nothing and completely unregulated.").

The idea isn't new, maybe everything's tanking
'Cause society is built on fractional reserve banking[63]

Under this view, centralization is bad; decentralization will free transactional activity from the middle-men who take bailout money and inflate currency through overprinting. From the beginning, the Bitcoin protocol has been shaped by a "digital metallism"—a term I borrow from Maurer, Nelms, and Swartz in their article on the semiotics of Bitcoin.[64] Indeed, the release of new bitcoins into the economy is explicitly compared to gold mining in Nakamoto's white paper.[65] The design of Bitcoin—hard-coded to be decentralized and deflationary—is informed by a very specific understanding of money. I would argue that the technology of Bitcoin can in itself be viewed as an critical response to theories of money centered on government issuance, and Bitcoin's mixed success can inform our understanding of what money is or should be.

<u>II. How to understand money?</u>

<u>A. Money as a method of transmission</u>

> *The Bitcoin actually has the balance and incentives right, and that is why it is starting to take off. The different combination of these things. No central nodes. It is all point to point. One does not need to trust any central mint. If we look at traditional currencies such as gold, we can see that they have sort of interesting properties that make them valuable as a medium of exchange. Gold is divisible, it is easy to chop up, actually out of all metals it is the easiest to chop up into fine segments. You can test relatively easily whether it is true or whether it is fake. You can take chopped up segments and you can put them back together by melting the gold. So that is what makes it a good medium of exchange and it is also a good medium of value store, because you can take it and put it in the ground and it is not going to decay like apples or steaks. The problems with traditional digital currencies on the internet is that you have to trust the mint not to print too much of it.*
>
> Julian Assange, June 23, 2011[66]
>
> *We have elected to put our money and faith in a mathematical framework that is free of politics and human error.*
>
> Tyler Winklevoss, April 11, 2013[67]

[63] *An Ode to Satoshi Nakamoto*, THE BITCOIN TRADER, Dec. 15, 2011, http://www.thebitcointrader.com/2011/12/ode-to-satoshi-nakamoto.html.

[64] Bill Maurer, Taylor Nelms & Lana Swartz, *"When perhaps the real problem is money itself!": the practical materiality of Bitcoin*, SOCIAL SEMIOTICS 2 (2013), *available at* http://llaannaa.com/papers/maurer_nelms_swartz_bitcoin.pdf.

[65] NAKAMOTO, BITCOIN WHITE PAPER, *supra* note 2, at 4 ("The steady addition of a constant of amount of new coins is analogous to gold miners expending resources to add gold to circulation. In our case, it is CPU time and electricity that is expended.").

[66] Transcript of secret meeting, *supra* note 1.

The debate on the nature of money tends to focus on the role of government. One understanding of money minimalizes the government's role as much as possible, the other sees it as necessary—one historical example of this disagreement would be the metallist and chartalist schools of thought in the 16th and 17th centuries, with the metallist tradition tending to take on a "real" analysis of money ("Money enters the picture only the modest role of a technical device that has been adopted in order to facilitate transactions") and the chartalist tradition taking on a "monetary" analysis in direct opposition to the "real" analysis.[68] (A modern-day version of this dichotomy would be the "Monetarist-Keynesian debates").[69]

In the metallist account, money originates as a medium of exchange, a method of transmitting value. Money reduces the inefficiency of barter, providing liquidity to markets. In order to fulfill this function, the commodity that becomes money must be "a thing that is useful and has exchange value independently of its monetary function."[70] Societies eventually settle on precious metals for a number of reasons—its divisibility, its permanence, its ability to take and retain an imprimatur for the purposes of "identifiability." For the metallist account, the existence of government, or some other central mint, is begrudged for the purposes of solving the "identifiability" problem—thus, government imprimatur on currency is a matter of alleviating consumer confusion.

The limited necessity of government is emphasized, to the point of suggesting "that the money chosen by society is either sanctioned (*ex post*) by the government . . . or that it somehow

[67] Nathaniel Popper & Peter Lattman, *Never Mind Facebook; Winklevoss Twins Rule in Digital Money*, NY TIMES, Apr. 11, 2013, http://dealbook.nytimes.com/2013/04/11/as-big-investors-emerge-bitcoin-gets-ready-for-its-close-up/.

[68] Stephanie Bell, *The role of the state and the hierarchy of money*, 25 CAMBRIDGE J. OF ECON. 149, 151 (2001), *available at* http://econpapers.repec.org/article/oupcambje/v_3a25_3ay_3a2001_3ai_3a2_3ap_3a149-63.htm.

[69] *Id.* at 161.

[70] *Id.* at 152 (quoting J.A. Schumpeter, HISTORY OF ECONOMIC ANALYSIS (1994)).

evolves into government-issued currency."[71] In order to minimize the role of government in this story, the metallist theory places great weight on the commodity value of the metal coins, "which [make] them a convenient medium of exchange, not because of any influence or encouragement from the state."[72] As money moved from metal coin, to paper notes with a metallic backing, to fiat paper currency, the metallist story evolved towards reducing money to "a pure number, the *numeraire*."[73]

A few points should be mentioned here. (1) Bitcoin seems to be an elaborate circumvention of the need for the government imprimatur to solve the "identifiability" problem, thus "proving" the metallist's contention that government involvement is not of central importance to currency. (2) On the other hand, the bitcoin does not fit with traditional metallist accounts, since it is not a commodity with any value in and of itself. Indeed, it does not fit with the labor theory of value either, since the "work" in "proof-of-work" is meaningless brute-force computer labor set to an arbitrary difficulty meant to keep the rate of mining constant. (3) However, as noted by Maurer et al., the Bitcoin community places its trust in "numbers"—that is, the integrity of the cryptographic code underlying Bitcoin—to create the kind of "soundness" of commodity money.[74] (4) The bitcoin, which only exists within a vast, publicly-broadcast purely electronic accounting system, at first seem to perfectly fit the bill of the Walrasian *numeraire*. But, in order to truly be a *numeraire* that "allow[s] the 'auctioneer' to announce prices . . . in order to bring about market-clearing equilibrium,"[75] the bitcoin must be able to be a stable unit of account. (In Section III, I will discuss Bitcoin's chronic instability).

[71] *Id.* at 152.
[72] *Id.* at 153.
[73] *Id.*
[74] Maurer, et al., *supra* note 64, at 13.
[75] Bell, *supra* note 68, at 153.

B. Money as a constitutional project

Nothing made by humans is ever free of politics or even error.

Dan Kaminsky, security researcher, May 3, 2013[76]

Alternatively, money can be viewed as a constitutional project, "a mode of governance."[77] Rather than evolving out of barter in the marketplace, money arises out of the government-imposed obligation to pay taxes—in an early era, this taxation takes the form of corvee labor and mandatory military service.[78] The stream of labor and services can be organized efficiently by the sovereign giving tokens in exchange for whatever is immediately needed. The tokens are then accepted by the sovereign at some future date in lieu of the specific taxation obligation. Households are incentivized to give the sovereign their contribution in advance through because the tokens provides liquidity to private exchange.

But under this view of money, this liquidity isn't an improvement upon barter, but rather the shuffle of legal obligations from household to household. Thus, private transactions become an extension of sovereign activity, and the sovereign has good reason to "recognize and support exchanges between individuals that occurred for money"[79]—that is, to enforce contracts under the law.

In contrast to the metallist account, under this view, it is not "the content of the coin that gave it a priced value, but the system that made coin into money"[80]—and that system was fiscal, built around "tax collections and routinized spending," with coins minted and aggressively reminted in order to keep tax periods from too much overlap. Monetary policies are instituted to

[76] Dan Kaminsky, *Let's Cut Through the Bitcoin Hype: A Hacker-Entrepreneur's Take*, WIRED, May 3, 2013, http://www.wired.com/opinion/2013/05/lets-cut-through-the-bitcoin-hype/ (specifically replying to the Winklevoss Twins' assertion that Bitcoin is "free of politics and human error.").

[77] Christine Desan, *Creation Stories: Myths About the Origins of Money*, at 30, (draft 2013), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2252074.

[78] *Id.* at 31.

[79] *Id.* at 34.

[80] *Id.* at 38.

stabilize the monetary demand and the price of coin (in medieval England, minting on demand for a price becomes such a monetary policy).[81] In this story, "[n]othing about the way money operates or the market it makes possible is static or self-equilibrating. The money supply itself is not fixed."[82] Money is not a market-created method of transmission, but an artificial, highly-engineered method of spreading tax obligations and instituting fiscal projects, with the sovereign a necessary and central aspect to the story.

III. The Politics of Bitcoin

A. Evaluating Bitcoin as a libertarian experiment

> *Who's to blame, is this caused by desire for wealth?*
> *When perhaps the real problem is money itself!*
> *The idea isn't new, maybe everything's tanking*
> *'Cause society is built on fractional reserve banking*
>
> Ode to Satoshi Nakomoto, Dec. 15, 2011[83]

If Bitcoin is money—and it may be fair to say it is not, though that would seem disingenuous, given the robust volume of trade in Bitcoin[84] and distinctly money-like flavor of the practices surrounding it—then the cryptocurrency represents a serious challenge to accounts of money as dependent on sovereign power and taxing obligations.[85] Bitcoin is designed to eschew a central mint. No government exists to impose taxes.

But if Bitcoin seems difficult to understand from those accounts, it is because it is purposefully designed libertarian, neo-metallist experiment. The first thing to do when approaching the question "How do we understand Bitcoin?" is to understand that the experiment

[81] *Id.* at 42–43.
[82] *Id.* at 45.
[83] *An Ode to Satoshi Nakamoto*, THE BITCOIN TRADER, Dec. 15, 2011, http://www.thebitcointrader.com/2011/12/ode-to-satoshi-nakamoto.html.
[84] *About – Bitcoin*, BITCOIN.ORG (last accessed: Apr. 28, 2013), http://bitcoin.org/en/about (claiming "[o]ver $1 million USD of daily trade volume distributed across 40,000 transactions.").
[85] Bitcoin probably contradicts Modern Monetary Theory with the greatest severity, because of the absence of the taxation. Although I argue here that Bitcoin can be reinterpreted as a constitutional project, under MMT, Bitcoin likely cannot be understood as money at all.

has met with mixed success. Bitcoin is decentralized in code, but not in practice. Because the "value" of Bitcoin to its users is dependent on its convertibility to sovereign currencies like the dollar,[86] and because the technological arms race in mining rigs means that the easiest way the average user can acquire more bitcoins with which to transact is by buying bitcoins with sovereign currency, economic activity is ultimately clustered around the exchanges, with only one or two exchanges handling the bulk of all dollar-to-Bitcoin conversions.[87]

The exchanges represent a dilemma for the Bitcoin community: at the moment they are—for the reasons I have described—necessary. But their centrality to transacting, and their active interest in deanonymizing their customers,[88] also makes them attractive targets for both sovereign governments and hackers.

The assent of Mt. Gox, the biggest exchange, to regulation by the United States through FinCEN[89] represents a major victory for the United States government in keeping Bitcoin under control. While anonymized illegal activity is still *possible*, in practice, even those who have much to hide do not take the necessary steps to anonymize their movements.[90] The regulation of Mt. Gox under FinCEN does not necessarily mean the surrender of all their customers' data and movements, but is an important signal that the largest exchange is willing to work with sovereign

[86] *See* Kashmir Hill, *Living on Bitcoin for a Week, Day 1*, Forbes.com, May 1, 2013, http://www.forbes.com/sites/kashmirhill/2013/05/01/living-on-bitcoin-for-a-week-the-journey-begins/ (detailing an attempt to live on Bitcoin for a week; Bitcoin is not widely accepted enough—even in the tech mecca of San Francisco—to meet one's needs without converting Bitcoin). Hill wrote on Twitter of her experience, "I'm living on Bitcoin for a week. So far it means I'm really hungry, caffeine deprived and walking many miles." https://twitter.com/kashhill/status/329671931118895104.

[87] *See, e.g.*, Adrianne Jeffries, *Barons of Bitcoin: the Tokyo-based powerhouse that controls the world's virtual money*, The Verge, Apr. 1, 2013, http://www.theverge.com/2013/4/1/4154500/mt-gox-barons-of-bitcoin.

[88] Mt. Gox, for instance, privileges transactions made by deanonymized customers, placing stricter withdrawal/buy limits on non-verified users. *See* AML Account Statuses, Mt. Gox, https://support.mtgox.com/entries/20919111-AML-Account-Statuses (last accessed: May, 8, 2013).

[89] Adrianne Jeffries, *supra* note 87, (noting that "Mt. Gox had already inked a partnership with a FINCEN-registered company in order to ensure that its North American transactions are all above-board."). In a strange turn of events, however, its FinCEN-registered partner is now suing Mt. Gox. Adrian Chen, *Massive Bitcoin Business Partnership Devolves into $75 Million Lawsuit*, Gawker, May 2, 2013, http://gawker.com/massive-bitcoin-business-partnership-devolves-into-75-487857656.

[90] Reid & Harrigan, *supra* note 9.

governments. Since a very significant chunk of all Bitcoin transactions are in the illegal traffic of drugs, Mt. Gox's cooperation with the United States government in this first instance is a nontrivial victory for the government, and a strange turn considering the libertarian, anti-statist origins of Bitcoin.

Mt. Gox, and other exchanges, are also extremely attractive to hackers, who can either aim to "steal" bitcoin held in trust for their customers[91] or to enact a distributed denial of service on the exchanges in order to manipulate the market[92]. When Mt. Gox is taken down, for instance, the price of Bitcoin plummets—when the largest market for Bitcoin is taken away, it apparently becomes difficult to find buyers (but not sellers, for some reason), and thus the exchange rate goes down. During a recent DDOS attack, I personally observed the exchange rate spiral down the longer Mt. Gox stayed unavailable, then watched it rocket upwards again when Mt. Gox came back online. In the interim, many of the alternate exchanges and money markets (for instance, Coinbase) actually ran out of bitcoins to sell. In a competitive market, supply and demand should have kept the exchange rate constant (especially since this DDOS market manipulation has happened more than once), but the fact that Mt. Gox handles such a large proportion of all exchange transactions and the other exchanges handle so few creates a very strange effect when Mt. Gox is attacked. Some have noted that it is impossible to tell whether the

[91] The bitcoins have to go somewhere for a dollars to bitcoins transaction. A wallet created on the spot, controlled directly by the exchange, but controllable by the user through the exchange interface is a simple way to handle this. Users can certainly withdraw bitcoins and send them to their own wallet addresses if they have them (subject to withdrawal limits). It would be feasible for exchanges to skip the exchange controlled wallet and send bitcoins directly to a user specified address, but none of the exchanges seem to practice this method.

[92] A distributed denial of service is an attack orchestrated to bring down a web server by drowning it too many requests for access. The requests are often "fraudulent," originating from botnets. Mt. Gox addressed the DDOS money market manipulation on their Facebook page, see https://www.facebook.com/MtGox/posts/453409538076792 ("Attackers wait until the price of Bitcoins reaches a certain value, sell, destabilize the exchange, wait for everybody to panic-sell their Bitcoins, wait for the price to drop to a certain amount, then stop the attack and start buying as much as t2whey can. Repeat this two or three times like we saw over the past few days and they profit."). *See also* Kim-mai Cutler, *Bitcoin Suffers a Correction Amid Apparent DDOS Attacks on Some Exchanges*, TECHCRUNCH, Apr. 10, 2013, http://techcrunch.com/2013/04/10/bitcoin-crash/.

exchange rate displayed by Mt. Gox is the "true" exchange rate in the free market[93]—such is the distorting effect of this particular exchange.

These issues—the centrality and importance of the exchanges, the attractiveness of the exchanges to DDOS attacks as market manipulation—occur against a background of extreme volatility for the value of the bitcoin. Volatility is the cause of these issues, and in turn, these issues likely contribute to volatility in turn. It is not entirely clear why bitcoin is so unstable, but certainly, part of its astronomic rise in price from 2009 to 2013 (around 1 BTC to $150 at the time of writing) has to be its intentionally deflationary tendencies (the constant rate of mining, the slowly decreasing rewards for mining) interacting with an ever-increasing demand for bitcoins as the Silk Road handles more and more transactions.[94] The frequent crashes are likely to due to speculation, which in turn probably occurs because the hyperdeflation makes Bitcoin seem like an attractive investment (and of course, increasing speculation feeds itself).

Volatility and hyperdeflation are serious problems with Bitcoin, but are hardly the death knell for Bitcoin that some believe it to be.[95] Certainly, these issues have caused real problems for real people. One Silk Road dealer reports losing $200,000 to currency price fluctuations.[96] These problems are not easily solved without a change to how the Bitcoin protocol operates—in other words, a change to its coded monetary policy of deflation, or through other price-

[93] Jeremy Kirk, *Largest bitcoin exchange, Mt. Gox, 'throttles' trading to tame price swings*, COMPUTERWORLD, Apr. 21, 2013, http://www.computerworld.com/s/article/9238571/Largest_bitcoin_exchange_Mt._Gox_39_throttles_39_trading_to_tame_price_swings ("…Mt. Gox's market tends to set the price of bitcoin since it is has the highest volume of trades and users.").

[94] Adrianne Jeffries, *Online drug dealers back on Silk Road after mysterious two-week outage*, THE VERGE, Nov. 21, 2012, http://www.theverge.com/2012/11/21/3675278/silk-road-operator-says-fail-whale-not-feds-brought-down-notorious/in/3709249 ("Server overload, basically, due to the continuous, rapid increase of members, which led to the site being unusable."). As noted earlier, the Silk Road only accepts Bitcoin; thus those wishing to transact in this marketplace *must* acquire bitcoins.

[95] *See, e.g.*, Joe Weisenthal, *The Bitcoin Economy Is Going Through A Massive Bout Of Hyperdeflation That Could Be Devastating*, BUSINESS INSIDER, Apr. 1, 2013, http://www.businessinsider.com/bitcoin-hyperdeflation-2013-4.

[96] Alex McClintock, *Internet Drug Dealers Are Really Nice Guys*, VICE.COM, Apr. 29, 2013, http://www.vice.com/read/internet-drug-dealers-are-really-nice-guys.

stabilizing mechanisms. But on the other hand, the effects of these problems can be diminished by simply using something else—e.g., a sovereign currency like the dollar—as a unit of account. This is how Silk Road handles this issue, offering an escrow option for dealers in order to peg the amount of money they receive to the going exchange rate at the time of the posting.[97] This is also how the Bitcoin Foundation—one of the few employers that does pay salaries in Bitcoin—deals with paying salaries.[98] The thought behind these remedial measures is that as long as prices are flexible (or indeed, automatically flexible), Bitcoin's volatility will not adversely affect its users.

But pegging the bitcoin to the dollar in these transactions has made Bitcoin into a shadow currency, dependent on the dollar. Vendors who accept bitcoin choose escrow mechanisms like that of Silk Road, thus depending on an exchange-like entity to stabilize their profits, or try to immediately cash out (through the exchanges),[99] or they voluntarily subject themselves to the volatility in price. (Small wonder then, that even in San Francisco, a city both bullish on technology and obsessed with coffee, one cannot even get a decent cup of coffee for bitcoin.)[100] No one takes on debt in Bitcoin.[101]

Bitcoin is most predictable and useful to transacting parties who rely heavily on the exchanges and escrow mechanisms to stabilize how their transactions come out: thus, Bitcoin is

[97]Greenberg, *Silk Road*, *supra* note 13.

[98] Noam Cohen, *Bubble or No, This Virtual Currency Is a Lot of Coin in Any Realm*, N.Y. TIMES, Apr. 7, 2013, http://www.nytimes.com/2013/04/08/business/media/bubble-or-no-virtual-bitcoins-show-real-worth.html (Andresen saying, "the foundation has decided that, because of those fluctuations, his bitcoin salary would be adjusted each month.").

[99] *See* Cyrus Farivar, *OKCupid says it will accept Bitcoin, as currency falls to recent low*, ARS TECHNICA, Apr. 16, 2013, http://arstechnica.com/business/2013/04/okcupid-says-it-will-accept-bitcoin-as-currency-falls-to-recent-low/ ("Our plan is to liquidate our holdings daily and turn them into US dollars.").

[100] Hill, *supra* note 86.

[101] However, some of the exchanges have voluntarily assumed responsibility for deposits lost to hacking. *See* Adrianne Jeffries, *Barons of Bitcoin*, *supra* note 15.

reduced to a pure method of transmission wholly dependent on the exchanges—just another PayPal.

This dependency on the exchanges is brushed off by some writers.[102] Indeed, if one simply seeks to promote Bitcoin as a mere technological innovation, as a platform for future money transmission services,[103] Bitcoin's dependence on the exchanges and on the dollar is not a problem. In fact, the fact that Bitcoin attempts to be a unit of account by adopting its own unit—the bitcoin—is a charming superfluity, a cute but wholly unnecessary cultural reference, similar to the 3d printed coins "containing" bitcoin in RFID chips that sometimes circulate as money.[104] The overemphasis on the metallist understanding of money as a method of transmission, as tool of liquidity in markets, rather than a unit of account leads us to a strange place where the *political project* of bitcoin (ironically a political project that draws from the libertarian tradition, its understanding of money and all) withers away into a pallid shadow of what it could be.

It becomes tempting, at this point, to simply say that if one believes that money is inherently political, then Bitcoin is not money at all, and that its failure to be used as a unit of account is proof that the libertarian experiment is a bust. But this would be an odd outcome: Bitcoin moves and circulates like currency, Bitcoin is traded for goods and services as though it were currency, and Bitcoin attempts to denominate itself in its own unit of account that is used in its own public, peer-to-peer ledgers—what is the protocol, other than a massive, unforgeable ledger system of debts paid and money moved?

[102] *See, e.g.*, Timothy B. Lee, *Bitcoin Is A Bad Currency But It Might Be A Good Platform For Financial Innovation*, FORBES.COM, Apr. 1, 2013, http://www.forbes.com/sites/timothylee/2013/04/01/bitcoin-is-a-bad-currency-but-it-might-be-a-good-platform-for-financial-innovation/.
[103] *Id.*
[104] *See, e.g.*, The NFC-Enabled Bitcoin, CRYPTOPRINTING, http://www.3dp4btc.com/the-nfc-enabled-bitcoin/ (last accessed: May 5, 2013).

Bitcoin is an evolving, distributed constitutional project. It is part currency and part payment system; part utopian and part pragmatic. Its problems and flaws are exceedingly difficult to address, but not fatal. Yes, Bitcoin is difficult to fit into a political understanding of money. But perhaps that understanding is presently incomplete. Is a sovereign government necessary for money? Is taxation necessary?[105] Is a fiscal project necessary?[106] In order to understand Bitcoin as a constitutional project, such projects must be expanded not only to include sovereign governments held together by formal laws backed by a monopoly on force, but on voluntaristic, anarchistic communities bounded by social understandings and code as law.

B. Bitcoin as Law

> *Your legal concepts of property, expression, identity, movement, and context do not apply to us. They are all based on matter, and there is no matter here.*
>
> John Perry Barlow, *A Declaration of the Independence of Cyberspace*, 1996

> *Liberty in cyberspace will not come from the absence of the state. Liberty there, as anywhere will come from a state of a certain kind.*
>
> Lawrence Lessig, *Code 2.0*, 2006

Understanding Bitcoin as a political project requires two steps. The first is a conceptual one—one must import Lawrence Lessig's understanding of code—architectural features of cyberspace—as regulation or law, into this discussion. The second step is part observation, and part conjecture: although Bitcoin's destiny *seems* to be hardcoded into its protocol, the fact is that changes can be implemented, and at some point in the future, assuming that Bitcoin lasts that long, *must* be implemented, and one can look to a much smaller crisis that occurred in March 2013 to see *who decides* when it comes to this putatively decentralized currency.

1. Code is Monetary Policy

[105] As I have noted earlier, voluntary donations in Bitcoin are often given to popular websites like the Internet Archive. The tendency of money to move into the hands of such organizations (which purport to serve the common good of the Internet at large) resembles, to me, a kind of voluntary tribute—a self-organized tax.

[106] David Graeber gives an account of debt and credit among medieval Muslim merchants, essentially a ledger system without any sovereign power to enforce it. DAVID GRAEBER, DEBT: THE FIRST 5,000 YEARS 271–82 (2011).

In Lawrence Lessig's *Code 2.0*, he describes *regulation* as a multiplicity of different kinds of constraints. Laws are only one kind of constraint; the others are the market, social norms, and architecture (in cyberspace, this architecture is code).[107] While formal legal constraints are most easily recognizable as law or regulation, the use of code as law can have as big of an effect on behavior in cyberspace. "The code or software or architecture or protocols set these features, which are selected by code writers. They constrain some behavior by making other behavior possible or impossible. The code embeds certain values or makes certain values impossible."[108]

Lessig uses this understanding of regulation to inform how to approach the question of regulating cyberspace *through* formal laws—how to use laws and code in tandem with each other, since code is also a kind of law. In the case of Bitcoin, Lessig's work is useful in understanding Bitcoin as legal and political (rather than the pure market force a libertarian account might make of it). The code of Bitcoin is law—a monetary or financial law. The very code of the Bitcoin protocol is analogous to Article I, Sec. 8, cl. 5 and 6 of the Constitution, to legal tender laws, to the Federal Reserve Act, to Glass-Steagall, to any number of laws that have created, enhanced, or regulated monetary policy in the United States.

The protocol sets the terms of who creates the currency (any one), how the currency shall be recognized (through the public ledger of the blockchain), who shall transact with whom (anyone, as long as the ledger says they have what they say they have), how to deal with those who are attempting to falsify the ledger (ignore them, steamroll past them), and how often more money will be added to the economy (a steady trickle that runs out in 2030).

[107] LAWRENCE LESSIG, CODE V2 123 (2006).
[108] *Id.* at 125.

There is no threat of violence that stands behind this law—perhaps that is the only thing that makes it un-lawlike. But this decentralized system handles the dishonest and the fraudulent (that is, those, that attempt to commit fraud on Bitcoin itself, rather than simply stealing bitcoins from other people: *counterfeiters*, to be distinguished from mere thieves) without the threat of force, simply by exposing the sum of all transactional activity to the entire peer to peer network. As Satoshi writes in his white paper—as long as there are more honest nodes than dishonest nodes, the dishonest ones are suppressed and Bitcoin remains whole.

But as mentioned earlier, much of this coded monetary policy has led to deflation and volatility in the currency, which hinders its long-term viability. Other issues, covered in Bitter to Better, include the possibility of the Doomsday Attack (in which, through technological means, dishonest nodes outnumber the honest nodes), various malware vulnerabilities, and general problems with anonymity.[109] These are all serious vulnerabilities, but can be addressed. The coded law which governs this money can be changed. Obviously, this cannot be through a central sovereign government, but Bitcoin is not without patches, remedies, and mechanisms through which a subtle evolution might be effected.

2. Community Decision-making

One might ask, how can we address problems within a decentralized, anarchic system?

Firstly, Bitcoin is not particularly decentralized. As described earlier, Bitcoin is already de facto centralized through patterns of commerce and use. The clusters of financial activity around the exchanges often result in high profile hacks and thefts. Possibly in response to the hack and subsequent closure of major exchange site BitFloor in September 2012, the Bitcoin Foundation, chaired by Peter Vessenes, came into being. In a letter of intent, Vessenes wrote,

[109] Simon Barber, Xavier Boyen, Elain Shi, & Erin Uzun, *Bitter to Better – How to Make Bitcoin a Better Currency*. http://crypto.stanford.edu/~xb/fc12/bitcoin.pdf

"the Bitcoin Foundation will be the organization that focuses and unlocks all of your energy and talents towards promoting Bitcoins, protecting them, and increasing their legitimacy through standardization."[110] The creation of the Foundation was somewhat of a coup d'état: prior to its formation, there was neither any such entity, nor any way for the community to decide to create one. In essence, by bringing Gavin Andresen on board—the developer who took over the project after Satoshi Nakamoto—the Foundation was able to seize control of the code. This coup was legitimized by the names listed on the Board: Mark Karpeles (the CEO of Mt. Gox), Charlie Shrem (CEO of BitInstant), Peter Vessenes (the founder of CoinLab), Jon Matonis (an editor of Bitcoin Magazine).[111] Vessenes has also states that Satoshi Nakamoto is a founding member of the Foundation.[112]

As one might imagine, the libertarian base of Bitcoin users have not wholly embraced the Foundation. On the whole, responses to the Foundation's formation were, at the time of the announcement, "supportive or at least optimistic," perhaps viewing the Foundation as more of an outward figurehead than a real central agency ("Seems like a good idea to have a foundation so that the public image of Bitcoin isn't just a bunch of drug dealers and money launderers"). [113] However, one wrote, "This feels like the beginning of the end to me. A good ol' boys club where only the Bitcoin rich get influence." This anti-Foundation sentiment was repeated again upon the

[110] Peter Vessenes, Bitcoin Foundation Letter of Intent, https://bitcoinfoundation.org/about/letter.

[111] The conflicts of interest within the Foundation are marked and severe, as evidenced by the recent filing of lawsuit between two prominent members of the Board. Adrian Chen, *Massive Bitcoin Business Partnership Devolves Into $75 Million Lawsuit*, GAWKER, May 2, 2013, http://gawker.com/massive-bitcoin-business-partnership-devolves-into-75-487857656.

[112] Adi Robertson, *Can the Bitcoin Foundation build legitimacy for an outlaw currency?* THE VERGE, Oct. 1, 2012, http://www.theverge.com/2012/10/1/3436984/bitcoin-foundation-legitimacy-and-standardization/in/3709249.

[113] *Id.*

announcement that CoinLab (i.e., Vessenes) was suing Mt. Gox (i.e., Karpeles) for breach of contract.[114]

By retaining and paying developers such as Gavin Andresen a regular salary, the Foundation seems to hold some kind of official influence over how Bitcoin evolves. (As a technical note, the basic protocol does not change, but the client that released on the bitcoin.org website is regularly updated by Andresen et al.). So far this influence has been very hands-off—for example, in response to the BitFloor hack, the Foundation developed an opt-in mechanism that would strengthen security for merchants. This is a far cry from the kind of intervention that would likely be required to address hyperdeflation, but it does not mean it is impossible.

But future changes in the Bitcoin system do not *need* to be implemented through a central agency like the Bitcoin Foundation. There is evidence that community consensus can result in the resolution of crisis. On March 11, 2013, the release of the 0.8 version of the client caused the blockchain to fork, with machines running the 0.7 client refusing to accept the blocks that the 0.8 version was verifying.[115] Two different versions of the ledger were propagating. Without centralized control, the solution to this problem had to be largely voluntaristic. First, the exchanges temporarily suspended all deposits. Gavin Andresen sent out an emergency alert asking miners to revert to 0.7. The solution became to get as many miners to switch back to 0.7 as possible, until the 0.7 chain overtook the 0.8 chain in length, and then became accepted by the remaining machines still running 0.8.

How this crisis was handled is revealing. It is true that the Bitcoin Foundation might be able to influence Andresen, and therefore how the client and additional features are written.

[114] Open Letter to the Bitcoin Foundation: In Light of Recent Events, Peter Vessenes' Position as Executive Director is Surely Now Untenable.
http://www.reddit.com/r/Bitcoin/comments/1dlsnl/open_letter_to_the_bitcoin_foundation_in_light_of/
[115] *Breaking: The Blockchain has Forked*, THE BITCOIN TRADER, Mar. 11, 2013, http://www.thebitcointrader.com/2013/03/breaking-blockchain-has-forked.html.

However, notably, no such undue influence has been observed, and in this particular case, the structure of decision-making seemed to run in the other direction—Andresen made a call, and the members of the Board acted in such a way as to make that call more effective. Andresen's decision could not compel others—either the influential members of the Foundation or smaller users—to do what they do not want. Rather, people saw what was happening, and chose on their own to react according. Exchanges suspended deposits, and those who saw the emergency alert complied. Andresen (and perhaps the Foundation) may have made a decision, but the decision was implemented in a request, not a demand.

In a similar fashion, the community may have to also come to a decision about what to do about the hyperlinks to child porn that have become encoded in the blockchain (similarly to how the first block is encoded with a headline about bailouts and banks).[116] This revelation has been met with hysteria—because of the way Bitcoin works, every peer in the network is broadcasting those links (albeit, in an encoded form). There is—somewhat reasonable fear—that this will constitute distribution or transport of child pornography.[117] Unlike the fork described above, the removal of these links would be a serious endeavor, since the blockchain is meant to be a permanent ledger of transactions. It is unclear whether this issue is possible to address at all within the current framework.

Much, much further in the distance is the inevitable point at which Bitcoin succumbs to the "cryptosystem time bomb."[118] The protocol currently relies on the cryptographic hash function SHA-256; but "all cryptosystems eventually become obsolete." When SHA-256 breaks,

[116] Steve Hargreaves & Stacy Cowley, *How porn links and Ben Bernanke snuck into Bitcoin's code*, CNN MONEY, May 2, 2013, http://money.cnn.com/2013/05/02/technology/security/bitcoin-porn.

[117] There is some caselaw from a military court that indicates that a hyperlink is not sufficient to count as distribution. United States v. Navrestad, 66 M.J. 262 (C.A.A.F. 2008), *available at* http://pub.bna.com/eclr/070199_051408.pdf.

[118] Edward Z. Yang, *Bitcoin is not Decentralized*, INSIDE 233, Jun. 1, 2011, http://blog.ezyang.com/2011/06/bitcoin-is-not-decentralized/.

whoever has the "solution" will be able to write blocks faster than those who do not, forcing the others to accept their version of the ledger, even though they are repeatedly rewriting it so that they can doublespend their money. There are two solutions to this distant problem: one is a decentralized transition in which all existing bitcoins become worthless, and a new cryptocurrency substantially similar to Bitcoin but based on a different cryptographic hash function takes its place. The centralized plan would involve creating a new protocol when concern for the time bomb becomes high enough. "This protocol will not only include a new hashing algorithm, but also be based off of the value of the old Bitcoin economy at some date: at that point, all newer transactions are invalid in the new Bitcoin scheme, and that snapshot is used to determine the amount of Bitcoins everyone has."[119] This would be a centralized scheme analogous to sovereigns recalling their currency and reminting it.

Serious proposals for changes and alternative implementations of Bitcoin have been circulating since 2011, including proposals by a group of researchers from Palo Alto Research Center and UC Berkeley[120] and a proposal from software engineer and former cypherpunk Ben Laurie.[121] (Laurie's proposal in particular seeks to eliminate the pure decentralized aspect of Bitcoin due to the inefficiency in power consumption it creates through the proof-of-work, but maintain its distributed nature by spreading the network over nodes he calls "mintettes"—miniature mints.)

My point in summarizing these events, eventualities, and alternative proposals is that there are decisions that must (and can) be made, and increased centralization that may need to occur. The Bitcoin community is still striking a cautious balance between more centralization

[119] *Id.*

[120] Barber, et al., *supra* note 109.

[121] Ben Laurie, *Decentralised Currencies Are Probably Impossible But Let's At Least Make Them Efficient*, Jul. 5, 2011, http://www.links.org/files/decentralised-currencies.pdf.; Ben Laurie, *An Efficient Distributed Currency*, Jul. 23, 2011, http://www.links.org/files/distributed-currency.pdf.

(e.g., the Foundation) and anarchy, but this does not mean lawlessness. Theoretically speaking, monetary policy can be changed and implemented, coin can be recalled and reminted. The law of Bitcoin is a mix of code, consensus, and oligarchy. These things are central to hold the currency together. Bitcoin is not a blind marker of value influenced solely by the market. To adopt the terminology of Lessig’s *Code 2.0*, the constraints of architecture and social norms also regulate it, allowing for the currency to embody a distributed, ever-shifting push towards political goals.

<u>Conclusion: Anarchists, Libertarians, and Utopia</u>

> *A specter is haunting the modern world, the specter of crypto anarchy.*
>
> Timothy C. May, *The Crypto Anarchist Manifesto*, November 22, 1992

Bitcoin seems futuristic, but when examined in the context of the cryptocurrencies that came before it, it appears to be a throwback. Much of it and its rhetoric belong to a time when people still thought that the internet was unregulable, to a time before Facebook and other commercial enterprises began to aggressively deanonymize the internet.

In fact, an anonymous transaction system has been central to the anti-government aspirations of the cypherpunks since the early 1990s. Eric Hughes’s 1993 Cypherpunk Manifesto, in fact, states:

> *Therefore, privacy in an open society requires anonymous transaction systems. Until now, cash has been the primary such system. An anonymous transaction system is not a secret transaction system. An anonymous system empowers individuals to reveal their identity when desired and only when desired; this is the essence of privacy.*

The combination of an anonymous transaction system with an anonymous system for leaking secrets (e.g., Tim May’s fictional Blacknet, or Julian Assange’s very real WikiLeaks) or an anonymous market for assassinations (e.g., Jim Bell’s Assassination Politics) is essential for this kind of radical, anti-government action.

I have, in this paper, been somewhat derisive of the media's fixation on Bitcoin's supposed anonymity. As I have said earlier, anonymity is *possible* with Bitcoin, but it is not a prominent design feature. But it is understandable why the media—and some Bitcoin advocates—would fixate on anonymity. Cryptography is the constitutive body and soul of Bitcoin, and the populist political project of cryptography since the 1980s has been one of privacy and anonymity. The persistent linkage of the feature of anonymity with Bitcoin, I think, is not only one of popular misunderstanding, but also cultural baggage from the early cypherpunks and cryptographers. There is nothing about Bitcoin that intrinsically links it to radical anarchist political aspirations: it rides alongside it as epiphenomenal froth, just like the 2.5 Mb of WikiLeaks cables that, at some point, became embedded into the blockchain.[122] The desire for anonymity and the desire for radical action perpetually dog Bitcoin, despite the attempts to make it more "mainstream" and "safe," as with the creation of the Bitcoin Foundation.

The anarchist and libertarian leanings of Bitcoin users fall along all points of the political spectrum. Some might seek violent overthrow of the government (e.g., a Blacknet type of future), others hope to simply decouple money from the Federal Reserve. Still, for others, using Bitcoin represents the creation of an insular community that rebels not through violence but through retreat. The project of anonymity and Bitcoin can be interpreted as one of evasion of the state, similar to the evasive maneuvers of the Tsimety, the "anarchists of northwest Madagascar."[123]

[122] *2.5Mb of Wikileaks Cables Embedded in the Bitcoin Blockchain*, THE BITCOIN TRADER, Apr. 23, 2013, http://www.thebitcointrader.com/2013/04/25mb-of-wikileaks-cables-embedded-in.html.

[123] DAVID GRAEBER, FRAGMENTS OF AN ANARCHIST ANTHROPOLOGY 55 (2004). Long-time resistors of the authority of Malagasy kings, the Tsimihety refused to acknowledge the authority of French colonizers—though, not through violent resistance. Graeber writes: "To this day, they have maintained a reputation as masters of evasion: under the French, administrators would complain that they could send delegations to arrange for labor to build a road near a Tsimihety village, negotiate the terms with apparently cooperative elders, and return with the equipment a week

Where Bitcoin goes and what it becomes largely depends on what kind of political inclinations win out in the community. If one is satisfied with Bitcoin becoming a mere transaction system, a new PayPal, then the rise of the exchanges and the current hyperdeflation is not as big of a concern. But those who see Bitcoin as intrinsic to anonymous political speech have a vested interest in limiting the power of the exchanges (who retain data key to potential government prosecution and persecution). This may involve solving the volatility issue with price-stabilizing mechanisms, to bring Bitcoin out of the shadow of sovereign currency. For those who use Bitcoin as for purposes of cultural identity—e.g., Brewster Kahle[124]—that particular development will be most important of all. And finally, resistance or acceptance of regulation by sovereign governments like the United States depends largely on one's political leanings.

Bitcoin, which begins with a quasi-metallist faith in the undilutability of its code, is still intrinsically political: governed by the informal legality of code and social norms, and with usage often aimed towards political purposes. Bitcoin is an anarchic constitutional project. Though no state is being built through sovereign fiscal activity, Bitcoin's retreat from the state, and occasional outright opposition to the state, is itself political.

later only to discover the village entirely abandoned—every single inhabitant had moved in with some relative in another part of the country."

[124] Indeed, Kahle has as much said that he hopes that Bitcoin will "go into circulation not just be converted to USD." Kashmir Hill, *Living on Bitcoin For a Week: The Bitcoin Diet, Day 3*, Forbes.com, May 3, 2013, http://www.forbes.com/sites/kashmirhill/2013/05/03/living-on-bitcoin-for-a-week-the-bitcoin-diet/.