

Algorithmic Authority: The Case of Bitcoin

Caitlin Lustig
University of California, Irvine
clustig@uci.edu

Bonnie Nardi
University of California, Irvine
nardi@uci.edu

Abstract

In this paper, we propose a new concept for understanding the role of algorithms in daily life: algorithmic authority. Algorithmic authority is the legitimate power of algorithms to direct human action and to impact which information is considered true. We use this concept to examine the culture of users of Bitcoin, a crypto-currency and payment platform. Through Bitcoin, we explore what it means to trust in algorithms. Our study utilizes interview and survey data. We found that Bitcoin users prefer algorithmic authority to the authority of conventional institutions, which they see as untrustworthy. However, we argue that Bitcoin users do not have blind faith in algorithms; rather, they acknowledge the need for mediating algorithmic authority with human judgment. We examine the tension between members of the Bitcoin community who would prefer to integrate Bitcoin with existing institutions and those who would prefer to resist integration.

1. Introduction

Algorithms have always been a crucial part of software development—they are “the fundamental entity with which computer scientists operate” [16]. Beyond just shaping the behavior of software, algorithms play a critical role in shaping societal and individual behavior. David Beer argued that with the Web 2.0, software became ubiquitous and participatory, which gave algorithms “the capacity to shape social and cultural formations and impact directly on individual lives” [8]. An example of the increasing power of algorithms in everyday life is Google’s PageRank algorithm, which influences the information users have access to and what they judge to be true [19]. The role of algorithms in shaping human behavior can also be observed in technologies of heteromation, which are characterized by their use of humans as integral “computational components” to

augment software algorithms. An example of heteromation is Amazon Mechanical Turk, in which “humans [are] rendered as bits of algorithmic function” [12]. In such systems, human beings are subordinate to algorithms, which function as employers. We call the emergent dynamic between algorithms and human actors “algorithmic authority”. Algorithmic authority is defined as *the trust in algorithms to direct human action and to verify information, in place of trusting or preferring human authority.*

In order to explain the concept of algorithmic authority, we will first define the two parts of the phrase. Algorithms are defined as “logic + control” [22]. They are simultaneously a set of abstract instructions (logic) and possibilities for action (control). Goffey argued that “[a]lgorithms do things, and their syntax embodies a command structure to enable this to happen” [16]. Algorithms are given authority to not only “do things” to software, but they cause human actors to respond accordingly. We draw from Weber for our definition of authority. He described authority as power that is perceived as legitimate, without coercion, or threat of violence [34].

We turn to Gambetta’s definition of trust to understand what it means to trust in algorithmic authority: “trust (or, symmetrically, distrust) is a particular level of the subjective probability with which an agent assesses that another agent or group of agents will perform a particular action, both *before* he can monitor such action (or independently of his capacity ever to be able to monitor it) *and* in a context in which it affects *his own* action” [13]. Algorithms generally have desired outcomes, such that savvy users can predict the algorithm’s outcome. They can trust that the software will behave in a certain way and act accordingly in response. Thrift stated that “software is best thought of as [...] an expectation of what will turn up in the everyday world” [31]. Software can shape our expectations and understanding of the world, but Thrift argued that while its effects are visible, the relationship between the inputs to the software and the exact mechanisms used are largely invisible, creating a sort

of “technological unconscious”. Users may trust in software because they may find that it has some level of predictability, but they are vulnerable to the invisible effects of software.

While our definition of algorithmic authority is unique, we distinguish our use of the phrase algorithmic authority from Clay Shirky’s. In a blog post, Shirky described algorithmic authority as “the decision to regard as authoritative an unmanaged process of extracting value from diverse, untrustworthy sources, without any human standing beside the result saying ‘Trust this because you trust me.’” [6]. Shirky uses Google’s PageRank algorithm as an example of how information can be generated automatically and trusted by most people as “legitimate”. Our use of the term algorithmic authority is broader. We argue that algorithms are given authority to not only decide which information is true, but to also direct human action.

In this paper, we examine what kind of trust people put in algorithms, what it means to trust in algorithms, and how users mediate algorithmic authority with their own personal judgment and the judgments of other, trusted people. We examine these questions through a qualitative study of Bitcoin, a crypto-currency that on June 15, 2014 had an exchange rate of \$562 USD to one bitcoin [3]. We chose Bitcoin as an example of algorithmic authority because it is not managed by governments or banks, but by algorithms. The main Bitcoin algorithm that we will refer to is the blockchain, a mechanism for producing the currency and verifying transactions. In this paper, we follow the convention of Bitcoin users by referring to the system as Bitcoin and the units of currency as bitcoin.

2. Background

Bitcoin was developed in 2008 during what has come to be known as the Great Recession. This financial crisis led to significantly higher rates of unemployment as well as lower wages for those who were still employed [9]. Overall, Americans were pessimistic about stock market and housing prices [18]. In 2009, 48% of Americans reported that they felt angry that the government was “[b]ailing out banks and financial institutions that made poor financial decisions” [4]. During and subsequent to the Great Recession, growing discontent with governments and capitalism led to the popularization of protest movements such as the Occupy movement [32]. Occupy protesters argued that the current way in which liberal democracies function is deficient [27].

Like members of the Occupy Movement, many Bitcoin users are drawn to the currency because they wish to disrupt traditional institutions. To understand

what it means to “disrupt” an institution, we turn to Schumpeter’s definition of “creative destruction”, i.e., that which “incessantly revolutionizes the economic structure from within, incessantly destroying the old one, incessantly creating a new one” [30]. Bitcoin is appealing to users because it not only provides an alternative to fiat currency, but because users believe it can transform governments and economic systems.

Bitcoin was first introduced in the whitepaper “Bitcoin: A Peer-to-Peer Electronic Cash System” by Satoshi Nakamoto [26]. It is widely believed that Satoshi Nakamoto is a pseudonym for the person or persons who created Bitcoin. Nakamoto’s motivation for creating a new type of currency was based on the shortcomings of electronic commerce using conventional currencies. In his seminal paper on Bitcoin, Nakamoto argued that electronic commerce is flawed because it has high transaction fees and affords consumers less privacy than cash transactions.

According to Nakamoto, the methods taken to prevent *double spending* are the main cause of the shortcomings of electronic commerce. Double spending refers to spending money in one online purchase, and then quickly making another purchase with the same money. To prevent double spending online, trusted third parties must verify transactions for merchants. However, these third parties charge transaction fees, which limit the types of transactions that are feasible by making micro-transactions prohibitively expensive. Third parties can also reverse transactions when there is customer fraud. While a third party’s ability to reverse transactions protects customers from identity theft, it also puts merchants at risk of losing money. In order to gain some level of trust in their customers, merchants must acquire information about their customers to confirm their identity. Consequently, consumers are unable to conduct anonymous or private transactions. Nakamoto argues that, “[t]hese 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” [26]. In response to these issues, Nakamoto designed Bitcoin to solve the issue of double spending without mandatory transaction fees or loss of privacy.

Nakamoto created Bitcoin as a currency and payment platform that is *pseudo-anonymous*, *supports micro-transactions*, and *has no inherent transaction fees*. Bitcoin has the same affordances as cash, but in a digital format. While cash typically relies on a government to regulate it, Nakamoto’s system relies on a distributed and decentralized user base to give it value through consensus and artificial scarcity—two concepts that are ingeniously tied together in Bitcoin’s implementation. The user base forms a peer-to-peer

network that keeps a public, pseudo-anonymous ledger of all transactions. This ledger is called the *blockchain*. When a transaction is made, the Bitcoin software running in the background on peers' computers use calculations to verify that the money has not been double spent by comparing it against this ledger. In order to incentivize users to run this software, there is a random chance that the user will be rewarded new bitcoins for completing a calculation. Bitcoin users refer to the generation of new bitcoins as "mining" bitcoins. When bitcoins are mined, the verified transactions are put into the blockchain.

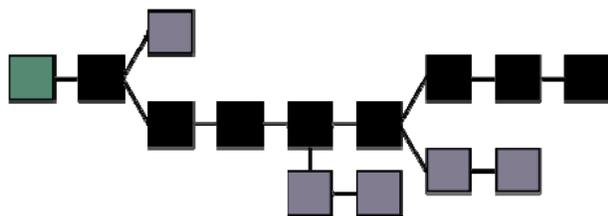


Figure 1: A graphical representation of the blockchain mechanism. [1]

The blockchain mechanism has been described as “the main innovation of Bitcoin” [1]. Through the blockchain, verified transactions are bundled into blocks that are made a part of the public ledger. These blocks are connected to each other through the use of hash algorithms, which cryptographically generate a unique value to represent each block. Every block contains the hash of the previous block in order to indicate its position in the blockchain. In the case that two or more blocks are mined within a few seconds of each other, the Bitcoin client software may be unable to determine which block should come next in the blockchain. In this situation, the blockchain creates a fork. Whichever branch of the fork is longer becomes a part of the main blockchain and the other branches are discarded. In Figure 1, the longest chain is shown in black and the other branches are unused.

The mining process serves as a way to control the growth rate of Bitcoin and eliminates the need for a centralized agency to distribute the currency. The code of Bitcoin dictates that there are 21 million bitcoins that can ever exist. As of June 15, 2014 nearly 13 million bitcoins had been mined. Bitcoin is designed such that on average, a block of bitcoins will be mined every ten minutes. Every four years, the number of bitcoins that are mined in each block goes down by 50%. Currently, 25 bitcoins are mined in each block. In 2017, the number of bitcoins in a block will be reduced to 12.5. Users have calculated that by the year 2140 all Bitcoins will have been mined. Most users who mine bitcoins pool together their resources and join a “mining pool”. Every time the pool mines bitcoins, the

coins are distributed in proportion to the amount of processing power that the miner contributed.

Bitcoin is hardly the first modern widespread alternative to fiat money, but it is the first to capture the public's attention. Bitcoin has been compared to two previous alternative currencies, Liberty Dollars (1998-2009) and e-gold (1996-2009). Liberty Dollars was shut down because the currency was in direct competition with and closely resembled the US dollar [17]. E-gold was shut down due to the corporation's lack of licensing as a “money transmitting business” and its inconsistently enforced policies against illegal activity. Unlike these currencies, Bitcoin is commonly characterized as being in a legal gray area. Because of Bitcoin's decentralized nature, it may be harder to shut down, as there is no central organization to prosecute. Unlike e-gold, there is no infrastructural mechanism to determine the identities of users ([17], [21]).

3. Related Work

Crypto-currency is an emergent area of study and consequently there is little research on the Bitcoin user base. As Bitcoin has gained more popularity a number of news articles have been written on the currency, but many focus on illegal activity conducted by Bitcoin users. Few academic articles explore Bitcoin from a social or theoretical perspective. A notable exception to this is Maurer et al.'s research, which examined the Bitcoin user base. They argued that Bitcoin users place their trust in Bitcoin's code to produce and distribute bitcoins correctly, as opposed to trusting a government or a central organization to do so [24]. One reason for this trust is the transparency of Bitcoin's code—users trust the code because of “their collective ability to review, effectively evaluate, and agree as a group to changes to it”. Maurer et al. argue that users can trust the code because of “the fact that such decentralization, as well as the public-key encryption of users' identities, is hardwired into the system”. Bitcoin is designed to prevent corruption, and consequently, users find the system more trustworthy than institutions such as governments and banks.

Mallard et al. build on Maurer et al.'s argument and suggest that trust in Bitcoin is distributed through several socio-technical mechanisms, one of which is the underlying algorithms of Bitcoin's code, in particular because it is a peer-to-peer system [23]. To use a peer-to-peer system, users must actively participate by pooling together resources, which builds trust. Users also trust in the resilience of peer-to-peer networks and trust in Bitcoin's core developers.

Other papers that discuss the behavior or ideals of Bitcoin users have largely utilized analyses of the

blockchain to learn about the aggregated behavior of Bitcoin users (e.g. [25], [28], [29]). Some researchers have taken a historical look at the ideas that influenced Bitcoin's design ([7], [11]).

4. Methods

This study consisted of two phases: a survey and a series of interviews. We also engaged in participant observation and actively read Bitcoin blogs, forums, and articles. Our findings in this study were derived using Grounded Theory methodology [15]. We did not begin with the theory of algorithmic authority, rather we developed it after analyzing our data.

We posted an exploratory survey of 36 questions on BitcoinTalk.org (326,031 users) and /r/Bitcoin, the Bitcoin subreddit (122,561 subscribed users) in October, 2013. We selected these forums due to their popularity and reputation among Bitcoin users. The purpose of the survey was to develop a better understanding of attitudes of the Bitcoin community. The survey was comprised of Likert scale questions to assess study participants' reasons for using Bitcoin; open-ended questions for topics such as anonymity, government regulation and the future of Bitcoin; and multiple-choice demographic questions. At the end of the survey participants had the option of leaving their email address so that they could be later contacted for an interview. Out of the 510 survey participants, 124 left their email addresses.

We used the data collected from the survey to craft interview questions based on the themes that emerged from the responses. From the survey data, we noted that participants had diverse views on the future of Bitcoin and government regulation of Bitcoin. We used exploratory and semi-structured interviews to learn more about the diversity of views on those issues, and we iteratively refined the questions based on previous interviews. We contacted a third of the survey participants for interviews in waves until over twenty participants agree to be interviewed. We did not contact survey participants who left short answers or did not answer a large number of questions. All interviewees were male; no women offered to be interviewed. We interviewed 22 participants from March, 2014 to May, 2014. Participants were given the option of being interviewed over any medium they wished: email, instant messaging, Skype, telephone, or in-person (if possible). Eight participants chose voice or video communication, three participants selected instant messaging, and 11 participants chose email.

All participants have been anonymized in this paper; any names used for interview participants are fictitious, with the exception of Frankenmint, a

participant who requested that he be identified by his online moniker, which was derived from how he took his "first hosting PC of spare parts to make it and it minted bitcoins with the assistance of miners." Original orthography and punctuation have been preserved for participants who communicated over instant messaging and email.

Over the course of this study, we systematically read Bitcoin forums and blogs from November, 2012 to the present, to immerse ourselves in the Bitcoin community. We primarily read posts on the website Reddit, a popular social networking and news website which consists of "subreddits"—smaller boards devoted to a specific topic. The forum and blog posts we read focused on the latest Bitcoin news, technical details of Bitcoin's implementation, and political economic theory. We also read mainstream news articles in order to understand the popular perception of Bitcoin users. Prior to the shutdown of the black market Silk Road (which utilized Bitcoin for payment) in October, 2013, news articles tended focus on illicit uses of Bitcoin. Since the shutdown of Silk Road, articles in mainstream media have taken a more serious look at how Bitcoin can be used.

We found that throughout this study Bitcoin users reached out to us—many were interested in the results of the research. Some participants sent links to articles or images they thought we would find interesting. One Bitcoin user even gave the first author a generous gift on Reddit for appreciation of our survey—0.05 bitcoins. At the time this was valued at around \$8 USD, but at the time of writing this paper, it is worth \$32.50 USD. This gift mirrored traditional ethnographers' experiences of receiving gifts from members of the communities they research.

5. Findings

Our findings examine the reasons Bitcoin users turned to algorithmic authority, and the ways in which that authority was mediated by human judgment. Our findings reveal some of the tensions and complexities of algorithmic authority. Participants demonstrated the difficulty in determining whether an algorithm is political or apolitical, promoting resistance or reifying institutional hegemony, centralized or decentralized. These binaries were further complicated by the difference in how Bitcoin users wanted the currency to function and the ways in which it was actually used.

Some Bitcoin users saw algorithms as apolitical and incorruptible tools that they preferred over existing institutions. However, participants also argued that human oversight and judgment were necessary for Bitcoin to function smoothly. Many participants argued

that existing institutions—the very ones that they rejected—needed to support Bitcoin for it to gain widespread adoption. While a number of participants indicated that widespread adoption would ultimately be positive for Bitcoin, some were concerned that this adoption would cause Bitcoin to become like the very institutions they opposed. For participants who raised these concerns, the authority of cryptographic algorithms was decoupled from the authority of Bitcoin, and they said that they would start using another crypto-currency if Bitcoin became centralized.

5.1. Demographics of Bitcoin

Our survey participants were predominantly American (51%), male (96%), heterosexual (92%), atheist or agnostic (74%), libertarian (60%), and between 25-34 years of age (50%). 63% had bachelor or graduate degrees. 44% self reported making more money than the average person in their country.

Table 1: Demographics of Bitcoin

<i>Gender:</i>	
Male (96.29%)	Female (2.09%)
Other (1.86%)	
<i>Sexual orientation:</i>	
Heterosexual (92.42%)	Other (4.27%)
Bisexual (3.55%)	Homosexual (2.13%)
<i>Religion: (participants were allowed to pick multiple options)</i>	
Atheist (47.75%)	Agnostic (33.81%)
Christian (17.97%)	Other (11.11%)
Buddhist (6.86%)	Jewish (2.13%)
Muslim (1.42%)	Hindu (0.95%)
<i>Self-reported income:</i>	
higher than national average of participant's country (44.71%)	around the national average of participant's country (27.40%)
less than national average of participant's country (27.88%)	
<i>Education:</i>	
Less than a high school degree (2.11%)	High school degree or equivalent (7.28%)
Some college but no degree (23.24%)	Associate degree (4.69%)
Bachelor degree (35.92%)	Graduate degree (26.76%)
<i>Age:</i>	
18 to 24 (18.82%)	25 to 34 (50.12%)
35 to 44 (21.41%)	45 to 54 (6.82%)
55 to 64 (2.35%)	65 to 74 (0.24%)
75 or older (0.24%)	
<i>Political beliefs: (participants were allowed to pick multiple options)</i>	
Libertarian (59.25%)	Moderate (36.25%)
Anarchist (27%)	Left-wing (25.25%)
Green (18%)	Socialist (11%)
Right-wing (8.25%)	Communist (2.50%)

Participants' political beliefs were varied. Many chose multiple political labels for themselves out of the eight that were provided, i.e., anarchist, communist, green, left-wing, libertarian, moderate, right-wing, and socialist. 53% of participants selected more than one label for an average of 1.87 labels per participant. For those that selected at least one political label, 59% selected libertarian. However, an open-ended question

about political beliefs showed that many participants had differing opinions about what these labels meant.

Survey participants came from 48 countries. The countries with more than 1% of the participants included: US (51%), Germany (7%), UK (6%), Canada (6%), Australia (4%), Netherlands (2%), Sweden (1%), Finland (1%), Norway (1%). There were 84 participants in 39 other countries, each with less than 1% of the participants. Of the 22 interview participants, 13 were from the US, two from Australia, two from Germany, one from Argentina, one from Canada, one from Croatia, one from India, and one American expatriate in China.

5.2. Algorithms are more trustworthy and authoritative than existing institutions

In this section we examine the reasons algorithmic authority was preferred over the authority of existing institutions such as governments or banks. We argue that for many, using Bitcoin was an act of resistance against institutions they felt had failed them. Beer argued that “algorithms are carving out new complex digital divides that emerge in unforeseen and often unnoticed ways in the lives of individual agents” and that it will be difficult to identify and research the ways in which people resist these algorithms [8]. However, in a reversal of Beer's concern, in this section we explore the ways in which *algorithms can explicitly and visibly act as resistance* to institutions.

Some Bitcoin users were drawn to the currency because of their dissatisfaction with current economic practices, particularly with how governments can print out money at will, causing inflation. One survey participant explained, “*Since we couldn't elect officials to be fiscally responsible and reign in the Federal Reserve, I actually have the freedom now, and means to preserve my savings and wealth through a non-inflationary currency. Everything else attractive about bitcoin is a bonus.*” Another survey participant stated that he liked Bitcoin because it “*is the convergence of technology (open source, p2p, cryptography) that is really going to change the world for the better and the more people that know about it the sooner we can get away from a debt based inflation run economy.*”

For participants who felt disenfranchised by governments and banks, Bitcoin offered an alternative. One participant, Terry, spoke about his distaste for banks. He had worked at a bank for years, and felt that banks did not act in the best interest of the people: “*I felt like I could punish the bank because I was able to write down finance charges and late fees and I was able to change interest rates.*” Tom, a participant who was particularly concerned with government

corruption, argued that fiat currency is coercive and violent: “*People can at last choose a form of money that isn't controlled by an entity which will shoot you if you misuse it.*” These participants lived in places such as the United States and Canada where they felt that the infrastructure was functional, but did not align with their morals. For these participants, Bitcoin was financial freedom from the forces governing fiat currency, which they felt that they had little to no control over, even in the case of Terry, who worked for a bank. Bitcoin, on the other hand, despite all of its technical complexity, gave the participants the feeling of being in control because of its transparency.

For some participants, Bitcoin was not just a technology of resistance, but also fulfilled practical needs. Franco, a participant in Argentina, explained that in his country, the official exchange rate between US dollars and Argentinian pesos was much worse than the black market exchange rate. He was employed by an American company and asked to be paid in bitcoins rather than US dollars in order to avoid dealing with either type of exchange. Roy, an American living in China, explained that his use for Bitcoin was based on getting around government restrictions: “*One of the best uses I've found for it is that it's the easiest way for me to get money from China into my American bank account. China has strict capital controls and foreigners can only send something like \$500 USD out of the country per day.*” For these participants, Bitcoin was not just a method of resistance, but also a way to cope with institutions that were unable to meet practical needs.

Some participants viewed Bitcoin as more trustworthy than governments because they considered Bitcoin an apolitical project. They considered the algorithms that govern Bitcoin incorruptible and impartial. Tom said, “*The cool part is, that the functionality of the software isn't political. It's concrete. Therefore, accurate information corroborated by the code will eventually filter out to the public at large. You can't politicize a lie based on verifiable facts forever. All you can do is temporarily create a lie meme that propagates, and take advantage of it before it gets destroyed by the rational types.*” Tom was referring to how although malicious users could spread misinformation for their own gain, Bitcoin is governed by an algorithm that, with time, would allow the misinformation to be countered by the authority of the code. Gillespie makes a similar argument in his essay “The Relevance of Algorithms” when he says, “That we are now turning to algorithms to identify what we need to know is as momentous as having relied on credentialed experts, the scientific method, common sense, or the word of God” [14].

Algorithms are replacing institutions that have historically been viewed as impartial and apolitical.

5.3. Algorithmic authority is mediated by human judgment

In this section, we explore the ways in which Bitcoin’s decentralized algorithmic authority required trust in a number of human actors. Participants preferred algorithms to institutions, but they argued that Bitcoin itself and third party Bitcoin services require human oversight. Users used their own judgments to take precautions to prevent theft or falling victim to scams. These kinds of human mediation suggest that the judgment of individuals is a necessary supplement to algorithmic authority. We use the term “mediation” to refer to Activity Theory’s definition of mediation. Mediation is the ways in which humans use technology as a tool to act out their desires and intentions in the world [20]. However, algorithmic authority reverses this concept and uses human judgment as a tool for algorithms to act on the world. In this section, we will explain the main ways in which human judgment supplemented Bitcoin’s algorithms.

In the absence of any formal centralized human authority, we found that Bitcoin users have to spend time and effort to discern which instances of human authority are legitimate. Most of the interview participants reported frequently spending 2-3 hours a day reading up on Bitcoin or communicating with other Bitcoin users. Jonathan, a participant who no longer felt that he had time to spend on Bitcoin, explained that Bitcoin could be time consuming because, “*First, it's complex and takes a while to understand. Then it is the constant revolutionary language—everything is about to change in an instant, so you keep checking in to witness that instant. You are (or one is) constantly waiting for your small holdings to make you rich.*” While many explained that they enjoyed keeping up with a technology that changed so rapidly and enjoyed communicating with other Bitcoin users, they also needed to be informed so that they could learn who to trust, how to protect their bitcoins from theft or fraud, and what community interventions were necessary to help Bitcoin itself run smoothly.

A notable example of when human mediation would have prevented a disaster occurred in February, 2014. The largest Bitcoin exchange market, MtGox, shut down suddenly and filed for bankruptcy in Japan. Bitcoin users who had been storing money on the exchange’s server lost their bitcoins. The closure was notable because MtGox, founded in 2010, was handling 70% of *all* Bitcoin transactions by 2013 [33]. The owners of MtGox claimed that \$480 million USD

of bitcoins had gone missing [10]. Participants argued that MtGox should have had more organizational oversight. Frankenmint directly addressed the issue of human mediation, commenting: *“I think that Mark [the CEO of MtGox] did have a leak of coins in the Gox system, and refused to put the expertise together to have the exchange algorithm better regulated by humans. He blamed malleability instead of his systems which lacked human verification. His organization was beyond incompetent, in my opinion.”* Ken, who had a large mining operation and was an active user of alternative crypto-currencies, stated, *“I also feel bad for the people who trusted Gox and didn't understand the implications of that trust.”* Earlier in this paper, we defined trust as the ability to reasonably predict the actions of other actors. While MtGox did have codified rules of operation, a number of participants stressed that the world of Bitcoin was quickly evolving.

While MtGox required organizational oversight, participants also considered individual judgment to be important. Most had at some point been scammed out of bitcoins or had made an investment that was not successful. Participants observed that with enough experience and time, it was not difficult to tell which services were trustworthy and which were scams. One participant said, *“If you want to know the most recent news about Bitcoin you have to spend a lot of time on it, but for the average consumer that's not really important.”* Users learned to look for services that were transparent and kept users informed. Frankenmint stated, *“I believe honesty and integrity are the most important as the community demands trust. There have been too many failed ventures and screw-ups, Mt Gox, simply being the largest quandary so far. ...2nd, having knowledge and being willing to share it with others [makes one perceived as more trustworthy].”*

Another area for human intervention was in preventing theft. Participants argued that new Bitcoin users had difficulty understanding how to keep their bitcoins safe, and that users would have to “relearn” how to protect their money. Lawrence, a participant who was quite active on Reddit, hoped that *“[a]s more people get involved, they will learn quickly what is necessary to secure their bitcoins. Hopefully these same practices will carry over to other services, which can bring exposure on proper security to other users, therefore making it less intimidating when/if they checkout bitcoin.”* Participants viewed this knowledge as something that had been culturally lost in an age in which transactions can easily be reversed and credit card companies will warn customers if their algorithms detect that the customer's identity has been stolen.

It was not just Bitcoin-related software that needed human judgment and intervention—Bitcoin users have had to step in to prevent Bitcoin itself from facing

serious problems. When version 0.8 of the beta Bitcoin client software was released, most *miners* upgraded to the latest version, but most *users* did not. Because of a change in the code, the 0.8 software recognized a block of transactions that the 0.7 software did not. This discrepancy caused the two different versions of the software client to use different chains of transactions. A prominent member of the Bitcoin community, Vitalik Buterin, noted that to make sure that everyone used the same blockchain, the “mining pool operators came together on IRC chat” and decided that they had to intentionally cause a 51% attack in order to resolve the fork [2]. A 51% attack is launched when the entity with a majority of computing power in the Bitcoin network chooses to manipulate the blockchain for their own purposes. Buterin pointed out that this “attack...was seen by the community as legitimate.” According to Buterin's argument, Bitcoin users saw this temporary assemblage of centralized power as more legitimately authoritative than Bitcoin's algorithms, which they had to “attack”.

Some participants saw centralization of human resources as a necessary evil. For example, some participants felt that the Bitcoin Foundation was necessary for Bitcoin to be taken seriously. The Bitcoin Foundation is the unofficial public face of Bitcoin in the United States, and interfaces with the American government to help shape the laws that govern Bitcoin. One survey participant said, *“Don't really like [the Bitcoin Foundation], but it is good to have some “legitimate” group trying to advance bitcoin interest in the political sphere. Their actual influence on bitcoin is pretty limited so that can't do much harm.”*

5.4. Algorithms need institutional support

Participants argued that the greatest barrier to the use and adoption of Bitcoin was lack of third party support. Many participants did not actively use Bitcoin, and for those that did, it was largely as a symbolic gesture in support of Bitcoin. To gain wider support, participants felt that Bitcoin must be seen as a legitimate and reputable currency. As we noted earlier, legitimacy is a requirement for authority. While participants felt that Bitcoin was legitimate, they found that they sometimes had trouble convincing others of this. One participant told us that he tried to give away bitcoin to people who he thought might find it compelling and they almost always refused him.

This issue of legitimacy and expanded authority is important because without it, participants were limited in what they could do with Bitcoin due to poor institutional support for the currency. Participants reported that brick-and-mortar stores that accepted bitcoin were few and far between. As a result, many

Bitcoin users amassed bitcoin with the expectation that they could use them in the future when they hoped that Bitcoin would be integrated into other institutions, either through laws or third-party applications.

A significant minority of participants (30% of survey participants) said that they were not necessarily opposed to some government regulation of Bitcoin. Participants gave two main reasons for this. First, they wanted Bitcoin to be recognized as a “legitimate” currency by mainstream society, which meant distancing Bitcoin from illegal activity. Second, they felt that regulation would make it easier for Bitcoin to be used with existing institutions. One survey participant said, *“Regulation is important in the financial sector. Bitcoins need to be able to be transacted without fear of criminal exploitation. This requires an empowered authority to prosecute fraudsters and other financial criminals. Anarchists will dispute any government intervention, but without established trust no market can succeed. Bitcoin cannot continue to be ‘the Wild West currency’ and also succeed in the long-term.”*

Because Bitcoin supports pseudo-anonymous transactions, it has been used as a currency of digital black markets, the most well known being the now defunct Silk Road. However, most participants were adamantly against using Bitcoin for illegal purchases; they felt that it would undermine Bitcoin’s legitimacy in the eyes of the greater public and governments. One survey participant said, *“People who have no idea what bitcoin is will be able to see that for example, Silk Road may be a bad thing (expressed by mainstream news sites), but then the Bitcoin Foundation pops up on their google search and maybe shows them that the bitcoin isn't just about drugs and illegal activities.”* Another participant, Terry, said that he did not try Bitcoin when he first heard of it because he thought it was only used for illicit purposes.

Similarly, some participants were cautious about identifying with the libertarian label because they felt it might seem extreme. For example, Ken said, *“I consider myself a libertarian, but I think that word gets abused a bit.”* Simon, a Bitcoin investor, had similar views: *“I think sometimes the very extreme libertarian perspectives will be detrimental to mainstream adoption and turn people off [...] I've been finding myself more sympathetic to liberaterian [sic] views, but I prefer to keep a level head”*. Lawrence expressed concern about how other users represented Bitcoin: *“I also like to think of myself as policing bitcoin's reputation. /r/Bitcoin is an important resource for people starting out or researching bitcoin. We do not need to come off as delusional.”*

A subset of users were concerned that the integration with existing institutions might

fundamentally change what Bitcoin means in a broader social context, and change how it is used. Keith, a participant who had written white papers on future uses of the blockchain and similar technologies, argued that Bitcoin will eventually evolve into the same centralized capitalist institution that many Bitcoin users oppose. He said, *“It only means we can have perhaps some time where it's decentralized until the arms race results in a sort of king/queen of mining [...] it's similar to what happens with capitalism where you end up with big businesses, then mega business, then just a few businesses who control everything. Bitcoin will develop in a similar way until a few businesses control every aspect of it. So it's about always innovating and always having different altcoins [other crypto-currencies] in competition.”*

For many participants, it was not Bitcoin that they had high hopes for, but the blockchain algorithm that Bitcoin employed. They stated that Bitcoin might not exist in the future, but they believed that cryptocurrencies would endure in the future. One survey participant argued, *“Even if Bitcoin isn't ‘the one’, it—or whatever comes after it—will change how we use/what we think about money forever.”* Alternative crypto-currencies were a divisive issue in the Bitcoin community; many participants felt that altcoins were unoriginal clones of Bitcoin that diluted the authority of Bitcoin. For these participants, the authority lay with Bitcoin itself. But for participants who feared that Bitcoin would become subsumed by a culture they rejected, alternatives were essential, and the blockchain algorithm itself was what held authority.

6. Discussion

We found considerable variance in how participants viewed the currency. It is not our goal to state which views of the participants were “correct”, but rather to demonstrate the ways in which an algorithm can still have authority over users who interpret the purpose and functionality of the software in a multiplicity of ways. Of particular interest were the different notions of what it means to trust in Bitcoin’s algorithmic authority. Trust in an actor comes from being able to predict how that actor will behave, something that is particularly easy to predict when users have an understanding of the open-source code of a project like Bitcoin, but much more difficult to predict when it comes to opaque, large institutions.

This notion of trust in Bitcoin’s code was expanded on by Andreas Antonopoulos, the Chief Security Officer of blockchain.info, in his article, “Bitcoin Security Model: Trust in Code” [5]. He says that the most important feature of this new model of

trust is that, “[n]o one actor is trusted, and no one needs to be trusted. [...] Trust does not depend on excluding bad actors, as they cannot ‘fake’ trust. They cannot pretend to be the trusted party, as there is none.” According to Antonopoulos, as long as over half of the computing power is controlled by what Nakamoto referred to as “honest nodes”, the decentralized and aggregated computing power of the network can be trusted. Users do not need to trust any other individual user in order to trust in Bitcoin, but they do need to trust the network as a whole. This concept of trust suggests that Bitcoin is a heteromated system, in which it is *essential* for human actors to offer their computing power to the system, in order to make the system trustworthy.

A similar perspective on trust was offered by Maurer et al. who argued that, “Bitcoin is [...] all about trust—about eliminating the need to trust governments and corporations and about learning to trust the Bitcoin algorithm instead” [24]. Maurer et al. do acknowledge the power of the network in regulating code, but emphasize that users ultimately trust the underlying code that manages the network.

We found that Bitcoin users had a more nuanced view of this trust than either of these theories might suggest; they recognized that it is not enough to just trust in the code. Bitcoin’s code was subject to change and on rare occasions it had serious errors (such as the issue with the 0.8 version of the software). Furthermore, although users may have placed authority in the code, as Maurer et al. suggested, or in the network, as Antonopoulos suggested, algorithms were unable to tell users whether to trust a specific vendor or whether to update their software right away.

It could be argued that trust in vendors is a different issue than trust in Bitcoin. However, without the involvement of third party vendors and services, Bitcoin does not have substance. Participants lamented the difficulties in using bitcoin for practical purposes—the most practical uses were for participants who needed it as an international means of exchange, but few used it for regular transactions. Therefore, trust in Bitcoin requires trust in more than just the code or network, but also trust in different related services.

Trust in algorithms refers to not just the algorithm itself but the uses of the algorithms. Participants found that determining whether they could trust third party applications and services took an extraordinary amount of time because they could not defer judgment to institutions. For passionate users of Bitcoin, this extra effort to determine trust may not be a significant drawback, but for other users, Bitcoin may only become appealing once social norms and regulations create a centralized method for determining trust.

We propose that algorithms are not just constituted by computer code, but also by the actors who are necessary for the algorithm to run smoothly. Without the Bitcoin developers, the Bitcoin miners who process transactions, and the judgments of Bitcoin users, Bitcoin would cease to function. The same is true for other technologies that use algorithms to manage users—without the users there would be no algorithmic authority. Therefore, when we consider this emergent trend towards using algorithms which have great influence over both the invisible everyday and the explicit actions of users, we must consider the relationships between the code, the users, and the institutions that support the application.

7. Conclusion

In this paper, we examined the concept of algorithmic authority and discussed the ways in which Bitcoin users trust in the code and in their own judgment. We found that algorithmic authority does not just reside in code, but in a diversity of sociotechnical actors. However, it is still unclear how this authority should be distributed and utilized. We found that our participants were of two minds about the potential algorithmic authority of Bitcoin. One group hoped that Bitcoin would provide a new disruptive authority with its blockchain mechanism, and all that it enabled for many possible applications. The other group felt that Bitcoin is only valuable to the extent that it is utilized and integrated into existing institutions. Participants concerned with Bitcoin as a disruptive technology saw the distribution of algorithmic authority across different sociotechnical actors as problematic. For them, the appeal of Bitcoin was based on utopian visions of a technology unhindered by centralized institutions. For these users, the blockchain algorithm was at the heart of the disruption; Bitcoin itself was just one application of the blockchain. The diversity of alternate crypto-currencies based on the blockchain algorithm provides the heterogeneity needed to continue promoting the utopian visions of Bitcoin users if Bitcoin fails to live up to their expectations.

Future research is needed to better understand the ways in which algorithmic authority can best be used to empower users. As Bitcoin evolves, more research will be needed to understand the relationship between the centralized institutions so many of its users oppose and the decentralized algorithmic authority of Bitcoin.

8. References

[1] https://en.bitcoin.it/wiki/Block_chain

- [2] <http://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/>
- [3] <https://coinbase.com/charts>
- [4] <http://www.pewresearch.org/daily-number/bailing-out-banks/>
- [5] <http://radar.oreilly.com/2014/02/bitcoin-security-model-trust-by-computation.html>
- [6] <http://www.shirky.com/weblog/2009/11/a-speculative-post-on-the-idea-of-algorithmic-authority/>
- [7] Barok, D., "Bitcoin: Censorship-Resistant Currency and Domain Name System to the People", *Piet Zwart Inst.*, 2011.
- [8] Beer, D., "Power through the Algorithm? Participatory Web Cultures and the Technological Unconscious", *New Media & Society*, 11(6), 2009, pp. 985-1002.
- [9] Blendon, R. and Benson, J., "America's Response to a Deep Recession", *Challenge*, 52(4), 2009, pp. 32-52.
- [10] Dougherty, C. and Huang, G., "Mt. Gox Seeks Bankruptcy after \$480 Million Bitcoin Loss", *Bloomberg*, 2014.
- [11] DuPont, Q., "The Politics of Cryptography: Bitcoin and the Ordering Machines", *Journal of Peer Production*, 4, 2014.
- [12] Ekbia, H. and Nardi, B., "Heteromation and its (Dis)contents: The Invisible Division of Labor between Humans and Machines". *First Monday*. June, 2014.
- [13] Gambetta, D., "Can We Trust Trust?", in (Gambetta, D., 'ed.'): *Trust: Making and Breaking Cooperative Relations*, Blackwell Pub, 1990.
- [14] Gillespie, T., "The Relevance of Algorithms", in (Gillespie, T., Boczkowski, P.J., and Foot, K.A., 'eds.'): *Media Technologies: Essays on Communication, Materiality, and Society*, MIT Press, 2014.
- [15] Glaser, B. and Strauss, A., *The discovery of grounded theory: Strategies for qualitative research*. Transaction Publishers, 2009.
- [16] Goffey, A., "Algorithm", in (Fuller, M., 'ed.'): *Software Studies: A Lexicon*, MIT Press, 2008.
- [17] Grinberg, R., "Bitcoin: An Innovative Alternative Digital Currency", *Hastings Science & Technology Law Journal*, 4, 2011, pp. 160-208.
- [18] Hurd, M.D. and Rohwedder, S., "Effects of the Financial Crisis and Great Recession on American Households", *National Bureau of Economic Research*, 2010.
- [19] Introna, L.D. and Nissenbaum, H., "Shaping the Web: Why the Politics of Search Engines Matters", *The Information Society*, 16(3), 2000, pp. 169-185.
- [20] Kaptelinin, V. and Nardi, B., *Acting with technology: Activity theory and interaction design*. MIT Press, 2006.
- [21] Kaplanov, N.M., "Nerdy Money: Bitcoin, the Private Digital Currency, and the Case against Its Regulation", *Loyola Consumer Law Review*, 25, 2012.
- [22] Kowalski, R., "Algorithm = Logic + Control", *Communications of the ACM*, 22(7), 1979, pp. 424-436.
- [23] Mallard, A., Méadel, C., and Musiani, F., "The Paradoxes of Distributed Trust: Peer-to-Peer Architecture and User Confidence in Bitcoin", *Journal of Peer Production*, 4, 2014.
- [24] Maurer, B., Nelms, T.C., and Swartz, L., "'When Perhaps the Real Problem Is Money Itself!': The Practical Materiality of Bitcoin", *Social Semiotics*, 23(2), 2013, pp. 261-277.
- [25] Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G.M., and Savage, S., "A Fistful of Bitcoins: Characterizing Payments among Men with No Names", *Proceedings, Conference on Internet Measurement*, 2013, pp. 127-140.
- [26] Nakamoto, S., "Bitcoin: A Peer-to-Peer Electronic Cash System", 2008.
- [27] Razsa, M. and Kurnik, A., "The Occupy Movement in Žižek's Hometown: Direct Democracy and a Politics of Becoming", *American Ethnologist*, 39(2), 2012, pp. 238-258.
- [28] Reid, F. and Harrigan, M., "An Analysis of Anonymity in the Bitcoin System", *Security and Privacy in Social Networks*, Springer, 2013, pp. 197-223.
- [29] Ron, D. and Shamir, A., "Quantitative Analysis of the Full Bitcoin Transaction Graph", *Financial Cryptography and Data Security*, Springer, 2013, pp. 6-24.
- [30] Schumpeter, J.A., *Capitalism, Socialism and Democracy*, Routledge, 2013.
- [31] Thrift, N., *Knowing Capitalism*. Sage, 2005.
- [32] Trudell, M., "The Occupy Movement and Class Politics in the Us", *International Socialism: A Quarterly Journal of Socialist Theory*, 133, 2012.
- [33] Vigna, P., "5 Things About Mt. Gox's Crisis", *The Wall Street Journal*, 2014.
- [34] Weber, M., *Economy and Society: An Outline of Interpretive Sociology*, Univ of California Press, 1978.