“Bitcoin” and those ‘cryptocurrencies’ derived from it are a public system of electronic ledgers recording payments designed to function like legal tender currency. It was proposed in October 2008, and implemented during the bursting of the housing bubble, starting with its registry as a project on the open source software site Source Forge in November 2008, with the first available software for trading Bitcoins released in January 2009. This initial specification for Bitcoin was written by “Satoshi Nakamoto” as a system of exchange employing a decentralized network—peer-to-peer—where individual transactions do not rely on a bank for their authorization, unlike echecks, credit cards, and other types of electronic funds transfer. Cryptographic currencies (crypto-

---

2 Bitcoin was registered November 9, 2008; the first ‘block’ was released January 3, 2009, the trading software followed on January 11, and the first use of Bitcoin in a transaction occurred on January 12; see https://en.bitcoin.it/wiki/History.
3 “Satoshi Nakamoto” may be a pseudonym; see the Satoshi Nakamoto page of the Bitcoin wiki: https://en.bitcoin.it/wiki/Satoshi_Nakamoto.
currencies) such as Bitcoin are intended to be electronic analogues of physical cash, protecting their users through a combination of strong encryption and shared information about possession—all transactions are recorded publically in a “block” that contains information about who owns all the Bitcoins currently in circulation. Unlike national currencies (legal tender currencies produced by national governments), Bitcoins are strictly limited in both quantity (the total quantity was constrained by the implementation to 2,100,000) and the rate of production (“mining”) by the linkage of new coin production to their use in exchange: new coins are a product of the verification process for the encrypted information that composes every transaction. A major distinction between Bitcoins and fiat currencies produced by national mints is that they exist independently from governmental ability to “print” money, a constraint inherently imposed by the “mining” process itself, making them a “digital commodity” designed for scarcity in the same way that physical commodities such as gold are scarce; this dimension attracted investment by securities traders and stock market speculators in 2011 and 2012.

Bitcoin appears to be a “hacker’s currency” par excellence: it saves the immaterial labor of computers as the Bitcoin, in the process transforming the mechanical procedure that is the foundation of the digital into a material exchangeable for other kinds of production. While the labor involved to produce Bitcoins is immaterial in nature, (it does not involve physical facture, instead employing the semiotic production common to digital technology), it still consumes resources—in the twin forms of the computation performed by the

---

4 See https://en.bitcoin.it/wiki/Bitcoin.
hardware itself and the electricity required to operate it—and only emerges out of specific types of digital processing. Bitcoins are not an autonomously arising product of computational activity, but rather the generated outcome of specific actions. While Bitcoin imitates aspects of the larger internet structure, it is nevertheless a currency, and so addressable in terms of socio-economic structure and significance, quite apart from its technological implication. These ideological implications of Bitcoin become apparent through a contextual situation of it in relation to the larger political economy: unlike historical currencies, Bitcoin, as initially proposed by Nakamoto, enables a perfect form of surveillance over economic transactions, a specific anonymity/privacy issue that the implementation of Bitcoin has attempted to address as Simon Barber, Xavier Boyen, Elaine Shi, and Ersin Uzun observed in their discussion of Bitcoin in Financial Cryptography; various early implementations of the initial Bitcoin specification, such as Bitcoin-Qt or BtCoin, attempt to resolve this problem. (Other popular alternative implementations such as Dogecoin, Maxcoin, etc. are primarily variants supported by financial speculation in cryptocurrencies, rather than technologically distinct attempts to restore the privacy of transactions.) Because all these cryptocurrencies are a developing technology and this issue has not been resolved (as

---


8 While the problems for anonymous transactions are well documented, the Bitcoin wiki claims there is no such issue. See http://en.bitcoinwiki.org/Bitcoin_history.
Barber, et al. noted in their 2012 analysis), the present discussion will focus on the initial proposal from which these implementations are derived. The surveillance (pervasive monitoring) embedded in the specifications for the currency itself integrates the authoritarian dimensions of globalized capitalism—a continuous surveillance and valorization of formerly non-commercial behaviors and relationships—literally into the system of exchange itself.

This foundation for the “Bitcoin” gives the immaterial labor common to the digital a tangible ‘form’—in this case, crystalizing both resources (electricity) and labor expended (computational cycles required to “mine” the coins), in effect, attempting to preserve this immaterial labor in a digitally-derived form that can then be used as a currency, much as commodity-based currencies in the past attempted to preserve labor in an exchangeable form. It is this transformation of immaterial production (semiosis) into Bitcoins that is the essential feature in this case: to extract these Bitcoins requires computational power because the coins are “contained” in mathematical “ore”—equations—that require complex processor-intensive labor to solve, as Simon Barber, Xavier Boyen, Elaine Shi, and Ersin Uzun explain in their technical analysis “Bitter to Better—How to Make Bitcoin a Better Currency,” published in 2012:

the generation of new bitcoins happens in a distributed fashion at a predictable rate: “bitcoin miners” solve computational puzzles to generate new bitcoins, and this process is closely coupled with the verification of previous transactions. At the same time, miners also get to collect optional transaction fees for their effort of vetting said transactions. This gives users clear economic incentives to invest spare computing cycles in the verification of Bitcoin transactions and the generation of new Bitcoins.

[...]

The bitcoin money supply expands as each block created
may contain a special generation transaction (with no explicit input) that pays the block creator a time-dependent amount for the effort (50 coins today, rapidly decreasing). The rate of block, hence money, creation is limited by a proof of work of adaptive difficulty, that strives to maintain a creation rate of one block every 10 minutes across the whole network. Bitcoin transaction verification is thus a lucrative race open to all, but a computationally expensive one.9

The ‘block’ is the complete public listing of all confirmed transactions; every coin, and to whom it belongs, is contained in a block. As new coins are mined, they are added to this chain. The resulting coins are thus a product of that labor indicating that it has been expended in their production. This saving of past labor places these digital products in the same category as any other commodity; their designated function as currency follows from their linkage to the universal foundation of digital production, the immaterial activity of computers, that is reified in a commodity form as/by the Bitcoin.

However, what this currency brings into sharp focus is not the difference between rentier/fiat currencies and those “backed” by a physical commodity, but contemporary attempts to reify digital or immaterial labor of autonomous systems as an emergent equivalent to physical production, as immaterial physicality. Unlike the physical commodity-basis that is the foundation of traditional currencies composed from a precious material (historically gold or silver)—that is simultaneously also a physical commodity in itself and can be employed for both exchange and has a use value in the production of other commodities—there is no use value contained by Bitcoin. This product of immaterial labor cannot be used in the production of other commodities once it has been created (mined)—unlike other immaterial labor products, the only purpose for Bitcoin is to be currency. The Bitcoin, unlike the physical commodity basis of historical currencies,

9 Barber et al., “Bitter to Better,” 400.
has only a currency function—as a commodity it is only valuable as a token of exchange either for other currencies, or through social exchange where it is a token dependent on both parties’ mutual agreement upon its value: this is the same reification of social relationship apparent in fiat currency itself. There is no other function for Bitcoin other than as currency, and consequently its value depends on social convention.

Social relationships are at the foundation of all tokens of exchange, whether based in a produced commodity or in the reification of that relationship (as with fiat currencies). The “transaction history” that is an inherent part of every individual Bitcoin allows the tracking and quantification (reification) of these social relationships as the currency itself. Thus, Bitcoin occupies an intermediate position between the historical physical commodity that functions as universal equivalent for exchange and the purely social reification of fiat currency. What distinguishes fiat currencies from Bitcoin is that Bitcoin is artificially constrained in an *a priori* fashion. Unlike fiat currencies that can be valued at any amount and so are functionally of unlimited value, and historical currency based in a physical commodity where value is limited by scarcity imposed by production, the Bitcoin simulates scarcity in an attempt to produce value. The scarcity of physical commodities is simulated in two ways: (1) the algorithmic nature of their mining which imposes physical constraints on the generation of Bitcoins, and (2) an absolute limit to the total number of coins potentially available (2,100,000). Other than its (artificial) scarcity Bitcoin resembles fiat currencies in its reliance upon a reified social relationship to ensure its value: it is *not* simultaneously both a token of exchange and a commodity in itself.

This foundation in a social relationship is *not* what Satoshi Nakamoto identifies as the “trust based model” in the initial proposal for Bitcoin. Nakamoto’s specification proceeds from a discussion of existing financial payments as being based upon Internet-based commerce using financial institutions, what he termed “trusted third parties,” as the
intermediary in a system of payments. The underlying “problem” that Nakamoto identified as the *raison d’être* for Bitcoin, specifically that “no mechanism exists to make payments over a communications channel without a trusted party,”\(^\text{10}\) is not actually removed from Nakamoto’s proposal for Bitcoin:

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. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.\(^\text{11}\)

The ‘nodes’ described in Nakamoto’s specification are the computer systems processing transactions, in the process ‘mining’ new Bitcoins. The “trusted third party” being rejected—the banking system—is subject to various forms of governmental oversight, constrained by laws covering fraud, provides a digital ‘paper trail’ of the transactions in question, and has an existing system of consumer protections already in place. The proposed replacement, Bitcoin, does not. This transformation is ironic in nature: that the “trusted third party,” the global banking system, is *not* trustworthy in itself is the reason for the multitude of legal and procedural oversight mechanisms. In place of these, Nakamoto’s design for Bitcoin relies on digital cryptography and limitations on computational power for most users to ensure the validity of

\(^{10}\) Nakamoto, “Bitcoin,” 1.

\(^{11}\) Nakamoto, “Bitcoin,” 1.
a system where the “trusted third party” may be purely technological—the timestamp server—rather than a bank that is already constrained by law:

The steps to run the network are as follows:

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.

Nodes always consider the longest chain to be the correct one and will keep working on extending it. If two nodes broadcast different versions of the next block simultaneously, some nodes may receive one or the other first. In that case, they work on the first one they received, but save the other branch in case it becomes longer. The tie will be broken when the next proof-of-work is found and one branch becomes longer; the nodes that were working on the other branch will then switch to the longer one.¹²

The ‘nodes’ in this description are the computers engaged in processing the transactions; the ‘blocks’ are the encrypted transaction keys that identify both parties to the exchange of Bitcoins: it is an automated system constructed to function outside of any human interaction and without requiring human oversight. This system is an example of the law of automation in action, in the process creating a mechanical

procedure to replace existing systems of financial circulation. As such it does not resolve the issue of the “trusted third party” or banking system, substituting a collection of other ‘third parties’ not subject to existing legal restraint or providing protection (the autonomous nodes) for a system based in human oversight and control—that these ‘nodes’ are, nevertheless, directed by humans is self-evident since they are set up and maintained by humans in exchange for a reward—the newly ‘mined’ Bitcoins. This substitution of a technological system (timestamp server) for institution where there is an established process to redress and resolve problems—i.e. legal recourse over fraud—is the aura of the digital inflating the assumption of technological superiority over established, physical (and historical) solutions. The trustworthiness of this productive system depends on a capitalist incentive—the profit generated by ‘mining.’

The Bitcoin proposal does more than eliminate human oversight and legal restrictions from the circulation of exchange values. It is an attempt to replace existing, formally organized, legal systems of protection for all parties in the transaction—the buyer, the seller, and the bank—with one based upon the assumption that the only parties involved in a transaction who need protection are sellers: this structural bias further reifies the same capitalist ideology that gives rise to digital rights management (DRM) in the transformation of everything that can be digitized into a digital form (the universal aspiration to the state of information). The only significant parties in such a framework are the owners (sellers) whose decisions about how to limit access find literal form in the DRM itself. Bitcoin is the reification of these interests at the level of exchange itself; this aspect of Nakamoto’s proposal has contributed to its embrace by grey and black markets (such as Silk Road) employing peer-to-peer exchanges

13 The Silk Road website, accessibly only through the TOR browser, is an anonymous marketplace that only accepts Bitcoin for its transactions, see http://veilednetwork.com/silk-road-url/ and http://en.wikipedia.org/wiki/Silk_Road_(marketplace).
where getting paid can be an issue. (The use of Bitcoin escrow at the original Silk Road\textsuperscript{14} contradicts Bitcoin’s purpose of avoiding the Bank or other middleman.) This embrace is ironic since it is a currency that inherently contains the ability to track all ownership and transactions. Unlike physical currency of all types, and in a fashion distinct from existing systems of exchange, Nakamoto’s description of Bitcoin eliminates the privacy afforded to purchases:

We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.\textsuperscript{15}

Every transfer of Bitcoin as Nakamoto designed the system offers the possibility to track the economic activity and associations of anyone using Bitcoin—as Barber, et. al. note, all Bitcoins are public knowledge.\textsuperscript{16} As a surveillance apparatus, it is difficult to imagine a more perfect way to monitor what and how citizens behave than to link transaction histories to the currency itself. Even peer-to-peer exchanges that would be beyond oversight with a traditional currency become subject to precise scrutiny. In attempting to remove the ‘third party’ (bank/government) from the exchange process, Bitcoin instead enshrines the authority it attempts to displace. The early embrace of Bitcoin by grey and black markets seeking to avoid the global banking system reflects this irony: the anonymity of “cash” is fundamentally eliminated in favor of a perfect economic surveillance of all transactions. The full

\textsuperscript{15} Nakamoto, “Bitcoin,” 2.
visibility of Bitcoin transactions enables the tracking of all informal association networks (all exchanges of value) involving any particular Bitcoin, thus providing sellers with demographic information about their customers (and anyone else with the computational power to penetrate the cryptography with metadata about association networks) without offering any possibility to “opt out” from having their privacy violated by the seller (or government). If coupled with an omnipresent government surveillance apparatus, Bitcoin enables a ‘Trojan horse’ surveillance of those unofficial marketplaces that specifically exist outside standard systems of exchange and which attempt to be anonymous by nature—this surveillance function of Bitcoin contributed to the conviction of Dread Pirate Roberts (Ross Ulbricht) over the original Silk Road.17

The valorizing process of capitalist expansion enabled by digital technologies is immediately apparent in the surveillance component inherent to Bitcoin. A further irony emerges from its lack of engagement with the formal banking system: Bitcoin lacks a formal system of recourse when problems of coin ownership, transaction validity, etc. do arise precisely because it is outside established legal frameworks. By creating this “private” currency outside of the legal and historical framework of governmental regulation and management of currency, Bitcoin is an ideological reification of globalized capitalism, and should be recognized as a tool whose alignment with authoritarian values has been masked by how the ideology of automation intersects with the aura of the digital: instead of being a “free” or “independent” form of money that transcends national boundaries, it is a technology of control aligned with globalized concerns over economic surveillance and monitoring the behaviors and associations of consumers’ behaviors in the physical world.

That in the current implementation and usage, the inherent surveillance is difficult to process due to the use of intermediary “digital wallets” does not eliminate its potential in the future. It is this in-built system of surveillance over transactions happening between individuals, especially since the current system forces the transfer of all the Bitcoins in a digital wallet, with a return transaction (change) being provided, that creates a demonstrable link for (and the value of) each transaction. This process also embeds the public keys for both parties in every transaction, further facilitating the correlation of keys to specific individuals even with randomly generated public key components.

Nakamoto acknowledges the privacy failure inherent in how Bitcoins record their transaction record as part of the currency itself. Nakamoto's solution, however, leaves the ability to “know” the full transaction history in place, just away from the “public” who employ the currency:

The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone. This is similar to the level of information released by stock exchanges, where the time and size of individual trades, the “tape,” is made public, but without telling who the parties were.

As an additional firewall, a new key pair should be used for each transaction to keep them from being linked to a common owner. Some linking is still unavoidable with multi-input transactions, which necessarily reveal that their inputs were owned by the same owner. The risk is that if the owner of a key is revealed, linking could reveal
other transactions that belonged to the same owner.\textsuperscript{18}

The only linkage that concerns Nakamoto’s proposal is a “public” one—but it is unclear who composes this “public.” However, multi-input transactions—the return of “change” in purchases involving a ‘digital wallet’ for example—as well as multiple purchases over time with the same vendors both offer the potential to ‘unmask’ the “privacy” as Nakamoto implements it. As Fergal Reid and Martin Harrigan note in their analysis of anonymity in the implementation of Bitcoin:

> With appropriate tools, the activity of known users can be observed in detail. This can be performed using a passive analysis only. Active analyses, where an interested party can potentially deploy ‘marked’ Bitcoins and collaborate with other users can discover even more information. We also believe that large centralized services such as the exchanges and wallet services are capable of identifying and tracking considerable portions of user activity.\textsuperscript{19}

The potential to track users is inherent to the Bitcoin implementation, and it is one where private transactions are, in fact, potentially fully public in spite of the use of cryptography. The availability of this information to sellers is clearly a potential even with the “safe guards” initially proposed. The result is a system where no privacy exists—except from casual perusal; the full availability of personal information to the seller is not only potential, it is highly likely given the organization of the system and its embedding of ‘a personal ownership history’ in the Bitcoin.

The conclusion for Nakamoto’s proposed financial exchange system does not solve the problems it identifies—the issue of “trust”—instead adding to those problems the poten-

\textsuperscript{18} Nakamoto, “Bitcoin,” 6.

tial for a complete dissolution of any privacy in economic activity. The statement that “We have proposed a system for electronic transactions without relying on trust.” that begins his conclusion is clearly without merit: not only does the system still rely on the reification of a social relationship as the currency, as with the fiat currencies it proposes to replace, it also still requires the currencies’ users trust a “third party” who is not involved in the transaction, while at the same time requiring an inherent surrender of privacy—all transactions employing Bitcoins are tracked in the “coins” themselves. The assumption that this information will remain private and secret is prima facie absurd given the history of both DRM restrictions on digital media and software, and the frequent challenges to even the most robust encryption technologies as new, more powerful computers become generally available.

What is apparent in Bitcoin is a dramatic reification of capitalist ideologies and valorization imperatives within/as the Bitcoin technology itself. The dissolution of privacy in Bitcoin is not the “problem”—it is a logical outcome given the valorization demands inherent in digital capitalism’s expansion into (formerly) social realms. The transformation of those social exchanges into the currency itself (new Bitcoins are “mined” through the exchange of existing Bitcoins) is a direct expression of this expansion: the valorization of social activities—such as friendship circles, browsing in a bookstore, or shopping without purchasing—becomes valuable data as digital technology valorizes those activities; Bitcoin is the valorization of authorship already present in “social media” taken to its logical conclusion. The creation of a currency from economic activity itself is the application of the same systemic shift focused on the generation of value through semiotic production rather than material facture.