Title
"When perhaps the real problem is money itself!": the practical materiality of Bitcoin

Journal
Social Semiotics, 23(2)

ISSN
1035-0330

Authors
Maurer, Bill
Nelms, Taylor C
Swartz, Lana

Publication Date
2013-04-01

DOI
10.1080/10350330.2013.777594

Peer reviewed

Social Semiotics, 2013
Vol. 23, No. 2, 261–277, http://dx.doi.org/10.1080/10350330.2013.777594

Routledge
Taylor & Francis Group

"When perhaps the real problem is money itself!": the practical materiality of Bitcoin

Bill Maurer[a]*, Taylor C. Nelms[a], and Lana Swartz[b]

[a]*Department of Anthropology, University of California, Irvine, CA, USA;* [b]*Annenberg School for Communication and Journalism, University of Southern California, Los Angeles, CA, USA*

(*Received XX XXX XXXX; final version received XX XXX XXXX*)

This paper investigates the semiotics of Bitcoin, an electronic cash system that uses decentralized networking to enable irreversible payments. For enthusiasts, Bitcoin provides an alternative to currencies and payment systems that are seen to threaten users' privacy, limit personal liberty, and undermine the value of money through state and corporate oversight. Bitcoin's promise lies in its apparent capacity to resolve these concerns not through regulatory institutions or interpersonal trust, but through its cryptographic protocols. We characterize this semiotics as a "practical materialism" and suggest it replays debates about privacy, labor, and value.

Keywords: money; cryptography; payment; labor; privacy; value

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

And so called "investment" and attempted control
May soon spiral fiat into a death roll [. . .].[1]

In early 2009, someone using the pseudonym Satoshi Nakamoto[2] announced on a cryptography listserv the release of a new open-source online currency system, which he (or she) called Bitcoin. Nakamoto emphasized that the currency, founded on a peer-to-peer (P2P) system that connects holders of the currency directly with one another rather than through a third party, would be "completely decentralized with no server or central authority."[3] By late 2009, a second version, updated by numerous individuals, was released. Throughout 2010 and 2011, excitement mounted about Bitcoin's potential to provide a payment channel that eludes the oversight and

*Corresponding author. Email: wmmaurer@uci.edu
Authors are listed in alphabetical order. All made coequal contributions to the research and writing of this piece.

interference of banks, centralized payment systems, and governments.[4] Internet forums, currency exchange websites, marketplaces, and experimental applications for Bitcoin were created by dedicated aficionados and interested newcomers. Bitcoin experienced what resembled to some a speculative bubble of both value and attention. But for its adherents, Bitcoin presents an alternative to a world where online payments have to pass through companies like PayPal, where government agencies are able to surveil one's commercial dealings and potentially impede transactions they deem objectionable, and where government officials and financial actors collude to manipulate the value of money.

Bitcoin's design appeals to diverse constituencies. It fascinates some as an intricately designed decentralized digital network and example of "free software." It taps into continuing unrest over the current financial crisis. It speaks to concerns about surveillance by payment intermediaries, who, like social networks, have begun to see consumer activity as a source of valuable, even monetizable, data. A fair number of Bitcoin enthusiasts espouse some combination of monetarist economic views and libertarian politics, finding in Bitcoin parallels to the gold standard or even a challenge to the US dollar, fiat currency, and fractional reserve banking. In the world of Bitcoin, there are goldbugs, hippies, anarchists, cyberpunks, cryptographers, payment systems experts, currency activists, commodity traders, and the curious.

This paper taps into this group's huge archive of conversations and those that they provoke in other venues. What proves crucial in our view about the semiotics of Bitcoin is the embracement of a monetary pragmatics: Bitcoin enthusiasts make the move from discourse to practice in their insistence that privacy, labor, and value are "built into" the currency's networked protocols. This semiotics replays debates not just about privacy and individual liberty, but about the nature of money, as a material commodity or chain of credits.[5] At the same time, Bitcoin brings matter back into the picture, and vitally so: in the code and in the computer "rigs" with which coins are "mined." These other materialisms – the hardware and infrastructures (often connected to the government and corporate actors Bitcoin is designed to excise) of apparently immaterial digital information (Blanchette 2011) – are obscured.

We characterize Bitcoin's semiotics as a "practical materialism," which in turn is expressed via a *digital metallism*. We borrow these terms from the theorist of money Geoffrey Ingham's (2004) coinage "practical metallism." Ingham uses this phrase to refer to the discursive work of commodity money theories in "naturalizing the social relations of credit that constitute money." The discursive politics of Bitcoin involves a similar foregrounding of materiality and backgrounding of credit relations. Despite the supposed immateriality of digital bits of information (Blanchette 2011), matter itself is very much at issue with Bitcoin, both in how it is conceptualized and in how individual Bitcoins are "mined."

This practical materialism involves a potent discursive investment by Bitcoin users in the determinist mechanics of Bitcoin's code: first, its apparent "privatization"[6] of the identities of those transacting Bitcoins (through network decentralization and cryptography); and second, its "digital metallism," the supposed grounding of value, inspired by gold standard economics, through algorithmic control of the money supply. Yet the social dynamics of community and trust – evident in the prose

and poetry produced by Bitcoin users – can still be heard through this practical materialism.

We should note that we write as Bitcoin agnostics, as observers of other forms of experimentation with and on money (Maurer 2011). Bitcoin is meaningful and valuable not so much as an actual complementary or alternative currency, but instead as an index of much broader discussions over the nature of money, credit and capital in the world today. The monetary value of Bitcoin rests as much in the future potential that its users imagine for it as on its current, relatively limited capacity to act as a medium of exchange. Similarly, its semiotic value grows out of the aspirations of Bitcoin adherents. The point is not whether Bitcoin "works" as a currency, but what it promises: solidity, materiality, stability, anonymity, and, strangely, community. Indeed, in its endeavor to cut out intermediaries with the capacity to direct or limit the flow of funds among users and instead build a networked world of individual nodes able to exchange directly and "freely" with one another, Bitcoin combines a practical materialism with a politics of community and trust that puts the code front and center. Insofar as Bitcoin's promises – of materiality, privacy, and community – are the stuff of credit, as we suggest below, Bitcoin provides a useful reflection on the sociality of money, despite its embedding of that sociality of trust in its code itself. In this world, there is no final settlement – as with a state demanding payment in the form of taxes or tribute – and trust in the code substitutes for the (socially and politically constituted) credibility of persons, institutions, and governments. It is this – not the anonymity or the cryptography or the economics – that makes Bitcoin novel in the long conversation about the nature of money.

The code

> On one cold winter day, a crypto-genius arrived
> With some rock solid code, picked up by the hive
> Audited and improved, then released to the wild
> Bitcoin had been born, Satoshi's brain-child

Bitcoin's code is its backbone; the currency functions on the basis of the trust its community of users have placed in the code – and, as with all free and open-source projects, the trust they place in their collective ability to review, effectively evaluate, and agree as a group to changes to it (Kelty 2008). Bitcoin is not underwritten by state fiat, a central bank, or a payments company, but by a decentralized, peer-to-peer network of computerized nodes generating mathematical codes that secure value stored in one's digital "wallet" and facilitate the exchange of that value between wallets. As an entry on the P2P Foundation website (attributed to Nakamoto) describes:

> It's completely decentralized, with no central server or trusted parties, because everything is based on crypto proof instead of trust. 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 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. We have to trust them with our privacy, trust them not to let identity thieves

> drain our accounts. [. . .] With e-currency based on cryptographic proof, without the need to trust a third party middleman, money can be secure and transactions effortless.[7]

For Bitcoin to work, one does not have to trust Nakamoto, a bank, or any other person or institution. One must simply trust the code – or, more precisely, the cryptographic algorithm.

Central to this algorithm is Nakamoto's solution to what has been called the "double-spending" problem. Cash solves the problem of double spending by virtue of its materiality: counterfeiting aside (although it is an important caveat), one simply cannot give a bill or coin away twice, to two different parties. This unique characteristic of cash – the difficulty of tracing its individual units, its *anonymity* – makes it vulnerable to theft or loss – to the teeth of hungry critters, for instance, or to fire or rain. All such cash transactions are irreversible.[8] The irreversibility and "anonymity" of cash dealings also make cash uniquely useful: to money launderers and others engaged in illegal transactions, undocumented workers, and those who value "the right to privacy" (or, as Warren and Brandeis described it in 1890, "the right to be left alone") who want to carry their money on their persons or simply wish to shield themselves from the intrusions of government. Here, the "anonymity" of the material thing is understood to translate into the anonymity of the bearer.

Unlike with a one hundred dollar bill – the material duplication of which is made difficult by serial numbers and other anti-counterfeiting measures – users of virtual or online currencies may more easily try to spend the same monetary unit more than once. An independent third-party or central clearing house is required to authorize digital transactions. Bitcoin's work-around, embedded in its code, is a decentralized verification system, in which the combined processing power of computers connected to one another over the Bitcoin network is put to use authenticating and recording every Bitcoin transaction. "The result," Nakamoto explains, "is a distributed system with no single point of failure."[9]

What makes Bitcoin different as an online form of payment is how it distributes the work of verifying transactions. Bitcoin transactions are transmitted to every node in the network, creating a database of all approved transactions to date – what one blogger suggests "can be thought of as a giant, shared accounting ledger" (Lee 2011). At certain intervals (about every ten minutes), all of the transactions during the preceding period are bundled together into a "block"; these blocks are then linked to form a chain. Within each block is a cryptographic puzzle, which, when solved, validates the chain as a whole. The puzzle can only be solved through trial and error; the process is dubbed, in recognition of the brute calculating strength needed to crack the code, "forced work." The mathematics of the puzzle ensures that while it is difficult to solve, it is not difficult to verify.[10] In this way, each node connected to the Bitcoin network lends its computing power to the work of authenticating the system's transaction logs, confirming one block at a time that all Bitcoin transactions follow the rules and the system remains counterfeit-free.

The node that succeeds in solving the cryptographic puzzle starts a new block by submitting its "proof of work" to the network. Solving the puzzle is a computationally demanding process, and it becomes more demanding each time, requiring increasing amounts of computing power to decipher. The node in the network that "wins" the race to decode the next block receives as its reward the ability to create a fixed quantity of new Bitcoins for itself. Via this incentive, the algorithm effectively

harnesses the computing power of all the Bitcoin holders to the process of verifying all the Bitcoin transactions in the world.

Materializing privacy

> One day bankers and fascists may look back with scorn
> On the day when the genesis block was born [. . .]
>
> Securing transactions of those who believe
> That middle-men shouldn't be there to receive
> More than a small fee to perform a transaction
> Or invade privacy of those taking the action

When Nakamoto gave the world the first 50 Bitcoins – called the "genesis block" – he also offered a short essay outlining the technical design of Bitcoin (Nakamoto 2008). Nakamoto suggested that he wrote the code after becoming upset by the financial crisis that began in 2007–2008 and governments' reactions to it.[11] Nakamoto's decentralized currency was a response to the crisis and, in particular, to the role of banks in mediating financial transactions. It was also linked into general hostility toward payment intermediaries like PayPal.

For Nakamoto and others, Bitcoin's power was that it could "free people from the tyranny of middlemen: banks; credit-card companies; and money shippers like Western Union, which charge exorbitant fees for performing a rather simple task" (Lyons 2011). The ordinary movement of money from one person's account to that of another had come to seem like a form of involuntary labor, kinetic energy that generated income for these "middlemen," a vibrancy sapped by payment intermediaries. A poster on the Bitcointalk forum described Bitcoin as marking the end of "*flow capitalism*," that is, the profits extracted by those with a "monopoly on transactions" from the "movement of values and not just their storage." With Bitcoin, the "flow" of transactions, instead of generating capital for this "middleman mafia," would generate new Bitcoins for fellow miners. For Bitcoin enthusiasts, the way to avoid exploitation by "flow capitalists" was to support monetary systems controlled not by impotent or corrupt regulators or by private-sector payment intermediaries, but through the "neutrality of a cryptographic authentication."[12]

Bitcoin promised not only to keep "middlemen" from profiting from transaction fees, but also from "invading" transactors' privacy (or allowing government entities to do the same). Many fear, for instance, that payment intermediaries have turned their users into laborers by transforming their activity into data. Indeed, the content of transaction activity has also become a site of value production for payment intermediaries, able to be used, for instance, along with more traditional indicators like credit score and income, to assess risk and assist in collections.[13] As Scholz (2008) explains, the user-centric ideology of Web 2.0 business models means that "the Web makes people easier to use. By 'surfing' it, people serve their virtual hosts and they are not unhappy about it." Bitcoin "mining" – participation in the transaction-verification process – is seen as providing an antidote to monetized surveillance via data mining of individuals' transactions across payment platforms.

Interestingly, Bitcoin emerged during a period of increased frustration with the failure of a surveillance application intended to benefit users: fraud protection. PayPal, the current leader in online payments, came under fire in the late 2000s for

excessive false positives in their fraud detection system and confusing policies that were harshly and inconsistently enforced. The movement against PayPal has become a flashpoint for those unhappy with these payment systems "middlemen."

This monitoring can also have an overtly political dimension. Kreimer (2006) describes the potential for Internet intermediaries to be used as proxy censors, recounting how Internet service providers and domain hosts have been successfully pressured by both state and private actors to deny service to entities accused – though not necessarily charged with or found liable for – illegal activity, from copyright infringement to terrorism and child pornography. Kreimer points out that payment intermediaries can effectively shutdown an organization by refusing transfer of funds to it. Indeed, at the height of the international firestorm in 2010 over its release of thousands of documents, Wikileaks' data-storage account was canceled, its domain-name service provider refused it service, and the accounts of those accepting donations were frozen by PayPal and other payment systems.[14] The backlash was swift; *Time Magazine* blogger Jerry Brito (2011) noted that payment intermediaries had become "choke points":

> Whether or not payment processors ought to be telling us how to spend our money online, the fact is they can. We rely on third parties to transact online, and when government wants to restrict how we can spend money online, it's these intermediaries they turn to. [. . .] To transact online, you have to have an account with a third party like PayPal that you trust will follow your payment instructions.

The promise of Bitcoin is that it appears to provide a means of exchange free from the oversight of private payment intermediaries and their unpredictable fraud detection algorithms and potential to collude with state actors. Brito, echoing other Bitcoin proponents, wrote:

> Want to contribute to WikiLeaks or some other politically unpopular organization? No problem. Live under a repressive regime and want to buy a repressed book or movie? Here's how.

Bitcoin soon became WikiLeaks' preferred donation mechanism. For Brito and others, Bitcoin began to seem like "a censorship-resistant digital currency," an ideal payment mechanism for "law-abiding citizens" who wanted to "carry on their affairs without anyone snooping on them or telling them what they can and cannot do."[15]

Perhaps for this same reason, Bitcoin was also reported to have attracted those hoping to buy illegal goods and services online. This proved to be a popular, if sensationalist, angle for Bitcoin press coverage. Through articles like Adrian Chen's (2011) unsubtly-titled "The Underground Website Where You Can Buy Any Drug Imaginable," Bitcoin became associated with the website Silk Road, a "digital black market" accessible only through the anonymized browsing service. Bitcoins, the article explained, were the "online equivalent of a brown paper bag of cash [. . .] championed by cyberpunks, libertarians and anarchists who dream of a distributed digital economy outside the law, one where money flows across borders as free as bits."

The comparison to cash is a common one. Brito explains: "There's been no such thing as 'online cash,' no currency that could be exchanged untraceably between two persons without a third party intermediary – no such thing, that is, until now." As

with the materiality of cash, certain privacy protections are "hardwired" into Bitcoin's code. Once you spend them, for instance, Bitcoins are gone; there's no chargeback possibility, as with other payment channels. It is telling that in the title of his original paper, Nakamoto (2008) called Bitcoin a "peer-to-peer electronic cash system." Like cash, of course, Bitcoin's apparent untraceability makes it vulnerable to theft, as one user found out in dramatic fashion, posting to a Bitcoin forum in June 2011 that 25,000 Bitcoins – worth at that time some $500,000 – had been transferred from her/his account to that of another user. The transaction was fully visible in the public log, available for anyone to review.[16] But the damage had been done; no one knew who the perpetrator might be.

What is often lost in the alternately utopian and sensationalist coverage of Bitcoin, as in such comparisons to cash, is that its protocols offer not anonymity, but "pseudo-anonymity." In the design paper, Nakamoto proposed a "new privacy model," in which identities, but not transactions, are shielded from public view (see Figure 1). Bitcoin transactions are recorded in a public log, but the anonymity of all the parties is secured using public-key encryption, a common technique for online commerce. As Jeff Garzik, identified as a member of the "Bitcoin core development team," explains, "You're looking at a global public transaction register [. . .] You can trace the history of every single Bitcoin through that log, from its creation through every transaction" (Simonite 2011).[17] Garzik suggests that such a database provides a deterrent against money laundering, but it also means that law enforcement could use network analysis to track down users. In response to Chen's piece, Garzik was blunt: "Attempting major illicit transactions with bitcoin, given existing statistical analysis techniques deployed in the field by law enforcement, is pretty damned dumb."

Furthermore, Bitcoin users continue to struggle to be completely untethered from payment "middlemen." There are a few ways to get Bitcoins: mine them yourself, accept them as payment, or exchange them for traditional currency. The final method might seem the most simple. But how can it be accomplished without compromising privacy? Websites like tradebitcoin.com provide the locations of Bitcoin traders so that users can set up cash-to-Bitcoin exchanges in person or via the mail. These options may not be practical on a regular basis. Moreover, relying on the postal service reconnects the Bitcoin user to a public infrastructure, maintained by an intermediary (the government) that, once again, could potentially exercise control over that channel. Bitcoin traders thus need a way to accept easy, low-cost payments of national currency that are aligned with their own sense of privacy and the morality of money. In this sense, Bitcoin represents a response not only to money but also to payment, to transforming the vibrancy of payments into fees for intermediaries, and

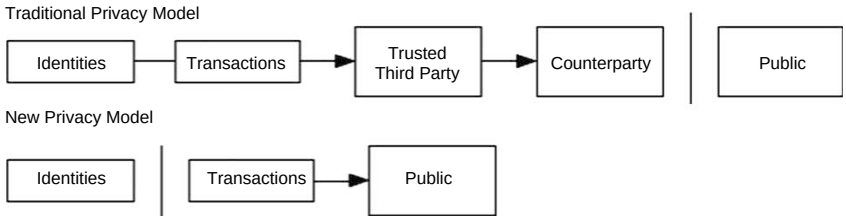

Figure 1. Contrasting models of privacy for electronic transactions. From Nakamoto (2008).

to the privacy implications of the control such intermediaries exercise over payment channels.

Oddly enough, perhaps the most common solution has been to turn to third-party payment providers, albeit those – like the Des Moines-based company Dwolla – that seemingly share the commitments of Bitcoin enthusiasts to privacy and minimal interference. And yet, many of these companies, including Dwolla, use the Federal Reserve-run Automated Clearing House (ACH) system to transfer payments and settle debts between users. Moreover, as the number of Bitcoins released by the algorithm declines and eventually slows to a halt, miners, those who ensure the soundness of the network, would receive compensation through "transaction fees."[18] In other words, miners would become much more like regulators or payment intermediaries.

Despite these complications, Bitcoin's privacy model remains attractive to many. And, again like cash, Bitcoin reassures in part because of its practical materialism: the privacy that Bitcoin ostensibly provides its users is inherent to the currency itself, built into its code. The possibility of surveillance by outside parties is complicated, if not (according to some users) eliminated, by the decentralization of the network itself. If the primary appeal of Bitcoin's privacy model is that the distributed network obviates intermediaries, then that appeal is founded on the trust of users in the code and the network, the fact that such decentralization, as well as the public-key encryption of users' identities, is hardwired into the system.

Materializing value

> [. . .] Like a clock set in motion, with springs that are wound
> By the hackers who joined, mining blocks to be found [. . .]

Bitcoin's practical materialism is not limited to the hardwiring of privacy; it finds another expression in the metaphors that describe the application of processing power to the transaction-verification process and the issue of new Bitcoins as "mining." The process of producing new Bitcoins, *The Economist* (J.P. 2011) suggests, "mimic[s] the extraction of minerals [. . .]. As the most readily available resources are exhausted, the supply dwindles." The "mining" metaphor is a deliberate nod to precious metal-based monetary systems. And like an ideal-typical gold-standard economy, there is a limit to the total amount of currency that will eventually circulate, although in the world of Bitcoins, this limit is already known. Over time, fewer and fewer Bitcoins can be produced by solving a block.[19] There will never be more than just under 21 million in existence, a kind of asymptotic upper bound. Built into the code, into the ever more processor-intensive calculations needed to "mine" new Bitcoins, is this ceiling.

This "digital metallism" is one of the most striking semiotic and financial features of Bitcoin. The imagery extends throughout the online Bitcoin universe. Bitcoin's software is called the "Bitcoin miner," as are those users who invest in expensive "rigs," with muscular hard drives and high-end video cards, whose processing power can be channeled into the work of solving Bitcoin's mathematical puzzles.[20] A website providing introductory information about Bitcoins, weusecoins.com, illustrates the production of new Bitcoins with animations of a pick-axe chipping at increasingly larger chunks of semi-transparent rock, eventually freeing a

Bitcoin, represented as an actual golden-colored coin with the Bitcoin symbol inscribed on its surface. In an ironic twist, several entrepreneurs have begun advertising the sale of metal tokens, brass and silver and gold, with real Bitcoin digital codes embedded inside.[21]

Just as the discourse about privacy draws on understandings about the anonymity of cash, Bitcoin's digital metallism parallels very old discourses about the "soundness" of "commodity money" – that is, currency deriving its value from the material out of which it is made. In eighteenth-century England, for instance, a debate that began over the best way to respond to the practice of clipping snippets of metal from coins transformed into an argument about whether the value of money derived from its metallic content or from state law. While some like Nicholas Barbon argued that "tis the Publik Authority upon the Metal that makes it money" (in Appleby 1976, 63), the philosopher John Locke staked out a famous position in which he denied "that money was a creature of politics," and insisted instead that the value of money lay in the universal, imaginary value human beings "consented" to bestow upon the precious metals. Value was intrinsic to money itself. Locke's metallism is linked, moreover, to his political liberalism: the very idea that money could be placed under the control of the sovereign infringes on the liberty of human beings. Money, according to Locke, operates independently of state authority, free from the arbitrary power of government.

Other parties to the eighteenth-century debates worried over the increasingly common practice of circulating bills of exchange as a form of currency. These promises were no better than the people who made them. And, in endorsing a note over to another, promises could be piled on promises to the point where value seemingly inhered only in the social commitments of each to all. Daniel Defoe's "Essay Upon Publick Credit," while expressing concerns about the speculation bills of exchange might foment, as well as their potential to corrupt public officials, still finds a way to ensure the soundness of paper money. Rather than rely on the reputations of those making promises, which can be inflated and unwarranted, Defoe emphasized honesty – particularly, the honesty of account books – to underwrite value and, ultimately, society itself (Sherman 1996). As J.G.A. Pocock (1985, 113) puts it, Defoe argued that "men should behave in such ways as to give one another good grounds for believing that promises would be performed and expectations fulfilled." The trust engendered by promises kept, according to Defoe, provides the foundation of the social world.[22]

This basic debate – over whether money is a "creature" of law or promises, or of its own "intrinsic" properties – is one that recurs throughout the intellectual history of money. It reappears in the postbellum USA in the political struggles between "greenbackers" and "bullionists" over whether fiat paper money could replace gold and silver currency (Carruthers and Babb 1996). And it has cropped up again today in the repopularization of the gold standard and, more narrowly, in Bitcoin's digital metallism. At the same time as Bitcoin rematerializes money – and as the material infrastructures and effects of Bitcoin mining became apparent to Bitcoin adherents – it also evokes earlier credit theories of money, especially in its users' outpouring of discourse – the sheer volume of talk – which parallels the honest accounting of credit and credibilities suggested by Defoe. It does so, however, with one important difference: Bitcoin embeds this accounting *in the code itself* and entrusts honesty to the algorithmic verification of Bitcoin transactions. The "proof of work" is

undertaken not by humans issuing bills of exchange, but by the algorithm. In this sense, the emphasis on Bitcoin's code – and specifically, its public transaction log – parallels Defoe's emphasis on account books: both are nonhuman, but deeply social technologies meant to ensure trust and thus value.

The comparison between Bitcoin and gold was one that Nakamoto himself made: "The steady addition of a constant of amount of new coins is analogous to gold miners expending resources to add gold to circulation" (Nakamoto 2008, 4). Nakamoto's purpose in drawing this parallel is more than illustrative. According to many Bitcoin proponents, the metallist metaphor captures an important truth about the economics of Bitcoin, specifically, the fact that there will be an absolute limit to the number of Bitcoins in circulation. The idea is that by hardwiring the *quantity* of money into the code, Bitcoin can avoid inflation or currency devaluation, such as that precipitated by a central bank's quantitative easing. The Bitcoin–gold parallel is thus also connected to a monetarism in the vein of Milton Friedman's quantity theory of money and, more generally, opposition to government control of the money supply.[23] Thus, Brito (2011) writes in favor of Bitcoin:

> For one thing, artificial currency inflation is impossible. In most countries, a central bank controls the money supply, and sometimes (such as during the recent economic crisis) it may decide to inject more money into an economy. A central bank does this essentially by printing more money. More cash in the system, however, means that the cash you already hold will be worth less. By contrast, because Bitcoin has no central authority, no one can decide to increase the money supply. The rate of new bitcoins introduced to the system is based on a public algorithm and therefore perfectly predictable.

Not only is the rate of creation of new Bitcoins predictable but also part of the attraction, and the very reason for its predictability is that changes in the rate itself are automatic, hardwired into the system itself and not subject to alteration by any individual human.[24] Indeed, the graph of Bitcoin emission over time has become a popular way to broadcast such sentiments; the slow, rounded curve, approaching 21 million but never quite reaching it, suggests the certainty and determinateness of Bitcoin's economics (see Figure 2). Like advocates of the gold standard, many Bitcoin enthusiasts find such certainty comforting. It takes the decision-making power out of the hands of potentially corruptible, inept, or self-interested policy-makers (or, echoing Locke, because it reflects deeply held principles about the independence of human beings from government). Hence another reason why the process of generating new Bitcoins is called "mining" and not "minting": In Nakamoto's design paper, "minting" is associated with a central authority like the Federal Reserve.

In detecting in Bitcoin an economic argument about the money supply, inflation, government, and the inherency of value, enthusiasts again trace the outlines of a practical materialism, in which the meaning of Bitcoin can be found hardwired into its code. That which makes Bitcoin meaningful – that is, its value – is specifically that which is intrinsic to it. The max cap on the supply of Bitcoins is understood to be built into Bitcoin, and so, therefore, is the economics of sound and stable money. The comparison to gold, Bitcoin's digital metallism, is an expression of this practical materialism (not necessarily its source).

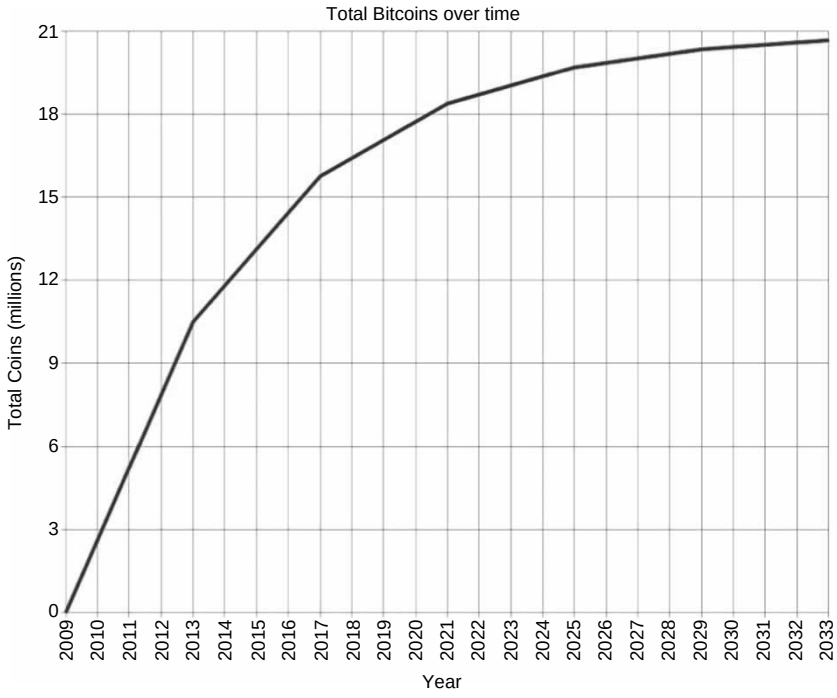

Figure 2. The total emission of Bitcoins, graphed by year from 2009 to 2033. From (https://en.bitcoin.it/wiki/File:Total_bitcoins_over_time_graph.png).

Laboring, electricity, and the infrastructures of mining

There is a final component of Bitcoin's practical materialism: the trope of labor that tracks the parallel between Bitcoin mining and gold standard economics. The issue of new Bitcoins does not happen on its own, even if the rate of emission is automatic, determined by the code. It requires, as Nakamoto (2008, 4) puts it, the "expending of resources." Only, "[i]n our case, it is CPU time and electricity that is expended," not the human labor power of miners. Here is where the immateriality of digital money is turned on its head.

As the difficulty of solving the mathematic puzzles embedded in Bitcoin's block chains has increased, so too has the processing power needed to mine successfully. Bitcoin mining rigs were, by late 2011, often operations with expensive and powerful processors and video cards dedicated wholly to mining. Davis (2011) describes the mining rig of Kentucky farmer and laptop repairman Kevin Groce as a wall in his uncles' business "lined with four-foot-tall homemade computers," all tangled wires and blinking lights. The computers, which cost $4000, give off so much heat that Groce's uncle, who offered to invest $30,000 in the mining operation, predicted that "they'll heat the whole building this winter." These arrangements echo the "work" suggested by the "proof of work" and "forced work" concepts in cryptography. Groce compares Bitcoin mining to "moon shining" and livestock care: "I grew up milking cows. [. . .] Now I'm just milking these things." There is, it turns out, labor involved in Bitcoin mining, both human and computer.

By the summer of 2011, Bitcoin mining began to seem like a developed industry. Miners determined that using a computer's graphics processing unit (GPU) rather than its central processing unit (CPU) was more computationally efficient. The Bitcoin Wiki compares a CPU to an "executive," "making decisions" and agilely switching between tasks. A GPU, in contrast, is seen as a "laborer," able to do "a lot of repetitive work" and large quantities of "bulky mathematical labor."[25] Miners unable to invest the significant capital required to keep up with increasing computing demands banded together to form "mining pools," each participating in the generation of a block and receiving in return a portion of the new Bitcoins.[26] Others began renting their rigs out to potential Bitcoin prospectors.[27] At least one enterprising miner attempted to recruit unsuspecting Internet surfers through an ad that enjoined them to "Use your video card to make money! Crunch numbers in the background!"[28]

Bitcoin miners also began to express more clearly that there would have to be at least two classes of Bitcoin users: those who mined them and those who "bought" them from the miners using state currency. As one blogger explained to a newcomer in October 2011, because of the cost of electricity, mining was only worth the effort of those who "enjoy economies of scale that aren't obtained by individual owner/operators."[29] In fact, there were some reports that the marginal cost of mining had exceeded the dollar-value of a Bitcoin (Arthur 2011). Bitcoin mining became profitable, if at all, only for those who industrialized it, not for mom-and-pop setups or hobbyists.[30] Indeed, the physical presence of the digital labor necessary to mine Bitcoins successfully is truly intimidating: rigs made of dozens of computer towers, often stacked on metal shelving with box fans providing cooling. The room is not only hot but also loud: the processors hum and vibrate, producing a noisy drone that fills the space, a kind of computerized chatter.

All of this human and nonhuman labor reminds us that alongside and partly hidden by Bitcoin's practical materialism are other materialisms, infrastructures that support the Bitcoin code and the network of Bitcoin users: the postal service and the Federal Reserve-mandated-and-partially-operated ACH network, for instance. But first and foremost among such infrastructures is the electrical grid, on which miners draw, often heavily, to power their rigs and sustain the P2P network. The electricity "expended" in the service of Bitcoin energizes not only the miners' race to generate the next block in the chain but also their interactions with one another, their own chatter in online forums and elsewhere.

What is the value of a Bitcoin? Trusting the code

> As elected officials looked dumber and dumber
> Others started to put their faith into numbers . . .

Within this comparative nexus – in which the "work" of mining Bitcoins corresponds to the labor of mining precious metals from the ground – Bitcoin can appear not only as a currency but also as a "commodity." Some argue, for instance, that perhaps the best way to understand the value of Bitcoin is not as a medium of exchange (there is still precious little you can buy with Bitcoins), but as an investment (and a speculative one at that), a part of an investment portfolio, alongside paper currencies and other commodities. In fact, like commodities on the open market,

Bitcoin has been vulnerable to speculation and hoarding in its short history, resulting in sudden, violent swings in its dollar exchange rate.[31]

It is not uncommon in the Bitcoin world to hear utopian (or dystopian) pronouncements that situate Bitcoin as the next step in the evolution of money. (The Kentucky miner Kevin Groce, interviewed by Davis [2011], quips "It's like eight-tracks going to cassettes to CDs and now MP3s.") That evolutionary narrative traces a path from more to less tangible: from barter to precious metals to coin to paper currency and checks to credit cards to purely digital value, "nothing" but strings of numbers and letters flashing across a computer screen. This is, of course, a familiar discourse on money (Desan 2005) and digital information (Blanchette 2011). But the slippage between currency and commodity is indicative of Bitcoin's broader practical materialism – a materialism that emphasizes all that is inherent to the code: the anti-inflationary economics of a hard cap on the money supply and the labor of a community of human miners and nonhuman hardware and software working together to solve cryptographic puzzles. In so doing, this assemblage serves as a distributed regulatory apparatus, constantly ensuring the validity of transactions across the network – and thus both the confidence of its participants and the security of the system as a whole. Attempts to embed Bitcoins in metal or plastic are simply attempts to stabilize and then to hold the effect of that practical materialism – money, rendered Bitcoin – in one's hands.

Within the evolutionary narrative of money, the materialism of Bitcoin seems, on the one hand, to reflect desire for the "soundness" and tangibility of commodity money. This is the immediate effect of Bitcoin's digital metallism – the imagery of mining, the discourses of labor and work, the monetarism – as well as its privacy model, which builds pseudo-anonymity and "protection" from corporate and government intermediaries, into the network. The digital metallism of Bitcoin echoes the materialism of commodity theories of money, such as those championed by Locke, the bullionists of the nineteenth-century, and the gold-standard supporters of today. And, as with Locke, this metallism is also part of a broader materialism linked to an ideology that emphasizes individual liberty and sees "sound" money as a key component of that liberty, as well as a key site for potential government intrusion.

On the other hand, as evidenced by the extraordinary volume of interaction among Bitcoin enthusiasts online, the network of computerized nodes – transacting with one another and contributing to the verification of the public transaction log – is interwoven with another network of social beings who communicate with one another, debate one another, contribute together to changes in the code, and ultimately together place their trust in the Bitcoin code's hardwiring of the very networked protocols that connect them. As Kelty (2008) explains for free software generally, this communication produces a public – and specifically a "recursive public" – in that its participants are explicitly concerned, in practical and moral terms, with the material bases of their association.

Bitcoin is not just semiotically materialist, so to speak, but also all about trust – about eliminating the need to trust governments and corporations and about learning to trust the Bitcoin algorithm instead. Bitcoin enthusiasts express this trust discursively in terms of what we have called practical materialism. A payments industry CEO, for instance, writes that:

> Bitcoin is backed [. . .] by the trust of the "network nodes" that is materialized in the aggregate computing power of this group of people. [. . .] Bitcoin proof of work protocol avoids the need for a secure web of trust, relying instead on the assumption that a majority of the computing power is in the hands of honest participants: "honest" here simply means that they will cooperate to make the network confirm legitimate transactions. (Noizat 2012)

And yet, trust in the code does not erase entirely the community that bestows it; Gavin Andresen, a lead Bitcoin programmer, explains that the decentralization coded by the Bitcoin program is "more comforting than thinking that politicians or central bankers won't screw it up. I actually trust the wisdom of the crowds more." (Goldstein and Kastenbaum 2011).

This distributed network of shared trust in the code – and, via the code, in a chain of relationships between nodes in the network – resembles not so much commodity money theories, in which the value of money derives from the stuff from which it is made, but credit theories of money. The investment of Bitcoin enthusiasts in their own liberty and privacy could be read as concern for personal credibility, although also, perhaps, an inversion of it: instead of establishing one's reputation by extending oneself via one's relations with others – issuing promises, circulating credit and credibility, and relying on the honesty and honest books of everyone in a market – one preserves oneself, cutting off all flows of information about oneself. And, moreover, it is the code that does this work of disconnection and silencing.

Inside the operations of the Bitcoin code lies a sociality of trust that is alternately expressed and obscured by a practical materialism with two components: concerns about privacy and concerns about value. Bitcoin's practical materialism allows the chatter in the code, the proof of work, the materiality of the machines humming and whirring in mining rigs to be simultaneously backgrounded and foregrounded. This is not simply commodity fetishism. The code and the labor are backgrounded when Bitcoin adherents become latter-day goldbugs. But the code and the labor are foregrounded because *they are practically all that Bitcoin enthusiasts ever talk about*. From this perspective, Bitcoin represents a promise like any other money form, but a promise underwritten and backed by an algorithm and its manifestation in a digital peer-to-peer network.

Acknowledgements

For critical commentary on earlier drafts, we would like to thank Jean-Francois Blanchette, Julia Elyachar, Kevin Driscoll, Josh Lauer, Melissa Loudon, Don Patterson, and two Bitcoin miners who would prefer to remain anonymous. We would also like to thank Gretchen Soderlund and our anonymous reviewers for editorial support. Research has been supported by the US National Science Foundation, Law and Social Sciences Program (SES 0960423) and the Intel Science and Technology Center for Social Computing. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation or any other organization.

Notes

1. Throughout this paper we will return to this poem, entitled "An Ode to Satoshi Nakamoto," written by Bitcointalk.org forum user "coretechs" to commemorate the two-year anniversary of the Bitcoin inventor's final post to Bitcointalk. It is reposted here (http://www.thebitcointrader.com/2011/12/ode-to-satoshi-nakamoto.html)

2. Nakamoto's identity – or even whether "he" is a single person – remains unknown. He claimed to be a Japanese male in his mid-30s, but never wrote in Japanese or issued a Bitcoin client for Japan. He used anonymized e-mail, hosting, and other web services and seemed to disappear in 2010.
3. Nakamoto's original post can be found here (http://www.mail-archive.com/cryptography@metzdowd.com/msg10142.html).
4. See the Bitcoin Wiki for a detailed chronology (https://en.bitcoin.it/wiki/History).
5. For more on theories of commodity money and credit money (see Hart 1986; Maurer 2006; Wray 2004).
6. We invoke privatization to indicate both the market sensibilities and the obsession with personal privacy among Bitcoin adherents.
7. Found here (http://p2pfoundation.net/Bitcoin).
8. The irreversibility of cash transaction is in fact supported by the common law tradition. *Miller v. Race* (1758), 1 Burr. 452, 457, 97 E.R. 398, 401 (K.B.).
9. From the P2P Foundation website (http://p2pfoundation.net/Bitcoin).
10. On the technical details of the cryptographic puzzle (see J.P. 2011).
11. Embedded in the code, for instance, was the title of a newspaper article published the same day that Nakamoto made the code public: "The Times 03/Jan/2009 Chancellor on brink of second bailout of banks" (Davis 2011).
12. See here (https://bitcointalk.org/index.php?topic=5671.0).
13. See, for example, Duhigg 2009.
14. For more complete discussion, see Benkler (2011).
15. Of course, a merchant would have to agree to accept Bitcoins for payment just as the merchant would have to agree to accept payments via the card networks; the fact that Bitcoin is open source does not change the character of this agreement except that Bitcoin would not involve a transaction fee. For proponents, Bitcoin's decentralization resists third-party efforts to control who chooses to accept payment via a given payment channel.
16. The original forum thread is here (https://bitcointalk.org/index.php?topic=16457.0). See also Worstall (2011).
17. In this aspect, Bitcoin echoes the work of Keith Hart (2001) on how money can act as a social "memory bank."
18. See here (https://en.bitcoin.it/wiki/Transaction_fees) or here (http://bitcoin.stackexchange.com/questions/876/how-much-will-transaction-fees-eventually-be).
19. For the current number, see here (http://blockexplorer.com/q/totalbc).
20. On mining rigs, see here (https://en.bitcoin.it/wiki/Mining_rig).
21. See, for example, here (https://www.casascius.com/) and "Bitbills," which resemble prepaid debt cards (http://www.bitbills.com/).
22. We are indebted to an unpublished manuscript by Julia Elyachar and Tomaz Mastnak (n.d.) on these eighteenth-century debates and their contemporary relevance.
23. For a cultural analysis of monetarist thinking, see Guyer (2007).
24. It *is* possible to change the code, but it is a political process in which users effectively "vote" for changes in the open-source code by choosing to adopt the new version or not.
25. See here (https://en.bitcoin.it/wiki/Why_a_GPU_mines_faster_than_a_CPU).
26. See here (https://en.bitcoin.it/wiki/Pooled_mining).
27. For example, this Hong Kong-based mining pool also offers mining contracts: http://21bitcoin.com/
28. See here (http://www.geeks3d.com/20110212/compute4cash-use-your-gpu-to-make-money-with-opencl/).
29. See here (http://www.bitcoinminer.com/post/11618474917/ask-anything-new-rig).
30. Indeed, it sometimes proved dangerous: one website collects stories, some apocryphal, from miners about electricity surges, fires, even brain damage. (http://www.bitcoinminingaccidents.com/?page_id=2.)
31. Paul Krugman (2011) and other commentators (e.g., Surowiecki 2011) argue that Bitcoin's value has been determined *not* by the quantity of Bitcoins in circulation but by growing demand on online exchanges like Mt. Gox, where a small number of transactions has made its exchange rate susceptible to such shifts. Many point to a Bitcoin bubble. From a low of about 80 cents to the dollar, the value of a Bitcoin soared to a high of over $30

during the first weeks of June, 2011. Bitcoin's dollar value then dropped drastically after news of a serious robbery, then that Mt. Gox had been hacked, and then that someone had tried to sell off several hundred thousand Bitcoins, dropping the exchange rate from $17 to about one cent (Arthur 2011; Karpeles 2011). By December, the exchange rate had stabilized between $2 and $3/Bitcoin, but then rebounded in late 2011/early 2012 and currently stands between $5 and $6.

Notes on contributors

Bill Maurer is Professor of Anthropology and Law at the University of California, Irvine, where he is also the Director of the Institute for Money, Technology, and Financial Inclusion, and Co-Director of the Intel Science and Technology Center for Social Computing.

Taylor C. Nelms is a Ph.D candidate in Anthropology at the University of California, Irvine and research assistant at the Institute for Money, Technology, and Financial Inclusion.

Lana Swartz is a Ph.D candidate and the Wallis Annenberg Chair in Communication, Technology, and Society Research Fellow at the Annenberg School of Communication and Journalism at the University of Southern California.

References

Appleby, J.O. 1976. Locke, liberalism, and the natural law of money. *Past and Present* 71, no. 1: 43–69.

Arthur, C. 2011. Bitcoin value crashes below cost of production as broader use stutters. *The Guardian*, October 18. http://www.guardian.co.uk/technology/2011/oct/18/bitcoin-value-crash-cryptocurrency.

Benkler, Y. 2011. A free irresponsible press: Wikileaks and the battle over the soul of the networked fourth estate. *Harvard Civil Rights-Civil Liberties Law Review* 46, no. 2: 311–97. Forthcoming.

Blanchette, J.-F. 2011. A material history of bits. *Journal of the American Society for Information Science and Technology* 62, no. 6: 1042–57.

Brito, J. 2011. Online cash Bitcoin could challenge governments. *Techland, Time Magazine*, April 4. http://techland.time.com/2011/04/16/online-cash-bitcoin-could-challenge-governments.

Carruthers, B.G., and S. Babb. 1996. The color of money and the nature of value: greenbacks and gold in postbellum America. *American Journal of Sociology* 101, no. 6: 1556–91.

Chen, A. 2011. The underground website where you can buy any drug imaginable. *Gawker*, June 1. http://gawker.com/5805928/the-underground-website-where-you-can-buy-any-drug-imaginable.

Davis, J. 2011. The crypto-currency. *New Yorker*, October 10.

Desan, C. 2005. The market as a matter of money: Denaturalizing economic currency in American constitutional history. *Law and Social Inquiry* 30, no. 1: 1–60.

Duhigg, C. 2009. What does your credit-card company know about you? *The New York Times Magazine*, May 17. www.nytimes.com/2009/05/17/magazine/17credit-t.html.

Elyachar, J. and T. Mastnak. n.d. 'Beings that have existence only in the minds of men': A look at the sources of thinking about financial speculation and its consequences. University of California, Irvine. Forthcoming.

Goldstein, J., and D. Kastenbaum. 2011. What is Bitcoin? *NPR*, August 24. http://m.npr.org/news/front/138673630.

Guyer, J.I. 2007. Prophecy and the near future: Thoughts on macroeconomic, evangelical, and punctuated times. *American Ethnologist* 34, no. 3: 409–21.

Hart, K. 1986. Heads or tails? Two sides of the coin. *Man (NS)* 21, no. 4: 637–56.

Hart, K. 2001. *Money in an unequal world: Keith Hart and his memory bank*. New York: Texere.

Ingham, G. 2004. The emergence of capitalist credit money. In *Credit and state theory of money*, ed. L. Randall Wray, 173–222. Cheltenham: Edward Elgar.

J.P. 2011. Bits and bob. *The Economist*, June 13. http://www.economist.com/blogs/babbage/2011/06/virtual-currency.

Karpeles, M. 2011. Clarification on Mt. Gox compromised accounts and major Bitcoin sell-off. *Mt. Gox*, June 30. https://mtgox.com/press_release_20110630.html.

Kelty, C. 2008. *Two bits: The cultural significance of free software*. Chapel Hill: Duke University Press.

Kreimer, S.F. 2006. Censorship by proxy: The first amendments, internet intermediaries, and the problem of the weakest link. *University of Pennsylvania Law Review* 155, no. 1: 11–101.

Krugman, P. 2011. Golden cyberfetters. *New York Times*, September 7. http://krugman.blogs.nytimes.com/2011/09/07/golden-cyberfetters.

Lee, T.B. 2011. Bitcoin's collusion problem. *Bottom Up*, April 19. http://timothyblee.com/2011/04/19/bitcoins-collusion-problem/.

Lyons, D. 2011. The web's secret cash. *The Daily Beast*, June 19. http://www.thedailybeast.com/newsweek/2011/06/19/the-web-s-secret-cash.html.

Maurer, B. 2006. The anthropology of money. *Annual Review of Anthropology* 35, no. 1: 15–36.

Maurer, B. 2011. Money nutters. Economic sociology. *The European Electronic Newsletter* 12, no. 3: 5–12.

Nakamoto, S. 2008. Bitcoin: A peer-to-peer electronic cash system. http://bitcoin.org/bitcoin.pdf.

Noizat, P. 2012. Bitcoin: A universal complementary currency? *ParisTech Review*, January 20. http://www.paristechreview.com/2012/01/20/bitcoin-universal-complementary-currency/.

Pocock, J.G.A. 1985. *Virtue, commerce, and history: Essays on political thought and history, chiefly in the eighteenth century*. Cambridge: Cambridge University Press.

Scholz, T. 2008. Market ideology and the myths of web 2.0. *First Monday* 13, no. 3. http://frodo.lib.uic.edu/ojsjournals/index.php/fm/article/view/2138/1945.

Sherman, S. 1996. *Finance and fictionality in the early eighteenth century: Accounting for Defoe*. Cambridge: Cambridge University Press.

Simonite, T. 2011. What Bitcoin is, and why it matters. *Technology Review*, May 25. http://www.technologyreview.com/computing/37619/?p1=A1.

Surowiecki, J. 2011. Cryptocurrency. *Technology Review*. http://www.technologyreview.com/review/425142/cryptocurrency (accessed August 23, 2011).

Warren, S., and L. Brandeis. 1890. The right to privacy. *Harvard Law Review* 4, no. 5. http://www.gutenberg.org/files/37368/37368-h/37368-h.htm.

Worstall, T. 2011. Bitcoin: The first $500,000 theft. *Forbes*, June 17. http://www.forbes.com/sites/timworstall/2011/06/17/bitcoin-the-first-500000-theft/.

Wray, L.R., ed. 2004 *Credit and state theories of money*. Cheltenham: Edward Elgar.