Table of Contents

Introduction ...................................................................................................................................... 2
Methodology ................................................................................................................................ 7
Chapter 1: What is Bitcoin? ........................................................................................................... 10
Chapter 2: Literature Review ......................................................................................................... 17
  Algorithms .................................................................................................................................. 17
  Internet ....................................................................................................................................... 21
  Globalization .............................................................................................................................. 26
  Money ........................................................................................................................................ 30
Chapter 3: Passwords as Technologies of Trust ............................................................................ 34
  Algorithmic Attacks ................................................................................................................... 34
  Meaning vs. Entropy .................................................................................................................. 36
  The Limits of Self-Reliance ....................................................................................................... 39
  Password Ideology ..................................................................................................................... 44
Chapter 4: Bitcoin's Non-Political Economy ................................................................................ .48
  Mining Trust .............................................................................................................................. 51
  Trust in Value ............................................................................................................................. 54
  Endgame ..................................................................................................................................... 56
  Trust in Crisis ............................................................................................................................. 59
Conclusion ...................................................................................................................................... 66
Works Cited ................................................................................................................................... 70
Introduction

I am to speak of what all people are busy about, but not one in forty understands: every man has a concern in it, few know what it is, nor is it easy to define or describe it. If a man goes about to explain it by words, he rather struggles to lose himself in the wood, than bring others out of it. It is best described by itself; it is like the wind that blows where it lifts, we hear the sound thereof, but hardly know whence it comes, or whither it goes. (Defoe 1710)

Daniel Defoe was writing in the wake of an 18th century credit crisis. Yet even now everyone agrees that money is mysterious. Money unfolds into questions of value, materiality, trust, and politics, for each of which we struggle to explain “whence it comes, or whither it goes.” Even seemingly simple questions such as how money acquires value leave us wandering in the woods. What, then, is the point of studying a new and suspect form of money like Bitcoin? It is still unclear that Bitcoin actually is a form of money. It is also not clear whether it will have any lasting impact, or whether it is just the passing fancy of a specific Internet subculture. Bitcoin will not get us to the 'core' of money, even as a clue or counterexample.

What the study of Bitcoin gives us is both more and less ambitious. Anthropologists have pointed out that trying to find out what money “really is” can leave us unable to understand the complex forces of its development (see Hart 1986; Maurer 2005). It is important to build up our own answers to the mysteries of money. However, using our theoretical apparatus of value, fetishism, etc. immediately on the workings of money risks ignoring the complex ways in which users of money think through the same concerns on their own terms. Using Defoe’s metaphor, my goal here is not to lead others out of the woods, but to describe the wildlife and map the terrain where people wander.
I find Bill Maurer's metaphor of the McGuffin helpful as a cartographic tool (2005). In the movies of Alfred Hitchcock, the McGuffin is an object of unexplained importance that nonetheless drives the plot forward by catching the attention of the characters and audience. Maurer writes that questions of value and representation act like McGuffins, “compelling novel associations” while they captivate us (2005:61). This means that the content of discussions about money does not just have a descriptive link to the workings of money. Maurer steps away from the logic of *adequatio intellectus et res*, which presumes that representation must always be adequate to, or in accordance with, reality (ibid: xiii). Instead, the McGuffin works through motion, pushing the plot to make an object (such as money) work. Taking this perspective means that one should not overemphasize the sensible and realistic when studying the ideas of Bitcoin. The muddled and conflicted aspects of debate, those whose claims to adequation are nonexistent or unconvincing, are just as important in moving the plot along.

This motive quality of knowledge is often apparent in discourses of money. In Georg Simmel's *Philosophy of Money*, a short passage on methodology is a good example:

For the practice of cognition this must develop in infinite reciprocity. Every interpretation of an ideal structure by means of an economic structure must lead to the demand that the latter in turn be understood from more ideal depths, while for these depths themselves the general economic base has to be sought, and so on indefinitely. In such an alternation and entanglement of the conceptually opposed principles of cognition, the unity of things, which seems intangible to our cognition but none the less establishes its coherence, becomes practical and vital for us. (Simmel 2011[1900]:56)

The interpreter thus goes endlessly back and forth between the ideal and the material. They are stuck in M.C. Escher's famous drawing, *Ascending and Descending* (Figure 1). On top of a building, a staircase forms a continuous loop, a geometrical impossibility, while hooded figures
walk up or down eternally. What is important is not the end destination, which is absent in Escher's drawing, but the motor-like quality of their circular motion.¹

Figure 1: Ascending and Descending

¹For the first use of Escher’s "strange loops" to describe complex systems, see Douglas Hofstadter’s Gödel, Escher, Bach: An Eternal Golden Braid (Hofstadter 1979).
For Simmel, this motion converges asymptotically on the unity of material and ideal. The ultimate goal is that of “finding in each of life's details the totality of its meaning” (2011[1900]:53). Bitcoin enthusiasts often have similar goals. They wish to link the details of Bitcoin to a totality. Bitcoin is 'good to think.' The people I study use it to think through such diverse topics as state power, globalization and technological change. Bitcoin and its McGuffins are doubly articulated. Concerns such as those above drive the workings of the currency. In turn, the mechanics of Bitcoin drive the political and social concerns of those who promote it.

In the following chapters I focus on trust as a paradigmatic concern. In particular, I am interested in the constant labelling of Bitcoin as a “trustless currency.” What does it mean for Bitcoin not to require trust? Sociologists since Simmel have been concerned with the necessity of trust in economic transactions. Capitalism presents its markets as a natural consequence of individuals' desires. At first these could be satisfied by direct bartering between people. The inefficiency of barter, its requirement of a 'double coincidence of wants', led directly to the creation of money to lubricate transactions. In fact, the barter economy with its double coincidence of wants is probably a myth, and the origins of money are much more complex (see Mauss 1990 [1924]; Polanyi 1957). If Bitcoin enthusiasts want trustless markets based entirely on individual actions, they are aspiring towards an imaginary ideal. However, the uses of trust here are more interested and less consistent.

I am inspired by Simmel's *Philosophy of Money*, which describes money as an objectification of trust (2011 [1900]). Exchange is the basic mode of social relation, and money allows us to abstract it. Unlike the pre-money exchange modes of theft and gift, money is rationalized and objective. We become less dependent on specific people and more dependent on an abstract social system. While money allows trust to be congealed in specific objects and
circulated between people, it still requires social stability as the ground of its trustworthiness. At the same time, money contains an element of alienation since it gains a life of its own apart from peoples' need for it.

Simmel’s perspective calls us to identify where the confidence in money comes from and what roles it plays in economic life. As a playful nod to Bill Maurer's call for attention to the 'pragmatics of money', I quote from William James' *Pragmatism* (see Maurer 2006; Maurer 2005).

> Truth lives, in fact, for the most part on a credit system. Our thoughts and beliefs "pass", so long as nothing challenges them, just as banknotes pass so long as nobody refuses them. But this all points to direct face-to-face verifications somewhere, without which the fabric of truth collapses like a financial system with no cash-basis whatever. You accept my verification of one thing, I yours of another. We trade on each other's truth. But beliefs verified concretely by somebody are the posts of the whole superstructure. (James 1991 [1907]:91)

Like truth for a pragmatist, money lives because it works, because people accept it. Most of the time the confidence that money indeed works is just taken for granted. However, the superstructure of abstract trust still needs something to hold it up at certain points. Bitcoin takes these 'posts' as a central concern.

In the following chapters I hope to show exactly how and where Bitcoin obviates trust, and how trust still haunts Bitcoin. Chapter 1 gives a short history of Bitcoin’s creation and explains the technical details of how the currency works. Chapter 2 looks over previous scholarship on such diverse topics as algorithms, money, and globalization. I hope to lay out a scene on which the dramas of Bitcoin can play out.

Chapter 3 zeroes in on the specific practice of password choice. Password security is one of the posts that holds up Bitcoin's superstructure of trust. Passwords, as a computational
technique to control access to information, are an object of deep social and political concern. I
suggest that password choice, while seemingly a superficial and innocuous topic, actually
represents some important issues of trust and distrust in the Bitcoin economy. In particular,
password security can act as an ideological cover for the insecurity of online services such as
Bitcoin exchanges.

Chapter 4 broadens the focus to the political elements of a specific discourse of trust. The
radical perspective of Bitcoin sees it as a way to subvert the state, ultimately rendering it
unnecessary. Bitcoin's trustlessness is its most subversive aspect, in this view, clashing with the
logic of the state as a "trusted third party." This chapter also traces in more detail the travels of
'trust' as a McGuffin, from a technical term in cryptography to a grand political statement. Again,
trust and distrust point us towards the instabilities in Bitcoin's economy. The repression or
disavowal of trust leads to a fundamental tension in markets that use Bitcoin.

Methodology
Most of my research examines an Internet forum called BitcoinTalk (bitcointalk.org).
BitcoinTalk is the "main Bitcoin Discussion forum", with subforums for general discussion,
technical development, mining, economics, etc. According to Alexa's site rankings, BitcoinTalk
is the second most visited Bitcoin website, and the only dedicated web forum among the top
twenty-five. BitcoinTalk is the latest evolution of the very first Bitcoin forum, founded by
Satoshi Nakamoto. The domain changed several times, eventually settling on BitcoinTalk in
order to emphasize its unofficial status (BitcoinTalk Forum n.d.).

Methodology
Most of my research examines an Internet forum called BitcoinTalk (bitcointalk.org).
BitcoinTalk is the "main Bitcoin Discussion forum", with subforums for general discussion,
technical development, mining, economics, etc. According to Alexa's site rankings, BitcoinTalk
is the second most visited Bitcoin website, and the only dedicated web forum among the top
twenty-five. BitcoinTalk is the latest evolution of the very first Bitcoin forum, founded by
Satoshi Nakamoto. The domain changed several times, eventually settling on BitcoinTalk in
order to emphasize its unofficial status (BitcoinTalk Forum n.d.).

\[ \text{http://www.alexa.com/siteinfo/bitcointalk.org} \]

\[ \text{d_Money/Alternative_Monetary_Systems/Bitcoin} \]
is not the only reason to choose this forum as a data-gathering site. Its status as the main forum draws in major players. Software developers take advantage of the development subforums to interact with users, playing out the construction of technology. The newest versions of the official Bitcoin client are posted on the main board by one of the developers, with discussion and technical support. The importance of BitcoinTalk in the Bitcoin community is attested to by its relationship with states. The Chinese government has blocked the website with its “Great Firewall” (Suberg 2014). When the FBI tracked down Ross Ulbricht, the alleged mastermind of online drug market Silk Road, it was partially because of his insufficiently anonymized postings on BitcoinTalk (Goodin 2013).

There is a rich field of possibility for extending traditional ethnographic practices to the Internet (Hart 2004). The institution of ‘avatars’, in which actors assume a virtual identity in chat rooms and online worlds, engages questions of self-presentation. Caroline Humphrey writes about online 'masks' and offline 'faces', and shows that the correspondence of mask and face is a common matter of concern for users of a Russian chat room (2009). Tom Boellstorff takes on a mask himself to conduct participant observation of the virtual world Second Life (2010). However, traditional ethnographic approaches are challenged by digital data “with elements of anonymity, modalities of hypermobility, ephemerality, and mutability” (Coleman 2010). Linguistic anthropologists Jones and Schieffelin turn away from immersive ethnography in studying YouTube comments, which are marked by these challenges (2009). Instead, they rely on a very close reading, paying attention to the language used rather than individuals and personalities. My research uses narrative ethnography and close reading to study discourse on a web forum. I am not quite a participant observer, but a “lurker”, Internet language for someone who reads forums without posting.
I supplement my personal reading with probabilistic topic modeling. Computer scientists envision topic modeling as an advanced form of archive searching, which isolates themes from a hidden structure, allowing an explorer to zoom in and out through themes and texts (Blei 2012). Topic modeling does not replace human interpretation, but rather allows me to sieve through large amounts of data. While research on the Internet often produces “a profound sense of spatial disorientation”, the method of topic modeling is similarly vertiginous (Burrell 2009:185). It allows me to slide quickly between macroscopic and microscopic analysis.

I wrote a program in the language Python to perform topic modeling. This program scrapes the BitcoinTalk website for forum threads and downloads whole web pages. The program then stores these pages using SQLite, a database management system. I use Radim Řehůřek's open source Python library Gensim to run a topic modeling algorithm called Latent Dirichlet Allocation (Řehůřek and Sojka 2010). This learns a set of topics and assigns them to each forum thread, weighted according to how well they describe that thread. Each topic is labelled by a list of common words. For example, my program tags threads about password choice with the topic “password, email, passwords, encrypted, encryption, passphrase, login, characters, random, factor”. For each topic, the program then calculates those threads it best describes and outputs them into a folder. In addition, I can search the database of threads for certain words or posting dates using simple Python commands.4

I supplement BitcoinTalk as a field of study with close readings of other texts. Other forums, manifestoes, and papers come into play.

---

4 For internal parameters and other implementation details, see the source code at https://github.com/eddiesaid/BitcoinTalk-Research-2.
Chapter 1: What is Bitcoin?

Bitcoin itself is just the final step of a long chain of advances (Peck 2012). The first of these is Hashcash, a system intended to reduce email spam. In 1997, cryptographer Adam Back sent the description of Hashcash to a cypherpunk mailing list (Back 1997). Hashcash is a “proof of work” system by which a computer can prove it has expended a certain amount of computational power. In its spam reduction application, Hashcash allows a computer to verify an email by spending a significant amount of work. Recipients can then only accept those emails that are verified. Ordinary users will not be inconvenienced, but spammers sending out hundreds of thousands of emails will find the cost prohibitive. A year later, Wei Dai speculated on the possibility of using Hashcash as a protocol for a monetary system (Dai 1998). His proposal for b-money involved a distributed digital currency in which new money would be minted by proof-of-work. In 2005, cryptographer Nick Szabo elaborated these ideas into a cryptocurrency scheme called bit gold, which uses proof-of-work to mint money, and a peer-to-peer distributed chain of transactions to prevent double-spending (Szabo 2005).

Bitcoin only appeared late in 2008, when a developer or group of developers going by the pseudonym Satoshi Nakamoto created the website bitcoin.org and posted the paper “Bitcoin: A Peer-to-Peer Electronic Cash System” (2008). Early in 2009, he linked his paper and software to the web forum of the P2P Foundation, an advocacy group for peer-to-peer techniques like BitTorrent:

I've developed a new open source P2P e-cash system called Bitcoin. It's completely decentralized, with no central server or trusted parties, because everything is based on crypto proof instead of trust. Give it a try, or take a look at the screenshots and design paper:
Download Bitcoin v0.1 at http://www.bitcoin.org (Nakamoto 2009)
Forum members greeted the proposal with both enthusiasm and skepticism. From here, Bitcoin became the first cryptocurrency to find widespread use.

A cryptocurrency is a currency based on cryptographic protocols rather than state issue. Previously, all online commerce had relied on a central party that keeps track of the accounts of each party to the transaction. Think of a debit card: the buyer gives their card number to the seller, who then contacts the bank with the specific amount of money needed. If the buyer tried to spend more money than was in their account, the bank would decline the payment. Without this central authority of the bank, nothing would stop an online customer from spending the ‘same’ money twice. Bitcoin solves this problem by allowing every user to be aware of every transaction, as well as the order in which they were made. All of this information is stored in the public “block chain”, and verified by individual computers (‘miners’) solving mathematical problems.

If someone wishes to make transactions with Bitcoin, they can either sign up with a trusted online service or download some client software. To send a Bitcoin payment, the sender gets the receiver’s public key, inputs that key and the amount into the software, and presses “send”. From that point on, the money is unrecoverable. The transaction has been sent out into the peer-to-peer network, to be verified and added irreversibly to the block chain. To mine Bitcoin, one downloads some mining software and joins a “pool”, a group that unites their resources to carry out Bitcoin’s algorithms and shares the reward. This is necessary because Bitcoins are rewarded in large amounts only to the single miner who happens to create a new block, and the chances of any one miner receiving this reward is astronomically small (Volastro 2014).
The technology of Bitcoin relies on cryptographic hashing. In computer science, a ‘hash’ is an algorithm that converts a variable-length value into a constant-length value. The goal of a hash function is to minimize hash collisions, in which two input values will produce the same output value. Cryptographic hash functions also strive to be irreversible. This means that, given an output value, it is virtually impossible to compute the input value even if you know the hash function (Schneier 1994:28).

This kind of irreversibility is behind RSA, the most common protocol for encrypted communication (Schneier 1994:282). RSA is a public-key method. Each person has both a public key and a key that they keep private. If Amir want to send a message to Brianna, he encrypts it using her public key. The message can then only be decrypted using Brianna’s private key. It is easy for Brianna to create a public key, but almost impossible for anyone to figure out her private key from her public key. Before sending his message, Amir can also ‘sign’ it with his private key. Brianna can then use Amir’s public key to verify that the message came from him rather than an imposter.

Bitcoin works in a similar way (Brito and Castillo 2013). If Amir wants to send Brianna money, he sends a message including Brianna’s public key, signed with his own private key. Each coin consists of a chain of transactions (see Figure 2).

---

5 RSA cryptography uses prime numbers to create keys. In order to find somebody’s private key, an attacker would have to find the prime factors of some very large number. Finding prime factors is currently an ‘intractable’ problem in computer science. This means that the only algorithms to do it are so tremendously inefficient that a large enough number will practically never be factored, regardless of how much computing power you throw at it. Interestingly, there is a quantum algorithm called Shor’s Algorithm that efficiently solves prime factorization. The day we build a quantum computer to run it on will be the death of most of cryptography.
Each transaction includes a hash value which denotes the previous transaction in the coin's chain (Nakamoto 2008:3). If Amir was the recipient of the previous transaction, then he can validly make a new transaction with that coin.

Amir can even send values more or less than a single coin. To do this, each transaction contains multiple input values and two output values (see Figure 3). Each of the inputs is a hash value that points to a previous transaction in which Amir received some amount of money. The sum of all of these input transactions is split into two outputs: the value sent to Brianna, and the change which is sent back to Amir.
It is thus easy to check that the transaction is valid. First, check that Amir’s signature is valid. Second, check that Amir has not already spent any of the inputs in a previous transaction.

These transactions get sent online to every node in the Bitcoin network. From here, Bitcoin ‘miners’ gather together a group of transactions, verifying that each one is valid. Each miner groups valid transactions into a ‘block’. They then run a proof-of-work algorithm on the block. This means trying to find a ‘nonce’ value such that, when the nonce is added to the block and the block is run through a cryptographic hash function, the resulting hash value has a certain number of leading zeros. There is only one way to do this: guess a nonce, hash the block, check the value, guess another nonce, etc. The solution is difficult to find, but easy to verify.

Eventually, somebody will ‘solve’ their block, and that block will be added to the ‘blockchain’. The solver of the block is rewarded with some amount of Bitcoins. Each block in the blockchain includes the hash value of the previous block, a list of transactions, and the nonce that solved it (see Figure 4). The blockchain itself does not live on any central server. Every miner has their own copy of the blockchain.
What is the point of the proof of work system? Say I want to scam the system. I cannot spend money I do not have, since the recipient will not accept the invalid transaction. All I can do is remove one of my previous transactions from the blockchain so I can spend that money again. Because each block includes the previous block’s hash, if I want to change a block, I would have to solve every block that comes after it. I could try to split the blockchain at that block, convincing everybody that my new branch is the correct one. However, nodes will only accept the longest chain as the valid one. I would have to solve enough blocks to ‘catch up’ to the valid chain with my own false chain.

In this way Bitcoin operates by a kind of democracy. The longest chain is the one with the most ‘votes’, represented by the most computational work that has been putting into solving blocks. The only way I can reverse a transaction is if I personally control more than half of the ‘votes’. This is called a “51% attack.” If I have more than half of the computational power put into mining Bitcoin, then I can make a false chain as long as the true one. This is so fantastically unlikely that Bitcoin transactions are effectively irreversible.

Minting of Bitcoins occurs only when a miner solves a block and receives a reward. The Bitcoin protocol regulates the rate at which miners solve blocks by changing the difficulty of the proof of work: that is, the number of leading zeros required in a hash value before the block counts as ‘solved’ (Nakamoto 2008:3). In addition, the reward for solving a block is always
decreasing. Eventually, there will be no more rewards and the total number of Bitcoins will be fixed at 21 million (Brito and Castillo 2013:7).
Chapter 2: Literature Review

Algorithms

Like all computational objects, Bitcoin operates through algorithms. According to computer scientist Donald Knuth, an algorithm is “a set of rules for getting a specific output from a specific input. Each step must be so precisely defined that it can be translated into computer language and executed by a machine” (1996:59). This second condition is important because, without it, almost anything can be seen as an algorithm. Nonetheless, algorithms long preexisted computing machines. Knuth even finds them in 4,000-year old Babylonian tablets (Knuth 1972). Decades after computer science rose as the study of algorithms, varied interdisciplinary studies of the social role of algorithms have emerged. These scholars have brought up many interrelated questions. What does the mechanistic character of algorithms mean for social categories such as style and politics (Wilf 2013; Helmreich 1998)? And where and for what purposes are algorithms being used (Muniesa 2011; Lenglet 2011; Mager 2011; Cheney-Lippold 2011)? A few themes of the new “critical algorithm studies” will benefit the discussion of Bitcoin (Seaver 2013). I will discuss the agenthood of algorithms, the role of algorithms in consumer society, and the varied intrusion of algorithms into financial capital.

A number of scholars have seen algorithms as an active component of social life. These studies are often influenced by the actor-network-theoretical view of society as a fabric of multiple interacting actants, including both humans and non-humans (see Latour 1990). For example, Eitan Wilf’s research on the jazz-playing robot Syrus shows that the algorithms by which computer scientists simulate improvisation constrain, and hence ‘style’, the “practices of styling styles” by which music occurs (Wilf 2013). The algorithm doesn't just simulate style, but itself styles. Online dating is another site where algorithms emerge as actors (Churchill and
Goodman 2008). The algorithms that dating websites use both teach users how to present
themselves and learn from users how to parse profiles. Desire is most literally embodied in the
"genetic algorithms" by which computational biologists create artificial life (Helmreich 1998).
The designers of these reproducing pieces of software assign to them the terms of heterosexual
desire and religious cosmology. In turn, the computer algorithms make their designers
reformulate biological concepts of reproduction and evolution in informatic terms, thus given
kinship discourses themselves a cybernetic tinge.

Algorithms play an increasing role in consumer society. Marketing algorithms track
users' internet browsing habits to infer demographic information, and then use that information
to target advertisements towards them. These algorithms act by defining, "the identification of
particular groups within populations largely through the marketing logic of consumption"
(Cheney-Lippold 2011:167). John Cheney-Lippold argues that algorithms produce a cybernetic
form of identification which is flexible and ever-changing (2011:168). Marketing algorithms take
disaggregated "dividuals", which are individual data points about internet users, as their objects
of control (ibid). Astrid Mager uses the concept of ideology to theorize marketing logic in
algorithms (2011). In the case of Google, which funds itself by advertising, "the capitalist spirit
gets embedded in search algorithms by way of social practices" of marketing (ibid:10). The ways
in which these algorithms work, as implanted by the practices of both providers and users,
reinforce the informational model of consumption and the profit-based model of Internet
searches. While marketing algorithms and Bitcoin algorithms operate in different sectors of

---

6Cheney-Lippold is drawing from Deleuze's concept of the societies of control, which replace Foucauldian
mechanisms of discipline with "modulations", constant and ever-changing means of control. Instead of the
pairing of masses and individuals, societies of control pair data and 'dividuals'. See (Deleuze 1992).
consumption, they still interact in the cultural sphere. Bitcoin's cryptographic discourse of privacy stemming from an algorithm competes with the discourse of information sharing for convenience that surrounds marketing algorithms.

The introduction of algorithms into financial markets is a complex theoretical topic because it comes parallel to a similar shift in economic science, the discipline most tasked with studying and creating these markets. Historian Phillip Mirowski describes how since World War II, economics has come under the influence of the “cyborg sciences”, which take the computer as the “paradigm object” in a cybernetic theory of everything (Mirowski 2002:13). Unlike the dominant neoclassical theories of economics, this cyborg revolution focused on disorder, drawing from thermodynamics, and attempted to specify economic agents as information processors, drawing from cybernetics. Even more recently, argues Mirowski, economics has turned away from specifying individual agents towards “the formal specification of markets as evolving computational algorithms” (2007:210). Computer science, the study of algorithms, made its mark on the field after it was found that much of the economic research done in the game-theoretical field of “mechanism design” had already been accomplished in the computer-scientific theory of automata. Economists synthesizing the two traditions came to see markets in computational terms of algorithms and state machines. Both of these shifts, the cyborg shift and the algorithmic shift, had the effect of “reifying 'information' as an entity that has ontologically stable properties, preserving its integrity under various transformations” (Mirowski 2002:16). Bitcoins are digital information in the most literal sense, and at least one economic study of Bitcoin has taken the cybernetic approach, focusing on information sharing and feedback loops (Garcia et al. 2014).
This materialization of information spreads from economists to economic actors themselves. The mechanization of the London Stock Exchange led to a dramatic change in the discourses of finance, with traders coming to see the market as “a series of interconnected information flows” (Pardo-Guerra 2010:85). The ontology of the market changes when prices are stored in a computational database rather than personally negotiated: price information displayed on an electronic billboard is no longer a representation of the market, but the market itself.

Another example comes from Fabian Muniesa’s study of the Arizona Stock Exchange, which attempted to maximize liquidity by using a central algorithm to determine prices and the allocation of orders (2011). This change challenged the very definition of a ‘stock exchange’, causing problems for the Securities and Exchange Commission. The SEC proposed a redefinition: instead of an exchange being characterized by its institutional nature, it should instead be reduced “to its purely mechanistic, algorithmic component”: a trading system that discovers the prices of assets (ibid:5). Sometimes these computer solutions had a strong ideological background, as in the example of Island, a short-lived electronic trading platform in New York which was founded with a libertarian hacker ethos (MacKenzie and Pardo-Guerra 2014). The trading books were to be completely open, and investors would be allowed to trade without the mediation of brokers. Bitcoin’s problematics of openness and immediacy have a mirror in the finance world, if a short-lived one.

Like these mechanized financial markets, the Bitcoin economy is constituted by a central set of algorithms. Yet these algorithms are also decentralized, and put into the hands of individual market participants. In this sense they are also similar to high-frequency trading algorithms that use computation to make very fast, very large trades (MacKenzie 2014; Lenglet 2011). As algorithms move from exchanges to market participants, “they reconfigure the nature
of agencies making markets, allowing institutions that have both the abilities to develop
machines and the financial resources to deploy such systems to make healthy profits” (Lenglet
2011:45). Likewise, Bitcoin mining decentralizes the making of markets, while requiring a large
amount of resources to make profit. Trading algorithms bring up problems of governance as their
machine code conflicts with the regulatory code. Both MacKenzie and Lenglet use the metaphor
of an “arms race,” drawing from images of technologized violence and acceleration. Speed and
inhumanity are parts of the social imaginary of finance that are exacerbated by algorithms.

Internet
A number of scholars have studied the Internet as a new site of social interaction. These
studies cover identity, politics, and governance.

Scholars studying the Internet have focused on the forms of identity and sociality that
arise there. Sherry Turkle has shown how identity on the Internet takes the form of multiple,
parallel selves (Turkle 1999). People will often take on different identities in different sites. On
web forums, where the body is represented by a textual description, people can control their
presentation of self to a greater extent than they can offline. These Internet spaces replace the
relatively stable identity of the name with the more customizable identity of the pseudonym. This
means than people can express new aspects of their selves or even take on multiple selves: “it is
not unusual for someone to be BroncoBill in one online community, ArmaniBoy in another, and
MrSensitive in a third” (ibid:643). A similar effect takes place in virtual worlds such as Second
Life, in which a user takes on a visual avatar and interacts with others (Boellstorff 2010). In Tom
Boellstorff's ethnography of second life, he argues that the 'actual' and 'virtual' should not be
placed on a hierarchy of real and not real. Virtual spaces are important sites of interaction and
cultural production. Boellstorff argues that the gap between the virtual and actual, created by the
practices of users, is foundational to the culture of virtual worlds. In consequence, people will inhabit entirely different identities in Second Life and "First Life". The authenticity of and correspondence between the two identities is a matter of concern for web users. In a Russian web forum that Caroline Humphrey studies, this binary is handled by a discourse of an online 'mask' over an offline 'face' (Humphrey 2009). The ideology of the avatar, or online representation, is that it "reveals to the world the aspects of the self that are suppressed in the ordinary life because of conventions or the gender/age/status pressures of family relations" (ibid:46). Thus, the mask and the face are each seen as more authentic than the other in different ways.

The use of Bitcoin falls into the category of the political use of digital media. The literature on political uses of the Internet is one of hot debate and contradiction. In the words of media theorist Zizi Papacharissi, expressive technologies such as the Internet "tend to trigger narratives of emancipation, autonomy, and freedom in the public imagination... Usually, these discourses are framed within utopian and dystopian polarities that represent hopes and fears projected onto these new technologies" (2010:3). On the utopian side are those who emphasize the democratizing power of social media. An 'environmental view' of social media sees them as generally strengthening civil society (Shirky 2011). According to this school, social media networks are politically effective because of their integration with personal networks, their low cost of entry, and their multiple means of access (Faris and Meier 2012). The Internet allows political movements to quickly mobilize supporters and organize actions. Drawing from sociologist Manuel Castells, Faris and Meier point out that the Internet creates interactivity, turning citizens from "passive recipients of information" to "co-producers and mediators of information" (ibid:201).
Other theorists think that the benefits of new media are overstated. Media theorist Lev Manovich sees the rise of interactivity not as a sign of greater participation, but as a shift from representation to manipulation (Manovich 1996). Media have always been interactive – viewing any art requires thinking, moving, and filling in missing parts - but “interactive” computer media asks us “to follow pre-programmed, objectively existing associations”. Think for example of a Facebook profile, in which interactivity involves filling in required personal information, clicking suggested links, etc. The criticism, later taken up by Alexander Galloway, that “today, interactivity means total participation, universal capture” echoes Herbert Marcuse's critique of technological rationality, which subordinates human spontaneity to a rationalized set of directions (Galloway 2006; Marcuse 1985). If Marcuse, Manovich, and Galloway are right, digital media are potentially more authoritarian than democratizing.

Further critiques of the political benefits of the Internet focus on whether it really is as effective as people claim it is. Social media, argues journalist Malcolm Gladwell, create and organize “weak ties” of acquaintances rather than close friends (Gladwell 2010). Activism, on the other hand, is most effective when built upon strong ties. Social media do not increase motivation, but rather participation in low-risk and low-cost efforts – liking a Facebook page, for example. While optimists assume that Internet platforms would make organizing faster and more efficient, pessimists like Evgeny Morozov observe that “leaner doesn't always mean louder” (Morozov 2009). Civil society organizations, argues Morozov, do not find it any easier to advocate or raise awareness in the Internet era. The reason is that “cyberspace politics is a zero-sum game”, empowering not only the friends of the open society but also its enemies, such as nationalist extremists and anti-vaccination movements (ibid). In addition, governments have
become more skilled at Internet censorship. Social movements that rely on the Internet for organization are more vulnerable to government surveillance by digital means.

Morozov's argument that the Internet empowers the voices of a large number of varied movements, regardless of their content, is a good thing from the perspective of liberalism. The only problem for a liberal is to avoid the second effect, that the Internet empowers government repression. Indeed, these are the concerns found among hackers, who use the language of free speech, privacy, individualism, and meritocracy (Coleman and Golub 2008). Anthropologists Gabriella Coleman and Alex Golub find that liberalism among hackers is not really a coherent body of thought or norms, but instead a cultural sensibility that is constantly being negotiated in practice. Out of the “constellation of shifting genres” that constitute hacker ethics emerge three major themes or categories: cryptography, free software, and hacker transgression. Cypherpunks promote cryptography as a way of ensuring negative freedom from intrusion into one's privacy, sometimes facing government repression for doing so. This strain emphasizes the autonomy of individual, self-reliant subjects produce their own freedom. The free and open source software community, on the other hand, promotes the positive freedom for hackers to be able to create new things. Sharing the source code of software for free allows developers to learn and express themselves through creation. The final strain is the hacker underground, which critiques political institutions by transgressing the norms and barriers of technological life. The morality of underground hackers “values the process of piercing through locks, disarming security, accessing the inaccessible, eliminating barriers, and reaching the pot of gold behind the locked door – knowing full well that barriers will always come back in some form” (ibid:264). All three of these practices of liberalism are relevant to Bitcoin: cypherpunks latch onto the concept of
“cryptocurrencies”, open-source software developers build Bitcoin clients, and hacker/trickster/scammers such as LulzSec use Bitcoin for payments.

Another line of study of the Internet focuses on the types of governance and power that it expresses. Bitcoin enthusiasts talk about regulation and censorship a lot. They see Bitcoin as a way of escaping the control that sites like PayPal have over the flow of money. But Bitcoin itself relies on its own governing practices. Legal scholar Lawrence Lessig's concept of 'code' is useful here because it shows how the software and protocols of the Internet are themselves a form of governance (Lessig 1998). The architecture of cyberspace, embedded in software and hardware, acts alongside laws and social norms to regulate how the Internet works. The way these features regulate our behavior often slips below our notice. These rules of protocol and infrastructure are subject to significant political contest, as political scientist Daniel Pare shows in his study of IP address policy (2003). On the flip side, there is the use of the Internet in governance and regulation. The Internet features heavily in neoliberal ideologies of transparency (Mazzarella 2006). These ideologies have even been updated for the fad of Big Data and algorithms, with some pushing for “algorithmic regulation” and “open source analytics” to replace government regulation, which they as inherently slow and heavy-handed (Bollier 2010; O’Reilly 2013).

Media theorist Alexander Galloway puts the Internet in the context of three different diagrams of power, which he calls centralized, decentralized, and distributed.

Centralized networks are hierarchical. They operate with a single authoritative hub. Each radial node, or branch of the hierarchy is subordinate to the central hub… A decentralized network is a multiplication of the centralized network. In a decentralized network, instead of one hub there are many hubs, each with its own array of dependent nodes… Distributed networks have no central hubs and no radial nodes. Instead each entity in the distributed network is an autonomous agent… A distributed network is always caught, to use an expression from Deleuze and
Guattari, au milieu, meaning that it is never complete, or integral to itself. The lines of a distributed network continue off the diagram (Galloway 2004:30).

Distributed networks are highly controlled, not by central points of control, but by the “formal apparatus” of protocol. Galloway's materialist approach to power on the Internet is useful because it includes infrastructure, software, and discourse. Like Lessig, he emphasizes the role of code as a governing structure, but 'protocol' is much broader than specific software. It also motivates comparison to other systems of distributed power.

Globalization

Much of the appeal of Bitcoin comes from its global status. Theoretically, anybody across the world can buy and spend Bitcoins online, allowing the currency to transcend territorial boundaries. But is Bitcoin truly a global phenomenon, or a transnational phenomenon, or a post-national phenomenon, or any of a number of related terms? Answering this benefits from the diverse scholarship on globalization.

Manuel Castells theorizes globalization as a network phenomenon. Just as everyone agrees we have entered a new economy, he argues, we have also entered a new society that works around global networks (Castells 2000). The changes taking place are multidimensional, including the deployment of information technology; globalization; hypertext and the culture of “real virtuality”; the demise of national sovereignty; and scientific progress leading to a “deep ecological consciousness” (ibid:694). The concerns of the New Economy discourse in the late 1990s overlap with those of Bitcoin: instant global communications, a digital economy, seemingly inevitable neoliberalism, and the hope that new financial techniques will lead to the extinction of business cycles (Downey and Fisher 2006). Yet the economic crisis consigned the New Economy's hopes to the dustbin, and its theories are largely abandoned. This bodes ill for the “new society”, but Castell's work is still relevant. Particularly important is his theorization of
social movements, which live or die based on their deployment of identity in a networked society (Castells 2004). Movements as diverse as feminism, Islamic fundamentalism, and the anti-globalization movement all attempt to oppose their own global networks to “the global networks of wealth and technology” (ibid:144). All of these groups are formed around particular oppositional identities.

The last movement mentioned, the “anti-globalization” movement, makes a fruitful comparison to the Bitcoin movement. First, the anti-globalization movement tolerates extraordinary diversity within itself, including everyone from Zapatistas to French farmers (Castells 2004:153). They are not unified around a central ideology, but instead mobilized by a network responding to certain shared interests. Second, anti-globalization protestors place a premium on “prefigurative politics”, in which the means are expected to include the political ends in them, and “direct action”, which takes place outside of existing political structures to directly build a new world inside the old (Graeber 2009). Finally, the anti-globalization movement uses decentralized digital networks to organize, and reflects the structure of these networks in their decentralized and nonhierarchical organization (Juris 2008). The use of Bitcoin is a type of libertarian direct action, since it means directly building new institutions to replace the old ones: making a new money, instead of just protesting the old one.

One of the most nuanced approaches to globalization comes from Saskia Sassen, who focuses on microscopic processes of denationalization that constitute globalization (Sassen 2006). These denationalizing processes are not always obviously global, and they often come from within the nation-state itself. This second point accommodates theories of globalization that criticize the myth of state powerlessness, preferring to focus on states' adaptability (Weiss 1997). Denationalization does not occur in opposition to the nation-state, but can itself be a state
strategy. There has been one sharp divergence, argues Sassen, between the logics of organization of the phase before globalization and the current phase. This is that “in earlier periods, including Bretton Woods, that logic was geared toward building national states; in today's phase, it is geared towards building global systems inside national states” (2006:16). Note the specificity that global systems occur inside nation-states. The organization of states is not static, but instead certain national components of national institutions have given way to non-national components of national institutions (ibid:232). An example of the former is the Keynesian economic policy of the 1930s which, Sassen writes, “functioned as an enlightened version of nationalism” (ibid:140). An example of the latter is the redistribution of power in the United States towards an increasingly privatized and deregulatory executive branch (ibid:174).

Sassen's account of globalization also takes into account the rise of digital networks, which she sees as global assemblages. The Internet is one of these assemblages, but much of the denationalizing power attributed to it comes not from public networks but private dedicated networks, such as those used for global digitized finance (Sassen 2006:335). New communication technologies are not as important for political mobilization as Clay Shirky thinks they are. The Internet is either unnecessary for political organization, or it is creatively integrated with older media to serve the needs of certain communities (ibid:367). For example, the M. S. Swaminathan Research Foundation in South India uses the Internet to send audio files that are then broadcast over loudspeakers to spread information to illiterate populations. This example of communication technologies being used for local needs is a far cry from Bitcoin and its accompanying discourses of liberation through high-tech modernity.

Bitcoin, as a globalized digital form of money, has certain affinities with the financial instruments that have developed over the past thirty years. Financial development is an important
aspect of globalization, whether viewed through Castell's network terms or as one of Sassen's microprocesses of denationalization. This "revolutionary change" in financial systems has allowed people to borrow greater amounts at cheaper rates, invest in a large diversity of instruments, and spread their risk globally (Rajan 2005). According to economist Raghuram Rajan, these changes can be explained as a result of technical change in communication and computation; deregulation; and institutional change with the creation of new financial entities such as hedge funds (ibid). More generally, LiPuma and Lee contextualize financial development as a result of capitalism's compulsion to "perpetually and compulsively drive toward higher and more globally encompassing levels of production" (2004:19). There exists now a huge amount of speculative capital which is not oriented towards production. The greatest amount of this is in the form of derivatives, contracts that distribute risk by trading it away. Derivatives produce new discourses of risk, which is quantified and distributed, and give speculative capital the alibi of spreading risk to those who can better handle it (ibid). However, Rajan argues that financial development has actually increased the amount of risk in the world, by incentivizing investment managers to take greater risks in investment choices and to herd with other managers. The credit crisis in 2007 proved his worries prescient.

Although financial markets seem abstract and impersonal, studies have focused on revealing their social character. Economic actors interpret and perform the market through "cultures of circulation" (Lee and LiPuma 2002). One example is the evaluation of financial instruments. Donald MacKenzie shows actors accomplish this evaluation through complex and evolving "clusters of evaluative practices" (MacKenzie 2011). These practices, in the form of faulty mathematical models, contributed to the credit crisis. Anthropologists have focused on cultures in specific trading floors, coming to terms with a "financialized time-space" that most
people feel estranged from (Maurer 2012). Caitlin Zaloom's ethnography of the Chicago Board of Trade reveals the enactment of a specific type of economic subject, characterized by hyper-masculinity and the fetishization of risk (2006). On the other hand, Mitchel Abolafia shows that market makers of the New York Stock Exchange take pride in how regulated their market is (2001).

In addition, studies of finance emphasize that, global rhetoric notwithstanding, financial markets take place in certain cities of the rich world. In Sassen's terms, financial globalization is 'lumpy' rather than smooth, concentrated in global cities such as London and New York (2006:332). These cities operate in a “space of flows” in which network connections rather than local characteristics are the defining features (Castells 2000). The national or local character of global finance also shows itself in tax havens. The OECD's campaign against “unfair tax competition” ran up against issues of sovereignty and fairness (Maurer 2010). Interestingly, most of the controversy has been about the sovereignty of nation-states, rather than the economic freedom of individuals. Bitcoin fits incongruously into this debate, since it attempts to free circulation from national governance as well as global governance, and thus denationalizes aspects of sovereignty.

Money

What narratives of the denationalization of money through globalization often miss is that money has not always been national. Challenges to territorial currencies are nothing new. While Jean Bodin declared in the 16th century that currency creation was an integral part of state sovereignty, national money would only come to exist in the 19th century (Helleiner 2003). There were a couple of prerequisites for this to occur. First, technological transformations were required to create territorial national money. In the late 18th century, people in Europe invented
machines that allowed the mass production of good-quality coins (Helleiner 2003:49).

Previously, coinage was slow to produce and easy to counterfeit. The difficulty of producing enough low-denomination currency made it hard to integrate the poor into the national money, and the frequency of counterfeiting made it hard to maintain the trust and stability of the currency’s value. Second, national money could not exist without the nation. The late 18th century rise of the nation-state and the “rule of law” as its way of handling the economy allowed states to enforce legal tender laws and prevent counterfeiting on a large scale – for example, this latter function motivated the creation of the United States’ Secret Service (Sassen 2006:105; Helleiner 2003:45). However, these two conditions only allow the creation of national money, not explain it. Even when they were met, some nations developed a territorial currency later than others or not at all.

Political economist Eric Helleiner puts forth four motivations to explain the creation of national currencies (2003). First, national moneys allowed states to create a national market by manipulating transaction costs. This involved the vertical integration of the poor into the national economy by creating low-denomination versions of the same currency. Previously, the poor and the rich often had to use completely different currencies. Vertical integration was motivated by industrialization pulling the poor into a market-based economic life, rather than one based on self and community sufficiency. Second, national moneys allowed states to implement macroeconomic policies by controlling the money supply. This motivation was of comparatively little importance, and only came into play after the Great Depression. Third, fiscal policies became possible with the nationalization of money. The ability to print money to finance short-term expenses was desirable, especially when it came to warfare. Finally, national money was used to construct a strong national identity. Government officials often tried to give money a
didactic function, as explained by a clerk with the mid-19th century United States treasury: notes should be printed with pictures of national incidents, so that “they would soon be familiar to those who would never read them in books, teaching them history and imbuing them with a National feeling” (quoted in Helleiner 2003:106).

The history of money teaches us that many of the issues of Bitcoin are nothing new. The technological issues of national money are one example. A major benefit of Bitcoin is that it makes it easy to send very small amounts of money. Micropayments were once the wave of the future in monetizing the Internet. Theoretically, users would be able to pay a fraction of a penny to read an article. This would eliminate the need for obnoxious advertisements, and consumers would barely notice the payments! Micropayments were a resounding failure, partly because of transaction costs and partly because of the “mental transaction costs” of deciding whether to pay (Shirky 2003). Bitcoin has revived these old hopes because people could use the same payment system for micro- and regular transactions, without any fees. If it succeeds, this would be a new kind of vertical integration.

The political concerns of Bitcoin also have their precedents. A particularly fruitful comparison is with the debates between ‘greenbackers’ and ‘bullionists’ in the 1870’s United States (Carruthers and Babb 1996). The bullionists advocated for a return to the gold standard for US currency, while the greenbackers advocated for “retention of greenbacks, nonconvertibility of notes into specie, rejection of the gold standard, and repayment of the national debt in paper currency” (ibid:1564). This dispute was partially motivated by economic interests: greenbackers were often farmers, who benefitted from inflation, while bullionists were often bankers. Nonetheless, the debate centered on powerful disputes over the nature of money and value. Greenbackers pointed out what we would call the ‘social construction’ of money. Money only
has value because of social agreement, and alternative systems are possible. Not even gold or silver have inherent value, according to the greenbackers. Bullionists asserted that paper money only has value because it represents ‘real money’ – gold, which has an inherent value. Governments cannot be trusted to assert the value of money. The only trustworthy standard of value is the “natural” standard of economic law (ibid:1572).

These arguments sound very familiar to observers of Bitcoin. When somebody argues that Bitcoin is not ‘real money’, advocates become strict nominalists. Money only has value because people are willing to exchange for it, so it is ridiculous to talk about ‘fake’ or ‘real’ money. On the other hand, there is a strong sense that Bitcoins do have an inherent value. Bitcoin tends to attract modern-day ‘goldbugs’. Like gold, it takes work to produce, and like gold, its quantity is limited. As such, Bitcoin proponents feel that it has a more stable and trustworthy value than the government’s fiat money. They often draw on Austrian School economists like Friedrich Hayek to argue that the state will never be able to control the money supply in a trustworthy way. Instead, money should be controlled by the ‘natural laws’ of the market.
Chapter 3: Passwords as Technologies of Trust

Choosing passkeys is a common thread topic on the BitcoinTalk forum. Forum users are constantly concerned with the security of their passwords. As such, they constantly give each other advice about how to choose a secure one. One representative thread starts with a list of rules posted by user Vladimir:

1. Do not use the same password in more than one place.
2. If you can remember your password, it is probably weak.
3. If your password is less than 12 character long it is probably weak.
4. If your password does not contain numbers, upper-case letters and some weird symbols, it is probably weak.
5. Use password management software to store and generate passwords, such as firefox's password manager, keepass etc...
6. Use long mnemonic pass phrases as master passwords for password managers and other accounts which you need to be able to access without using password management software (like gmail account and truecrypt containers, for example)
7. Consider writing some important passwords down on paper and storing it in secure location.

This list exemplifies two of the three concerns that mark these threads. First, there is the consideration of the limitations placed on password choice. Second, there are the strategies to create a password within these limits. Third, there is the conflict over the boundary between threats that can be avoided by user password choice and those that are out of the user's control. These concerns work to both conceal and unveil the elements of distrust and insecurity that characterize the current Bitcoin economy. Threads about password choice represent the repressed instability of online services like Bitcoin exchanges.

Algorithmic Attacks
The figure of the hacker motivates password choice in these discussions. Posters never describe these hackers, nor do they question why they exist. Instead, people take for granted that
anything protected by a password will be attacked, and users are responsible for choosing a password that is difficult to crack. Hackers are just part of the online landscape. Part of the reason that hackers are so faceless in these threads is that passwords are a generic technology. The tips that people give for password security are intended for any specific application. Nonetheless, when there is a crisis in the confidence that passwords provide, Bitcoin and Bitcoin-related applications are the cases that people bring up.

As user bcearl explains, passwords can be divided between 'online' and 'offline'. Online passwords are what a user enters to log into a website. The website can limit the frequency of login attempts, so these are less susceptible to being broken. All other passwords are offline, without a website to act as a gatekeeping mechanism. The private key of a Bitcoin wallet, or a key used to encrypt a local file, are examples of offline passwords. A hacker who has access to the encrypted file can use an algorithm to try out as many different passwords as quickly as they want.

The most naïve algorithm to do this is called a *brute-force search*. It iterates through every possible value, trying out each of them. If, for example, you have a password of eight lowercase Roman alphabet letters, the brute-force search algorithm would have to try out about two billion possible passwords, which is not that many for a computer. This is why password threads usually recommend using much longer passwords, with a mix of letters, numbers, and symbols. See points 3 and 4 of Vladimir's list. This increases the *search space*: the number of possible solutions that the algorithm has to try out.

A better algorithm takes into account that passwords are usually not entirely arbitrary. *Dictionary-based search* uses a dictionary of commonly used words and phrases to make guesses. If your password is “password”, dictionary-based search will find it on the first or
second try rather than the billionth. In order to be secure against dictionary attacks, forum posters advise that the characters in a password be independent of each other. Posters contrast a strong, dictionary-word-free password like “n41iR32Rr22141R32Rr221” with a more susceptible password like “rascal101”, which will fall quickly to a dictionary-based attack.

**Meaning vs. Entropy**

Users do not only want a secure password. They also want one they can remember. Dictionary words are tempting in passwords because their meanings makes them memorable. The reliance on dictionary-based attacks turns hackers into a counter-signifying force, punishing people for using meaningful passwords by cracking their files. Users, on the other hand, struggle to maintain the significance of their passwords in a way that will not expose them to attack.

**Strategies to do this make up the bulk of the posts in password threads.** Poster Timo Y describes a common technique:

- Write you own poem, and keep reciting the poem at least once a week.
- Then create your own rule for converting the poem into a password. eg. take 3rd and 5th letter from each word and capitalize if word is a verb... or something more complex. Just make sure you keep the rule to yourself.
- 40 character password that is *both* secure and hard to forget. Sorted!
- Needless to say, don't ever use that password online.

The idea of using a poem comes up many times in these threads. Converting a poem into a seemingly meaningless string of letters with a memorable rule allows meaningful passwords to escape the counter-signifying dictionary attack. Poster bitplane in the same thread makes a similar suggestion:

- You have to read a lot and have a good memory, my favourite password system is to take either the first or last letter from a memorable sentence in something you have read, will never forget and has a tedious link to the site/file you're logging into. For example, you could associate a gambling account with a couple of lines from If by Rudyard Kipling:
If you can make one heap of all your winnings
And risk it on one turn of pitch-and-toss
Could make the password "IycmohoaywAriootopat", which you're unlikely to forget.
If you read a lot you'll have an endless supply of fresh, very memorable and
extremely long passwords!

Bitplane's post is unique among poem posts in that they advocate using a preexisting poem.
Every other similar post I have seen has suggested making a unique and personal poem. The
logic of this is clear: now that I know bitplane's strategy, I could theoretically write an algorithm
that cycles through sentences by classic authors, taking the first or last letter of each word, and
tries it out as a password. Oddly enough, they seem to recognize this possibility, and even leave
it as a challenge for the reader:

Now, knowing this, can you crack an old password of mine from the book Fight
Club?
Clues: It's 14 chars long, it's based on the first letter of each word in two sentences
and includes punctuation.
Here's the md5 sum:
7de46151e06abe0ad53c4513d22e9a437

Bitplane's post brings to light the element of play in password design. Security is not just a
practical exercise for them. A cat and mouse game is no fun if the cat has no chance. In turn, this

7The MD5 sum is the result of a cryptographic hashing algorithm that transforms some input into a hexadecimal
value. The algorithm is impossible to invert, meaning one can never figure out the input value from the output,
and almost never collides, meaning that a specific output will only map to one specific input. If I thought I had
figured out bitplane's password, I could run my guess through MD5. If the output matches the sum he
provides, I know that my guess was right. Coincidentally, this is exactly how web applications use passwords
for logins. Instead of storing the passwords in a database and directly checking it against the user's entry, they
store the hash values in a database, hash the user’s entry, and then compare the two hash values. This only
works because cryptographic hash algorithms make it almost impossible to find two inputs with the same
hash. For more information about this sort of thing, see the classic introductory text in cryptography, Bruce
Schneier's Applied Cryptography (Schneier 1994).
exemplifies what one could call the poetics of code: the ways in which people treat the formal, technical aspects of Bitcoin as a source of pleasure.

Other posters, however, are fully against using any sort of meaning as a memory aid for passwords. This discourse is often characterized by an absurd escalation of constraint, with strong moral overtones. Vladimir, for example, rejects any possibility of keeping passwords in one’s own memory. Several other posters in the thread recommend using LastPass, a website that allows users to store all of their passwords online. Whenever LastPass is brought up, however, one or two posters will vehemently reject the supposed security of the site. In the words of poster Bitsky, “Anybody who stores his passwords with a 3rd party online service is in a state of sin.”

In 2011, LastPass experienced an unexplained traffic anomaly which, in the worst case, might have been caused by somebody hacking into a database of people's encrypted passwords. This is an instance of how passwords can slip between the online and offline worlds. The hackers could potentially use a dictionary-based attack to decrypt any entries protected by a weak master password, giving them access to all of the passwords stored by that person on LastPass. When somebody brings up this event, a common response is to escalate to suggesting offline password managing software such as KeePass.

Sometimes, the game escalates even further. In a later thread, a poster going by Gareth Nelson writes:

You can generate [passwords] yourself on your own trusted hardware. Take a linux netbook with no internet connection and run uuidgen a few times, memorise some of the results and store them in your brain. If you MUST store passwords outside your

---

8https://blog.lastpass.com/2011/05/lastpass-security-notification.html/
brain, make sure that whatever you use to store the passwords remains on your person 24/7 even while sleeping.

Uuidgen is a command in the Unix operating system that generates a random universal unique identifier (UUID). UUIDs are usually used to identify objects in software because they contain so much entropy that a randomly generated one will practically always be unique. A sample run of uuidgen gave me: 66F0DE3A-B008-11E4-8A2F-3A386D82512D. Memorizing something like this each time one needs a password would be an astounding feat, as other posters quickly bring up. Gareth has a response to these memory concerns:

Go to relentlessimprovement.com, order ortho-mind, alpha-GPC and piracetam. Next, get some pregnolone from healthmonthly.co.uk. Take the above daily and avoid alcohol and bumps to the head while practicing neurofeedback and meditation. Long term memory is EASY to enhance.

Gareth is very active in this thread, attacking any suggestions for passwords with less than “true entropy.” He is not the only person to advocate only storing passwords in one's brain, but he is perhaps the most radical. His position is the farthest one can go in password purity. He both rejects passwords with preexisting mental associations, and he rejects any technological prostheses for password storage. The concern here is with the sticky interface between body and machine. The mind requires meaning while the machine requires entropy. In order to create a condition of perfect confidence, he must alter the workings of his body to fit the workings of the machine.

The Limits of Self-Reliance
Conflict enters these password threads when posters contest the importance of password choice on security. This is usually framed as a recognition of the limits of user control. For example, the very first response to Vladimir's seven rules comes from poster killer2021:
You also have to realize that the complexity of your password doesn't really matter. Why? Because hackers these days get the passwords through other methods (ie. stealing the database and cracking the passwords). The only real thing a complex password protects you from is brute force attack. Bruteforce attack only works if your password is insanely simple or the webserver doesn't ban your ip after 3-4 failed login attempts.

Now I am not saying that your rules are bad. They are good rules to follow. What I am saying is that people need to take more precautions than just making a complex password and thinking they are safe. You need to make it so that even IF a hacker gets into your account that they can't do much damage and that you always have the upper hand.

There is no password one could choose that would be secure if the website's database were compromised. Soon after killer2021's response, the discussion turns towards best practices for web developers to store passwords. As killer2021 explains, “you could have the most complex password ever, but if the website is not secure then you’re screwed.” The conflict becomes what sort of hash function developers should use to store passwords. Are developers at fault for using MD5 instead of SHA-512? Yes, argues nathanrees19: with SHA-512, “each hash will still take ten times longer, and remove a layer of script kiddies who can't be bothered finding cracking tools that support SHA-512.” This is a rare mention of the actual hackers threatening passwords. “Script kiddy” is a derogatory term for someone who doesn't write their own software or find their own exploits, and thus do not deserve the term 'hacker'. Instead, they just download and run one of many 'scripts' floating around the Web, simple computer programs written to attack a specific target. If their script only works on MD5, they would just give up instead of searching for a new one or writing their own.

---

9MD5 and SHA-512 are both cryptographic hash functions: see footnote 1. SHA-512 is considered stronger than MD5. SHA produces a longer hash (meaning brute-force attacks take a lot longer), with less possibility of hash collisions. It's also newer, meaning that there are fewer programs designed to crack it.
Vladimir, the thread's creator, is not happy with the change in thread topic. “Guys, this thread was not intended as educational resource for PHP programmers,” he writes. “It is and the password handling rules are for regular users. How this could not be obvious? Please continue your "how to develop secure web apps" discussion elsewhere.” Vladimir is experiencing the difficulty of keeping a thread focused on a single topic. Message board threads often develop through a flight of associations. Posters respond to each other with anecdotes and opinions often only tangentially related to the previous posts. Occasionally somebody brings up an idea that hits a flash point, leading to a quick succession of closely related posts. More confusingly, multiple dialogs about different things interweave in the same thread, requiring the reader to switch back and forth between contexts. Imagine a diagram of a casual conversation, with topics drifting about, branching outwards, halting, reappearing, and recombining, in a huge variety of speeds and directions. A forum thread, while superficially linear, operates with the same degree of complexity and contingency. The original poster is not the root of a tree, determining the direction of the thread, but simply one node of a network. As such, they have little success when they try to direct thread content. The other posters do not even acknowledge Vladimir's attempt to do so. The free movement of the thread allows an important ideological element of passwords to be challenged: the assumption that people have control over their own security. This can be called the ideology of password optimism.

When killer2021 turns the conversation towards web development practices, he reveals how much trust is involved in web services. When users give a service their data, they have to trust that the developers will keep it safe. In particular, online Bitcoin exchanges have consistently failed to secure themselves against hacker attacks. As poster aral puts it bluntly in a revision of Vladimir's list of advice:
Mt. Gox was a popular online Bitcoin exchange. The day before this thread was posted, a hacker exploited a faulty web form to sneak into a password database. They were then able to retrieve the credentials of a site administrator, and use them to steal thousands of Bitcoins from Mt. Gox's reserves.10 Another poster replies sarcastically to aral, writing “Yes, if you are using bitcoin7.com instead, then you're probably alright,” together with an animated smiley face rolling its eyes. Bitcoin7.com is another online Bitcoin exchange that had been announced on the forum five days earlier. Not surprisingly, in less than two months a hacker attacked the site and stole users' Bitcoins, bringing the exchange to an end. In the context of Bitcoin's crisis-ridden exchange sector, password optimism seems like a feeble reaction to the constant reminders of the breakdowns of and need for trust. Certainly, choosing strong passwords can improve one's security, but this pales in importance compared to the security practices of web developers. In this context, posts about password choice come to be ideological cover for an inherent instability in the Bitcoin economy.

Password optimism has its roots in Cypherpunk, a movement and aesthetic that combines technology boosterism, a love of cryptography, and a concern for privacy and autonomy (Coleman and Golub 2008). A general outline of the cypherpunk project is as follows (Karlstrøm 2014). With communication routed through electronic media, anonymity becomes more and more possible. People can now do and say what they want without the threat of government violence, since their online identity can no longer be linked to their corporeal identity. Of course,

governments do not like this, and try to deanonymize and track actions as much as they can.

Encryption allows each person individually to escape government control, by allowing them to control access to any information they share. Cryptography is the way to bring the fantasies of individualist anarchism to life. Cypherpunks closely link their political goals of privacy with the mechanics of crypto technology. I quote extensively from one influential cypherpunk's manifesto (Hughes 1993):

Since we desire privacy, we must ensure that each party to a transaction have knowledge only of that which is directly necessary for that transaction. Since any information can be spoken of, we must ensure that we reveal as little as possible. In most cases personal identity is not salient. When I purchase a magazine at a store and hand cash to the clerk, there is no need to know who I am. When I ask my electronic mail provider to send and receive messages, my provider need not know to whom I am speaking or what I am saying or what others are saying to me; my provider only need know how to get the message there and how much I owe them in fees. When my identity is revealed by the underlying mechanism of the transaction, I have no privacy. I cannot here selectively reveal myself; I must always reveal myself.

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.

Privacy in an open society also requires cryptography. If I say something, I want it heard only by those for whom I intend it. If the content of my speech is available to the world, I have no privacy. To encrypt is to indicate the desire for privacy, and to encrypt with weak cryptography is to indicate not too much desire for privacy. Furthermore, to reveal one's identity with assurance when the default is anonymity requires the cryptographic signature.

We cannot expect governments, corporations, or other large, faceless organizations to grant us privacy out of their beneficence... We must defend our own privacy if we expect to have any.

The center of cypherpunk's radically individualist project is the ability to control access to information. For the first time, cryptography (seems to) allow us complete control over what information we share. To the extent that they are the most common technique for allowing and
disallowing access, passwords occupy a central role in cypherpunk culture. In particular, Neal Stephenson's seminal cypherpunk novel *Cryptonomicon* is filled with descriptions of password choice very similar to the forum discussions described above.

Password Ideology

The task here is to show how a specific ideological element functions in a specific social context. I argue that password optimism, taken from cypherpunk, comes to play the role of symbol of trustworthiness in the Bitcoin economy. In doing so, it represses the fundamental lack of security. This explains one function of the constant escalation of password security discussed above. If somebody gets their account hacked, one can always say that their password was not secure enough. There is always some higher level of caution they could have taken, and thus always some reason to blame the victim. This fits an ideological system based on individual responsibility. Security becomes a purely individual goal, but since the ideal of individual security is never attainable, the focus will never shift to a scale larger than the individual. This ideological move can even escalate to reject online exchanges entirely, and see any other security flaw as the victim's responsibility. As one frequent poster writes in a password thread, “Thank Goodness that you can do all your Bitcoining offline. If you don't have enough sense to protect your computer from hacking... well, it's your own fault.” The Bitcoin economy itself is thus completely saved from criticism.

The role of password ideology becomes obvious in one thread when a user posts a list of hacked passwords from Mt. Gox. The complexity of the passwords immediately confuse other posters.

Some of the cracked passwords look pretty secure. Like
1036 ... ccFy7KpgN
How did that get cracked? Was that one of the unsalted ones?
1938 ... BESys*t3M
This seems like it should be secure, even though it is leetspeak.
1955 ... RYL4McGT
Again, unsalted? How was this cracked?
13434 ... djcnbimil99332k
I think this was is too far down to be unsalted, and it is too long for rainbow tables. Is it following a pattern I don't see?
13449 ... n833bgva
This looks secure enough to me. How are these getting cracked? How much time does it take?

People expect that the hackers would have cracked the passwords using a ‘rainbow table’. This is a table of precomputed partial results of the brute-force algorithm. Using a rainbow table saves a significant amount of time if the attacker is trying to crack a large number of passwords at once. This is because the password search does not have to redo calculations that are already done in the rainbow table. Rainbow tables run into two problems. First, because of space limitations they only work on passwords of up to a certain length. Second, they are easily defeated by ‘salting’ the passwords in the database. Salting a password means adding a randomized value so that each password is hashed differently. The randomized ‘salts’ are then stored with the encrypted passwords. Because each password is hashed differently, an attacker would have to compute a new rainbow table for each password.

How did the hackers crack these passwords, if not with a rainbow table? If long, complex passwords are not enough to ensure security, then password optimism is harder to maintain. Another forum user soon finds a solution, posting that “the fact that a password is in this list doesn’t imply that it was cracked… the complex passwords were probably stolen by some other means – e.g. phishing – and happened to be reused.” Phishing is a type of attack in which a hacker pretends to be someone trustworthy to steal a password. Phishing attacks are fairly easy to avoid – just avoid clicking on email links – so the consensus is that their victims must be
somewhat primitive.\textsuperscript{11} One poster replies, “Hmm, so someone who uses the password "7XiBKeJe5ochSqVW" has been phished?” It is unbelievable that someone smart enough to use a complex password (one of us) would also be stupid enough to be a phishing victim (one of them).

What a puzzle! Thankfully, the Internet age makes sleuthing a lot easier. Another poster quickly looks up the victim on Facebook. “He's an older guy whose activities include singing, sailing, barefoot hiking, etc. No evidence of computer expertise. The complex password was a false sense of security, and he was phished, in all likelihood.” The victim does not fit their image of a tech-savvy, security-conscious person. He was unsuited to using Bitcoin in the first place due to his age and hobbies. By extension, all of those users with complex passwords were still not doing enough to ensure their security. If they were skilled enough their passwords would not have been cracked.

This thread exemplifies how password ideology functions in a time of crisis. The feeling of untrustworthiness slips away from the Bitcoin economy and even the specific web service. It comes to rest on the victims of the crisis, who become individually responsible. The ritual of password choice is a way of feeling part of an elite for whom Bitcoin will always be secure. Password choice is so effective in this role because of its cathetic nature. People are willing to invest their identities and emotions into their passwords. They write their own poems to put into passwords. They medically alter their bodies to better store passwords. They incorporate their surroundings, their locations, and their emotional associations into passwords. Password choice

\textsuperscript{11} In reality, anybody could be a victim. When I visited Google’s Silicon Valley offices – headquarters of the tech \textit{ubermenschen} – there were notices posted all over with advice on how to avoid being phished. It only takes one unguarded moment to give up a password to a deceptive website.
threads even have a dramatic conflict, between the attack algorithms of hackers and the memories of ordinary folk. All of this explains why such a seemingly small technical detail takes up so much space on the forum.
Chapter 4: Bitcoin's Non-Political Economy

At one point, the website of the Bitcoin Foundation, Bitcoin's foremost advocacy group, listed the three “core principles” of Bitcoin: “non-political economy, openness and independence.” While the phrase “non-political economy” sounds strange, it is an apt description of one goal of many Bitcoin advocates: the end of the involvement of the state in the economic sphere. This is itself a political move, concerned with the reconfiguration rather than the end of politics. However, there is a great variety of political positions that Bitcoin advocates can take. I wish here to identify and describe one strain of Bitcoin politics. This is the radical strain, which takes Bitcoin to be inherently subversive of the State.

A taste of the radical perspective and its clashes with other positions comes from a BitcoinTalk thread posted with the topic “How many of you still believe bitcoin will free you from paying tax one day?” The original poster, a forum Senior Member going by cuddaloreappu, starts the thread with an anguished post about Bitcoin's opposition to taxes.

Is this dream even still alive?
regulated exchanges are popping up..
mining is increasingly becoming centralized!
every idea that created bitcoin seems to fade away.
back the dream was in a world where you could buy or hire anything in bitcoin, the government will never be able to prove your wealth you own in bitcoin and thereby you need not pay taxes or pay them little and keep all your wealth yourself!
Thereby, the hard to earn wealth that you earned with hard work is all yours!

But if this was true by now, some few millions from the trillions kept in Swiss banks should have flown into bitcoins market cap!

He then asks the forum whether they still have hope that Bitcoin will end taxes. However, the immediate responses are hostile. Other posters dispute that avoiding taxation was ever one of Bitcoin's founding goals. "It was only ever a dream in the minds of those who didn't understand what bitcoin provides and what governments demand," writes user DannyHamilton in a long response. "I've been reporting income and paying the taxes on everything that I earn from bitcoin related activities since I started." Many of these posters point out that Satoshi Nakamoto, Bitcoin's inventor, never advocated the end of the state. They separate the technology of Bitcoin from the political goals that radicals have for it:

"Bitcoin is not about paying or avoiding tax whatsoever. It's about an independent, worldwide form of money and payment infrastructure, that no longer depends on trust (in some authority or middle man, like a bank, who thus has enormous power over our money) but on cryptographic proof."

The debate comes down to just how incompatible Bitcoin is with the state. Forum posters on one side believe that Bitcoin does not mean the end of taxes, and that its promise is in preventing states' and banks' control of the money supply. Posters on the other side believe that Bitcoin promises the complete end of the state.

These concerns put Bitcoin in the company of radical movements of all sorts that struggle with the question of how much compromise is acceptable. Among Marxists, Lenin's pamphlet on Left-Wing Communism exemplifies the problem. The Russian Revolution, he writes, was endangered from two sides. On the right, there were the "opportunists", who were too willing to work with existing structures in order to gain in the short term while giving up the long-term revolutionary struggle. On the left, there were the "petty-bourgeois revolutionists", whose
unwillingness to compromise drove them to anarchism. “The two monstrosities complemented each other”, as revulsion against opportunism lead people to revolutionism, and vice versa (Lenin 1920). The lesson for Communist parties is to work in the parliaments and reactionary trade unions, but not compromise too much! This meant parties had to stake out a firm middle ground so they could avoid both “left-deviationism” and “right-deviationism”.

A second example comes from psychoanalysis. Freud recognized a tension between the medical goal of transforming “misery into common unhappiness” and the subversive theoretical orientation “to change other social factors so that men and women shall no longer be forced into hopeless situations” (quoted in Turkle 1978:142). In analogy to political movement, the first could be called 'reformist' and the second 'revolutionary'. The subversive core of psychoanalysis, argues sociologist Sherry Turkle, is its recognition that the individual is not the center of itself (ibid: 233). Society does not intrude into an integral individual. On the contrary, society is always necessarily inside the individual. In the United States, psychoanalysis fell towards the medical side of the dichotomy, with ego psychology appealing to an autonomous “I” as ally in medical cure. The opposite occurred in France. Following Jacques Lacan, French psychoanalysis theorized a radically decentered self, produced by a grand social structure: the symbolic order. Lacanian psychoanalysis emphasized the subversive aspects of Freud, even questioning the very notion of a cure. This 'French Freud' had a close connection with political radicals, while the 'American Freud' “drew people away from politics toward a search for personal solutions” (ibid: 225).

Bitcoin is in a similar situation, with reformists on one side and revolutionaries on the other. In drawing the analogy to Marxism and psychoanalysis, I don’t wish to positively identify a single revolutionary aspect of Bitcoin, nor to make value judgments about it. Instead, using this
perspective means asking how the disruptive or subversive aspects of Bitcoin are socially constructed. More precisely, in a specific field, what ideas about Bitcoin get marked as incompatible with the existing order? How does this demarcation occur, and what are its consequences?

A blog post by software designer Oleg Andreev exemplifies an oppositional construction of Bitcoin. I choose this post because one very active user, jonald_fyookball, posts a link to it in the thread described above. In doing so, he marked a turn in the thread from reformist statements to the emergence of revolutionary statements. Andreev starts his article by stating that “Bitcoin and State do not go together at all. Neither logically, nor economically” (Andreev 2014a). What is interesting about his argument is that he does not attempt to show that Bitcoin is good, or that the state is bad. Instead, he tries to drive a wedge between the two in order to close off the possibility of a reformist Bitcoin politics. If one accepts his argument, any usage of Bitcoin includes the overthrow of the state as goal or consequence. In Lenin's terms, this repudiates opportunism because it is impossible to give up the long term goal for a short term gain.

Mining Trust

Andreev constructs the opposition between Bitcoin and State by identifying trustlessness as a subversive aspect. His argument positions the state as a technical entity. For Andreev, “State is a hierarchical construction of “trusted third parties” (TTPs). In theory, some social interactions may involve a conflict that may be resolved by a trusted third party (arbiter). In a nation state it is ultimately some government agency (e.g. a cop)” (2014a). TTP is a cryptographic term for an entity that verifies some interaction between two people. Andreev is not just drawing an analogy between the state and a cryptographic technique. The state literally is a set of techniques through
which people associate. As such, problems of governance are technical problems which software engineers can solve.

For cryptographers, explains anthropologist Christopher Kelty, “the very use of the word “trust”... has less to do with the kind of people assumed to be untrustable – criminals, pirates, hackers or any other ostensible reasons for the existence of so-called computer security – and much more to do with the way in which asymmetric cryptography itself is authenticated” (Kelty 2005:137). When they deal with trust, they deal with technical problems. In turn, this creates an exteriority of trust that cannot be dealt with by the algorithms. For example, when cryptographer Bruce Schneier discusses certificates, he brings up a complex issue: “What is the meaning of certification? Or, to put it another way, who is trusted to issue certificates to whom?” However, he calls these questions “noncryptographic” (Schneier 1994). Bitcoin revolutionaries depart from the scientific discourse by refusing to draw this boundary. This involves speaking the political in cryptographic terms.

In addition to technologizing the political, Andreev politicizes technology by taking the Bitcoin protocol as a matter of political concern. “Bitcoin is an attempt to remove some trusted third parties from the equation,” he writes (Andreev 2014a). “That is all sorts of financial institutions including government regulators. From the Bitcoin perspective, it is a moral hazard to enable control over money supply and monetary flows to a hierarchy of trusted third parties.” What does it mean for Bitcoin to have a perspective? Bitcoin isn't just a piece of software here, but an epistemic object constantly open to new significations. Andreev uses one such signification when he refers to “the idea of Bitcoin”: “If you support the idea of Bitcoin, you acknowledge the hazard of entrusting the entire economy to trusted third parties” (ibid). In this phrase, Bitcoin is simultaneously the object and manifestation of the idea. This specific
totalization takes libertarian economics to be the essence of Bitcoin. With these two paragraphs, Andreev shows that the political state is essentially technical and Bitcoin is essentially political, dismantling the opposition that Bruce Schneier put forth between 'cryptographic' and 'noncryptographic' issues.

Radical discourse opposes Bitcoin to the State by obviating trust. Obviation means simultaneously to dispose of and to make obvious: "a process of innovation that is simultaneously analysis and reanalysis; in making new relationships through its overlaying or eclipsing of others, it continually mines new meanings, analyses, and realizations out of its initial configurations" (Maurer 2005:61). Bill Maurer links obviation to Alfred Hitchcock's cinematic device of the McGuffin, "the object that is seemingly of no consequence and is often forgotten, and yet drives the plot forward by compelling novel associations" (ibid). Maurer finds that two principles, similitude and exchange, act as McGuffins in discussions of alternate currencies.

The politics of Bitcoin uses trust as a McGuffin. Starting as a specific technical term – as in "trusted third parties" – trust leads the narrative into the ethical issues of sovereignty and state power. "So if you support the idea of Bitcoin...," Andreev continues, "you acknowledge that the ultimate power must be spread thin among every single participant and never be entrusted in hands of a few, even if it's a democratically elected government... But if you acknowledge the hazard of TTPs, then what arguments are left for any other government activity? Government is the ultimate trusted third party to resolve disputes in the entire economy" (ibid). Bitcoin requires no trust in the cryptographic sense. In Satoshi Nakamoto's original paper introducing Bitcoin, this just means that it is impossible to reverse a transaction (2008). Bitcoin imports the benefits of cash into the digital realm by simulating materiality (see Maurer, Nelms, and Swartz 2013). However, Bitcoin radicals mine a political configuration out of cryptographic trust by making an
associative leap to political power. This political configuration valorizes distributed power, power “spread thin.” Representative democracy is not enough.

There are strong shades here of the Austrian School economist Friedrich Hayek, whose proposal for denationalizing money is strongly influential on discussions of alternative currencies. “It is wholly impossible for a central bank subject to political control... to regulate the quantity of money in a way conducive to a smoothly functioning market order” (Hayek 1976:89). The market must be protected from political interference, and thus from people’s interference. Note that neither Andreev’s nor Hayek’s arguments refer to “freedom.” On the contrary, as Fredric Jameson points out, the market for the Austrian School plays the authoritarian role of Hobbes’ Leviathan: “market ideology assures us that human beings make a mess of it when they try to control their destinies... and that we are fortunate in possessing an interpersonal mechanism – the market – that can replace human decisions altogether” (2012:290). Leviathan becomes a set of distributed protocols, the market, along with other distributed protocols such as the Internet and Bitcoin.

Trust in Value
The concern with trust dates back to the creation of Bitcoin. When Satoshi Nakamoto initially posted on the forums of the P2P foundation announcing his development of the system, trust was his major concern:

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. Their massive overhead costs make micropayments impossible. (Nakamoto 2009)
The three main worries referenced here are inflation, bank runs, and transaction costs. The trust that the central bank will not print too much new currency, leading to inflation, is basically trust in the value of the currency. The trust that banks will hold enough in reserve to survive a bank run is trust in access to one's own money. This can also be seen as a problem of the value of credit money, as opposed to cash money. The third worry, that of transaction costs, is a problem of the technologies of mediation involved in payment.

Compare this with the language regarding trust in Nakamoto's actual paper:

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party. (Nakamoto 2008)

The problem of trust slips away from broad confidence in the value of currency to the narrow trust involved in the actual action of payment. This corresponds only to the third point of the forum post, that of technologies of mediation. The need for trust in the value of cash, as in his previous worries about inflation, is completely elided. The last sentence of this passage makes out Bitcoin as little more than a transposition of physical currency into the digital realm. These two different explanations of the (lack of) trust involved in Bitcoin mirror two different narratives of the currency: the radical political one and the moderate technological one.
A couple of scholars have attempted to show that trust is still necessary for the use of Bitcoins. Instead of completely removing the trust in human institutions, Bitcoin replaces this form of trust with another “based on the supposed infallibility of machine code” (Karlstrøm 2014:31). Karlstrøm shows that the technologies that give rise to Bitcoin are materially embedded both in the infrastructure of the Internet and the processes of technical invention. This challenges the discourses of Bitcoin that sees its technology as asocial and apolitical. On the other hand, some aspects of Bitcoin are relatively out of human control: no-one can change the rate at which coins are mined, for example, or forge counterfeits. As writes Maurer, “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” (Maurer, Nelms, and Swartz 2013:264).

It is important to understand what exactly the “work” of Bitcoin is here. The essence of the Bitcoin code is that it simulates materiality very well. Like gold, Bitcoins require work to produce and cannot be duplicated. Unlike gold, they are extremely easy to transfer and store. Because of these properties, Bitcoin has given rise to a semiotics of “practical materialism” in which the code securing its materiality is also seen as securing its value (Maurer, Nelms, and Swartz 2013:262). Trust thus slips back in the other direction, from technique to value. The fact that Bitcoin’s secure code has done nothing to stem its volatile exchange rates is ignored or explained away.

Endgame

The oppositional construction of Bitcoin gains force in Andreev’s political futurology. Bitcoin and the state are not just (ideo)logically opposed, but economically opposed. The state only exists because it can pay for itself, he writes. This revenue comes from two sources. First, it comes from the government’s control of money:
If needed, money is just being “borrowed” from the government’s puppet bank under promise to repay the debt (with interest!) from the extracted taxes (or by borrowing even more from the same place). When the state wants to go to war, enormous amount of money can’t be just extracted and is being printed. Extra money flows into markets, prices go up, business plans get messed up, people’s savings get destroyed and they lose their jobs at the same time. But we are at war, so folks are better to work harder “for the children” and maybe even join the army (you lost your job, after all). (Andreev 2014a)

This is very similar to Hayek's argument for the denationalization of money (Hayek 1976). Even (and especially) democratic governments cannot be trusted with the money supply because they will necessarily cause inflation.

Second, revenue comes from taxation on businesses that use the banking system. People will naturally try to avoid taxes, but unfortunately “the banking system is all heavily licensed and cooperative with the state” (Andreev 2014a). The only businesses that can avoid taxes now are those that use cash. However, “with Bitcoin banks are not necessary. Bitcoin allows you to trade with anyone on the entire planet with near-zero costs. More businesses would bypass banks and as a side effect, more businesses would be able to withhold their taxes from the state. Competition would force other businesses to drive their costs down the same way. Bitcoin will become a black hole that grows and attracts more and more people in it” (ibid). As the adoption of Bitcoin inevitably accelerates, the government will become unable to find funding for itself. Government officials will want to be paid in Bitcoin as it is now the default consumer currency. Governments cannot just print Bitcoin as they can fiat money, so they can only get it from taxation, which is now impossible. “So if Bitcoin continues to grow, the nation state would peacefully dissolve... At some point we will witness a critical mass of supporters that no one will be able to stop. And then there will be no state anymore” (ibid).
This narrative exemplifies many of the revolution stories that gather around Bitcoin. The revolution starts off gradually, but accelerates quickly as people are forced to use Bitcoin by market pressures. Eventually, a “critical mass” is reached at which it cannot be stopped. At this point the state finds itself outdated and impotent, and gracefully collapses. Bitcoin radical Cody Wilson even gives this a Hegelian spin by referring to “the total sublation of the state” (Feuer 2013). It is not easy to take Andreev’s version seriously. His statements on the untaxability of Bitcoin are particularly dubious. However, the specific logic of this narrative brings up important aspects of Bitcoin’s political mythology.

The transition to Bitcoin does not follow the traditional models of political change. Instead, people think of it in terms of other technological changes. This model is similar to what Raymond Williams calls “technological determinism”, in which “new technologies are discovered, by an essentially internal process of research and development, which then sets the conditions for social change and progress” (Williams 1975:13). Technological determinism posits a break between technology and society. A specific technology comes about by independent progress, but then its inherent properties frame the development of society. In another blog post, Andreev compares Bitcoin to the Web:

Bitcoin economy is not a revolution in a sense of violent redistribution of wealth in a “fairer” manner. It is a leap forward by forgetting about how much was destroyed or stolen and focusing on how much can be preserved and protected. It’s a truly peace-making tool for the whole humanity. People who think about Bitcoin as only a money-moving tool, or a get-rich-quick scheme grossly underestimate it. It enables much more than what the web gives. The web gives us freedom to exchange information. Bitcoin gives us freedom to exchange everything. (Andreev 2014b)

The technology of Bitcoin has several inherent properties that radically change society, in his view. His reference to the Web calls to mind optimistic discourses that view the Internet as a
public space for the exchange of information, allowing democratization. Bitcoin is much more than this for Andreev. Like the Web, it is a decentralized information sharing protocol. However, the information it shares takes the form of trustworthy money. Free digital transactions through Bitcoin are particularly important because they will alter the economic sphere as well as the cultural sphere.

Labeling Bitcoin politics as technological determinism still does not account for the intensely political dimension of technological development. The development of open source wallets, applications, and protocols for Bitcoin is often a passion project. Oleg Andreev leads several such projects. In technical posts, both on developers' blogs and the BitcoinTalk forums, people recognize that this technological development is necessary for their political project, and that technological development has its own motivations. “Bitcoin will be adopted only if it can be used as safely as conventional money and banks,” writes Andreev.13 “We need a long-term strategy for easy to use, yet very robust way to store arbitrary amounts of bitcoins so more people can jump on it and make investors rich.” Bitcoin holders have an interest in making the currency more widely used both to bring about political change and to increase the value of their own stash. Recognizing these motivations conflicts with the determinist narrative, found in political discourse, which distinguishes a clear interior and exterior to technological development. The Bitcoin revolution no longer looks so inevitable.

Trust in Crisis

The same subversive aspects of Bitcoin that people have constructed as its political strength cause a structural weakness in the Bitcoin economy. Again, one can make analogy to

psychoanalysis. Associations of psychoanalysts are bound together by the same libidinal mechanisms that psychoanalysis claims to study. According to Sherry Turkle, “Since a successful analysis dissolves such investments and liquidates the transference to the analyst in the analysis itself, psychoanalysis may face an internal contradiction similar to that faced by anarchism. It may subvert all structures, including its own” (Turkle 1978:120). This problem was particularly salient to Lacanian schools, which emphasized lack of hierarchy in the training and organization of psychoanalysts. French psychoanalytic associations were subject to constant schism as a result (ibid). The ways in which Bitcoin's political discourse obviates trust creates a similar contradiction. To the extent that any market requires trust, replacing “trusted third parties” with anonymous distributed protocols creates instability in the Bitcoin economy.

This problem is most obvious in dark web markets. The “dark web” or “hidden internet” is a part of the Internet that is not accessible to standard browsers. To access it, one needs to use The Onion Router (Tor), software that allows untraceable communication by bouncing requests randomly around a distributed network of relays. Tor uses multiple layers of encryption, nested like the layers of an onion, to guarantee anonymity online. Like Bitcoin, it does away with trusted third parties by using a distributed protocol for security. The affinity between Tor and Bitcoin manifests itself in hidden online marketplaces like Silk Road, where users can exchange Bitcoins for drugs and other illicit commodities.

These marketplaces allow people to buy and sell stock without government interference. However, as political scientist Henry Farrell describes, the anonymity of Tor and Bitcoin undermines the trust required to make transactions (Farrell 2014). Without much knowledge of the identity of sellers, buyers are under constant threat of being scammed. Farrell quotes one commenter on the Hidden Wiki, a directory of dark web services:
I have been scammed more than twice now by assholes who say they're legit when I say I want to purchase stolen credit cards. I want to do tons of business but I DO NOT want to be scammed. I wish there were people who were honest crooks. If anyone could help me out that would be awesome! I just want to buy one at first so I know the seller is legit and honest. (ibid)

Just like the need for institutional coherence forced Lacanian societies to compromise their egalitarian ethics, the crises of scams forced Silk Road to build up a bureaucracy. However, even measures like ratings systems and bans could not fully ensure trust. Transactions could not be fully anonymous, since people had to give mailing addresses to receive drugs. As a result, each seller had a list of names of all of their customers:

If any reasonably successful dealer leaked the contact details for users en masse, customers would flee and the site would collapse. And so, when a Silk Road user with the pseudonym FriendlyChemist threatened to do just that, [Silk Road founder Ross] Ulbricht did not invoke Silk Road’s internal rules or rely on impersonal market forces. Instead, he tried to use the final argument of kings: physical violence. He paid $150,000 to someone whom he believed to be a senior member of the Hells Angels to arrange for the murder of his blackmailer. (ibid)

Farrell speculates that the assassin was himself a scammer associated with FriendlyChemist. While impossible to verify, it would not be surprising. When posters on Bitcoin forums bring up the hit-men offering their services on the dark web, the consensus is that they are all scams.

Silk Road collapsed when its founder Ross Ulbricht was arrested. As I write this, one of its replacements is also in crisis. The Evolution marketplace has fallen to an exit scam, in which its two founders stole over twelve million dollars’ worth of Bitcoins held in escrow. The first notification of the scam comes from a Reddit thread on the DarkNetMarkets subreddit.14 An

---

14See https://www.reddit.com/r/DarkNetMarkets/comments/2zeuxo/complaintwarning_evolution_admins_exit_scamming/. A 'subreddit' is a particular community on Reddit. Any user can create and post to a subreddit.
Evolution staff member posts a warning that the founders, Kimble and Verto, had frozen withdrawals and prepared an exit strategy. “I can't fucking believe it, absolute scum. I am giving this warning to you all as soon as I possibly could of. Confronted Kimble and Verto about it, they confirmed it and they're doing it right now...” This thread is a fascinating look into the politics of black markets on the deep web. One highly popular response is from a user called DeepThroat_, giving an overblown threat with a cryptographic signature.15

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512
There is more going on here then meets the eye. Thats all I'll say for tonight, but I will put this message out there (and MANY, MANY in this community can vouche for me. /u/lamoustache for one)
TO VERTO/KIMBLE: What you have done is despicable. Didn't think I was serious about our discussion? Okay. It's nearly 9PM on the US West Coast. You've got 24 hours (and that is being generous) to make this right and re-open the market, and allow people access to their funds. Once that time passes - my crystal ball starts talking and unless you've changed identities and moved, you will be FUCKED. Moderators please do not delete this. I will not doxx anyone (even these pieces of shit here). They've got 1 chance. The sub will filter posts talking about PMs, therefore, those who want Verto, Kimble and cohorts heads on a spike, get in touch. Rethinking your stunt, boys?
-----BEGIN PGP SIGNATURE-----
iQlcBAEBCgAGBQJVCPrEAoJEKU+LnLvKq4hARWk [...] 
-----END PGP SIGNATURE-----
EDIT: Realized I should have signed this. Just did.
EDIT2: Here's my answer to your private offer to "do business": Fuck You.
```

15Reddit allows users to upvote or downvote comments. The number of upvotes that a comment gets is a rough measure of how popular it is. DeepThroat_'s post had almost 400 net upvotes, the highest of any in the thread.

16To “doxx” someone or “drop doxx” is to release their real identity to the Internet. Doxxing is against Reddit’s site rules, and would lead to DeepThroat_'s comment being deleted and him being banned. This leads him to a contradiction, in which he simultaneously promises not to doxx the scammers and offers to give their doxx to anyone who sends him a private message (PM).
EDIT3: Thieves attempting to either intimidate or buy me off. Answer is still fuck you.

It is unclear what he is threatening, but some posters are certain that it is serious:

Hunting them down and killing them? Torture? I dunno. A lot of vendors have a bit more real life power than we give them credit for. Remember the hells angels being involved with the alleged DPR murder for hire shit?

The “DPR murder for hire shit” refers to the Silk Road situation that Henry Farrell described. Ross Ulbricht went by the pseudonym “Dread Pirate Roberts”, or DPR.

Other posters are much less impressed. One person replies with a reminder that the supposed Hell's Angel was probably a fake, “some geek in his mom's basement who managed to scam DPR for close to $1 million.” Many responses have a mocking tone, as a popular comment from user klklj234 exemplifies:

this is some ultimate internet toughguy shit.
theyre going to get away with what they did the same way every other bitcoin scammer gets away with it. you have literally no power to do anything to them. i can smell the food caught in your neckbeard from here.

'Neckbeard' is a general insult on Reddit for a nerd, someone with poor grooming habits who takes the Internet too seriously. DeepThroat_ is a neckbeard because he talks tough on the Web but can do nothing in real life.

Klklj234 expresses the sense of futility that the endless succession of Bitcoin scams engenders. The lack of institutional safeguards in the underground Bitcoin economy leaves only one hope for justice: vigilante violence from powerful criminals. Even this hope seems hollow when surrounded by fake assassins and Internet toughguys. Unsurprisingly, nothing has come from DeepThroat_’s threat. His last posts are angry responses to those who disbelieve him: “I am genuinely losing patience with your idiotic posts. What the fuck do you want? Are you dense?...
Literally, damned if I do, damned if I don't. So how about this? I WON'T. I will do NOTHING. I will speak to nobody, I will not shed light on ANYTHING to ANYONE.\textsuperscript{17}

For Bitcoin radicals, the "idea of Bitcoin" is to build an alternative economy apart from state control. Bitcoin tries to replace centralized trust with a distributed protocol, a non-hierarchical network of algorithms that ensures security through cryptography. In distributing the Leviathan, Bitcoin operates in parallel with other projects of decentralization: the Internet and the 'free market'. Adam Smith famously wrote about the market system that "it is not from the benevolence of the butcher, the brewer, or the baker that we expect our dinner, but from their regard to their own interest" (Smith 1937 [1776]). In the same way, it is not out of trust in a centralized authority that we recognize Bitcoin transactions, but out of the protocological imperatives of network nodes. However, the radical discourse of Bitcoin is constantly butting against the realities of economic life. A long line of sociologists have shown that markets do not arise naturally from individual calculation. Economic production and exchange require processes of framing and rationalization before capitalist calculation can even enter the picture (Weber 1930 [1905]; Durkheim 1984 [1893]; Simmel 2011 [1900]). Crisis results when the subversive aspects of Bitcoin challenge or exclude these processes.

This does not mean that radical Bitcoin's opposition to the state is futile. I have not discussed the role of the state in crushing deep web markets. If the sellers on Silk Road or Evolution did not have to worry about state coercion, surely many of the problems described

\textsuperscript{17}A final note about this situation: the DarkNetMarkets subreddit is one of the most prominent forums for discussing online drug sales. It's also completely open for anybody to see. The only security measure possible is the use of a pseudonym, but this is not foolproof. Ten days after the scam, the Department of Homeland Security served Reddit with a subpoena for the identities of DeepThroat\_ and four other posters in the thread (Greenberg 2015).
above would disappear. However, radical Bitcoin still has an internal contradiction insofar as it proposes to replace trust entirely with anonymous distributed networks. This tension would not go away with the sublation of the state, and it is destructive of Bitcoin's attempt to build an alternative alongside the state. It is not fatal, though. Trustlessness and trust can exist side by side, as shown by an anecdote that historian Finn Brunton told me. At a libertarian gathering Brunton went to, a shopkeeper had left his wares unguarded as he went for a smoke. He left a sign: “Bitcoin is a trustless currency. But we trust you.”
Conclusion

Bitcoin is still in its early days, but it could die at any moment. There are currently too many problems with the Bitcoin economy – those of security and value – for it to become a lasting currency solution. Nonetheless, Bitcoin is a fascinating case study in the history of money. I hope this thesis conveys some of the intensity of the discussions around Bitcoin. The currency brings together powerful concepts of the value of money; the trustworthiness of government; the importance of anonymity; and the need for security.

The need for trust is a particularly important plot device in the drama of Bitcoin. Bitcoin users want to be absolutely sure that their money is what it says it is and does what it says it does. They have much to fear from thieving hackers and intrusive governments. What they want goes beyond pragmatic confidence towards an ideal of perfect, mathematical certainty. Satoshi Nakamoto gave them a mathematical proof that Bitcoin ‘works’, in a very narrow sense (2008). Barring a 51% attack, nobody will ever be able to reverse a transaction. Yet Bitcoin users often come up against crises of trust that fall outside this narrow ledge of certainty.

In the case of theft by hackers, Bitcoin users simulate mathematical certainty through practices of password choice. They seek ‘pure entropy’ for their passwords: a state of absolute meaninglessness which will allow them to avoid hackers. Combined with an ideology of self-reliance, the discourse of password choice protects the institution of Bitcoin from criticism regarding insecurity. The concerns of trust also show themselves in the radical politics of Bitcoin. Its adherents believe that Bitcoin’s cryptographic certainty gives it revolutionary potential. The distributed protocol of Bitcoin will entirely replace ‘trusted third parties’ such as the state or financial institutions. When this happens, we will achieve the cypherpunk goal of an
anonymous, anarchic public sphere. However, these very ideals contribute to weaknesses of the Bitcoin economy.

The study here is still cursory. I focus on very specific themes and sites of Bitcoin discourse. The limits of method, scope, and time prevent me from commenting on some important questions. For example, just how global is Bitcoin? People often present it as a post-state and post-national currency. Bitcoin breaks down barriers of distance and difference by providing a single, neutral protocol for the sharing of money. I have shown that the protocol is in fact far from neutral. Users and developers link it with specific political and economic standpoints, on trust for example. These concerns might be local or ethnocentric in nature. Cypherpunk, for example is a United States phenomenon, more specifically bound to Northern California (Coleman and Golub 2008). Proponents of the type of technological libertarianism that spawned Bitcoin try to make it seem global. They refocus on dissidents in repressive regimes and people suffering through currency crises. Critics, on the other hand, tend to localize it, referring to the “Califomian Ideology” or the “creationist capitalism” of Silicon Valley (Barbrook and Cameron 1996; Boellstorff 2010; Ruckenstein 2010).

To take it for granted that Bitcoin is global would be to buy too far into its ideology. As of now it is mostly the concern of technological elites in the global North. The only people who get paid in Bitcoin are the true believers who work for Bitcoin organizations. Living this way requires a lot of social capital (to find people who will take the currency) and financial capital (to withstand the huge value fluctuations that the currency goes through) (Kirby 2013). Nonetheless, there are other ways in which Bitcoin is global. An example is the process of mining. Much of this takes place in China, where cheap electricity and parts make mining more profitable. It is
difficult to study these mining operations since they are so secretive.\textsuperscript{18} Nonetheless, the globalization of mining is a matter of political economy that affects and underlies the discursive aspects I have described here.

Gender is another form of difference that Bitcoin discourse both represses and makes apparent. I have not discussed a question that comes up occasionally on the BitcoinTalk forum: why are so few women into Bitcoin? The ranks of Important Bitcoin Figures are filled with men, and the male gender is default in Bitcoin discussions. It is a basic fact of modern societies that technology is coded as male. Nonetheless, feminist scholars of technology have shown through studies of domestication and coproduction that the relationships of technology and gender is complex and dialectical (Bray 2007). Does Bitcoin have a space for women? One possible strategy for answering is to trace the tacit genderings of Bitcoin's utopic imaginaries. Another is to explore the potentials of technology in reconfiguring the household and economy.

In closing, I would like to defend the value of ethnography as a way to study Bitcoin. My use of topic modeling software certainly inspires the possibility of quantitative methods here. While topic modeling is not yet anywhere near precise enough to quantify trends with, other data processing methods could be helpful. For example, two economists have recently used Google Trends data to study the motivations for interest in Bitcoin (Wilson and Yelowitz 2014). They find no support for politics motivating Bitcoin use. These methods are tempting because they have a much broader reach than the close readings I rely on in this paper. Studying discourse on a particular web forum, as well as its connections to other sites of cultural production, may not

\textsuperscript{18}A Vice documentary from this February gives a short glimpse into one of these massive secretive mining operations. View it at http://motherboard.vice.com/read/chinas-biggest-secret-bitcoin-mine.
reveal much about why the majority of people use Bitcoin. However, qualitative, interpretive study is still necessary to understand Bitcoin as a cultural phenomenon. Part of the proof of this is historical. The forum users I study articulate the very same concerns that motivated Satoshi Nakamoto and his cryptocurrency predecessors. It is undeniable that the political discourses of trust are a major and visible aspect of Bitcoin's presence. These discourses are complex, contradictory, and above all unorthodox. It is important to study them closely, with an anthropologist's eye, to draw out their nuances.
Works Cited

Abolafia, Mitchel


Andreev, Oleg


Back, Adam


Barbrook, Richard, and Andy Cameron


BitcoinTalk Forum


Blei, David


Boellstorff, Tom


Bollier, David

Bray, Francesca


Brito, Jerry, and Andrea Castillo


Burrell, Jenna


Carruthers, BG, and Sarah Babb


Castells, Manuel


Cheney-Lippold, John


Churchill, Elizabeth F, and Elizabeth S Goodman


Coleman, E. Gabriella


Coleman, E. Gabriella, and Alex Golub

Dai, Wei


Defoe, Daniel

1710 An Essay upon Public Credit. London.

Deleuze, Gilles


Downey, Greg, and Melissa Fisher


Durkheim, Emile


Faris, David, and Patrick Meier


Farrell, Henry


Feuer, Alan


Galloway, Alexander R.


Garcia, David, C Tessone, Pavlin Mavrodiev, and Nicolas Perony

Gladwell, Malcolm


Goodin, Dan


Graeber, David


Greenberg, Andy


Hart, Keith


Hayek, Friedrich


Helleiner, Eric


Helmreich, Stefan

Hofstadter, Douglas


Hughes, Eric


Humphrey, Caroline


James, William


Jameson, Fredric


Jones, Graham M., and Bambi B. Schieffelin


Juris, Jeffrey


Karlstrøm, Henrik


Kelty, Christopher


Kirby, Carrie

Knuth, Donald


Latour, Bruno


Lee, Benjamin, and Edward LiPuma


Lenglet, M.


Lenin, Vladimir


Lessig, Lawrence


LiPuma, Edward, and Benjamin Lee


MacKenzie, Donald


MacKenzie, Donald, and Juan Pablo Pardo-Guerra

Mager, Astrid


Manovich, Lev


Marcuse, Herbert


Maurer, Bill


Maurer, Bill, Taylor Nelms, and Lana Swartz


Mauss, Marcel


Mazzarella, W.

Mirowski, Philip


Morozov, Evgeny

2009 The Internet: A Room of Our Own? Dissent 56(3): 80–85.

Muniesa, Fabian


Nakamoto, Satoshi


O’Reilly, Tim


Papacharissi, Zizi A.


Pardo-Guerra, Juan Pablo


Pare, Daniel

Peck, Morgen E.


Polanyi, Karl


Rajan, Raghuram G.


Řehůřek, Radim, and Petr Sojka


Ruckenstein, Minna


Sassen, Saskia


Schneier, Bruce


Seaver, Nick


Shirky, Clay