UNIVERSITY OF CALIFORNIA,
IRVINE

Algorithmic Authority of the Bitcoin Blockchain

THESIS

submitted in partial satisfaction of the requirements
for the degree of

MASTER OF SCIENCE

in Informatics

by

Caitlin Lustig

Thesis Committee:
Professor Bonnie Nardi, Co-chair
Professor Geoffrey C. Bowker Co-chair
Assistant Professor Joshua Tanenbaum

2018

DEDICATION

To

Laura Louise Lustig (1993-2004)

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACKNOWLEDGEMENTS

There are more people to thank than I could possibly list here, but I value everyone who has ever contributed ideas that have made it into this document or given me support that made it possible for me to write it. I thank my participants, some of whom took considerable amounts of time to share their thoughts with me and even reached out later and sent me materials they thought I might find useful. I deeply appreciate their generosity and enthusiasm. Thank you to Bodhisattva Chattopadhyay, Cassidy Dever-Baker, Yubo Kou, Dave Miller, and Jaime Snyder, who all read and critiqued my thesis. I especially thank Hope Sisley for putting significant amounts of time and energy into improving my writing.

Words cannot really describe how much Bonnie Nardi and Geof Bowker, my co-advisors, have supported me through what has been an unconventional path through my academic career. When I entered the University of California, Irvine's Informatics department, Bonnie and Geof took a chance on a green student from a computer engineering background who did not have much of the theoretical knowledge or many methodological skills needed to pursue research in their areas of study—just passion and interest. They were always patient co-advisors and provided invaluable advice, mentorship, and opportunities for growth. Geof and Bonnie believed in me even when I did not or when I could not see the value in my work. My third committee member, Josh Tanenbaum, has not only provided an incredible amount of support, but he inspires me to be more creative and to seek out the research that most excites me. I also thank Jonathan Alexander, Finn Brunton,

Bill Maurer, Don Patterson, and Alladi Venkatesh who were on committees for me at various stages of my career.

I have been fortunate to have a number of unofficial mentors during graduate school as well. Yong Ming Kow collaborated with me on my research on the imaginaries of actors in the Bitcoin ecosystem and gave me opportunities to do fieldwork that I would not have had otherwise. But more than that, he has been a good friend and mentor. I aspire to one day have his drive, generosity, and positivity. Jaime Snyder has been an invaluable source of local support as I finished my degree remotely in Seattle. She helped me to reframe many of the challenges that caused writer's block into opportunities. Over the course of my graduate career, I was also privileged to work as a graduate research assistant with Bill Maurer and the Institute for Money, Technology & Financial Inclusion (IMTFI), Judith Gregory, and Don Patterson. I especially want to extend a thank you to Judith, who is incredibly generous with her time, wisdom, and resources. I also worked as a teaching assistant for a number of classes with David Kay, and I value what he taught me about pedagogy. I thank the Graduate Resource Center at UCI, where I worked as a writing consultant. Karen Friedlander, the operations manager, was the best boss that I could ask for.

I would not have gotten through graduate school without the support and help of the Informatics department, particularly André van der Hoek, our current department chair, and Melissa Mazmanian, our current vice-chair of graduate affairs. I also want to extend my deepest thanks to the department's administrative staff—Adriana Avina, Suzie Barrows, and Julio Rodriguez.

Throughout my graduate career, I have consistently relied on Six Silberman, Lynn Dombrowski, and Jed Brubaker for career advice, emotional support, and friendship. They have the ability to see the best in my work and myself. They have an uncanny knack for understanding what I want to convey even when I cannot quite articulate it to myself.

Xinning Gui, Nikki Crenshaw, Yubo Kou, and Colin Wheelock: I will always treasure the time we spent together; I am so glad that we found each other.

Thank you to the many friends I made in graduate school who opened their homes to me, engaged in many late night conversations, and have been confidants: Nazanin Andalibi, Bodhisattva Chattopadhyay, Shiloh Cousins, Andy Echenique, Abram Gastelum, Oliver Haimson, Julia Haines, Jina Hong, Leah Horgan, Sara C. Kingsley, Katherine Lo, Katie Pine, Ankita Raturi, Noopur Raval, John S. Seberger, Martin Shelton, Aubrey Slaughter, Steve Slota, Karen Tanenbaum, Tao Wang, and Yiran Wang.

Over the years, countless colleagues have given me friendship, support, guidance, or inspiration at one point or another: Sanna Ali, Morgan Ames, Bill Aspray, Matt Bietz, Lindsay Blackwell, Tom Boellstorff, Scott Allen Cambo, Charu Chaudhari, Phoebe Chua, Courtney Loder Coolidge, Kate Crawford, Roderic Crooks, Amanda Cullen, Yao Du, Quinn DuPont, Nicole Ellison, Sheena Erete, Casey Fiesler, Dan Gardner, Tarleton Gillespie, Sandy Gould, Tesh Goyal, Mary Gray, Jean Hardy, Ellie Harmon, Dahlia He, Libby Hemphill, Garnet Hertz, Mustafa Hussein, Lilly Irani, Sam Kaufman, Chris Kelty, Vera Khonvanskaya, Bart Knijnenburg., Marina Kogan,

Ksenia A. Korobkova, Simone Lanette, William Lawrence, Alex Leavitt, Zaki Manian, Andrea Marshall, Dave Miller, Mark S. Miller, Norma Möllers, Javed Mostafa, Taylor Nelms, Juliet Norton, Alberto Pareja-Lecaros, Samir Passi, Leysia Palen, Jessica Pater, Justin Petelka, Nicholas Proferes, Michelle Purcell, Nishchint Raina, Eugenia Ha Rim Rho, Jennifer A. Rode, Seth Schoen, Bryan Semaan, Patrick Shih, Luke Stark, Katta Spiel, Si Sun, Aaron Trammell, A.M. Tsaasan, Pablo R. Velasco González, Janet Vertesi, Yvette Wohn, Chris Wolf, Adam Worrall, Melissa Wrapp, Lynette Yarger, and Tim Young.

In addition to Bonnie Nardi and Yong Ming Kow, I thank my other collaborators with whom I organized events: the CSCW 2016 workshop on Algorithms at Work: Susann Wagenknecht, Min Kyung Lee, Jacki O'Neill, and Himanshu Zade; the CHI 2016 panel on Algorithmic Authority: Katie Pine, Bonnie Nardi, Lilly Irani, Min Kyung Lee, Dawn Nafus, and Christian Sandvig; the ICWSM 2017 workshop on Studying User Perceptions and Experiences with Algorithms: Nick Proferes, Alissa Centivany, Jed Brubaker, Lala Hajibayova, Marina Kogan, Tanushree Mitra, and Nicole Ellison; and the CHI 2018 workshop on HCI for Blockchain: Chris Elsden, Bettina Nissen, Karim Jabbar, Reem Talhouk, Paul Dunphy, Chris Speed, and John Vines.

I have been fortunate to attend many conferences and events over the years through the generous funding that I received from the ACM-W; the Associated Graduate Students of UCI; UCI's Donald Bren School of Information and Computer Sciences; Gary Olson; Bonnie Nardi; the Financial Cryptography and Data Security 2016 conference—thank you to Ray Hirschfeld in particular; the iConference 2016

Doctoral Colloquium—thank you to the doctoral colloquium chairs, Greg Leazer and Iris Xie; the Consortium for the Science of Sociotechnical Systems (CSST) summer research institute 2016—thank you to Steve Sawyer and Wayne Lutters; the Hackademia Summer School 2016 hosted by Leuphana University's Centre for Digital Cultures and organized by Paula Bialski, Gabriella Coleman, and Marcell Mars; the City University of Hong Kong (which funded some of my travel expenses); and the National Science Foundation (which funded some of the projects for which I worked as a research assistant).

I want to thank the people who helped me even before I began in Informatics. I would never have gone to graduate school if not for the mentorship of my colleagues when I was an undergraduate computer engineering student at the University of Washington: Gaetano Borriello and Evan Welbourne, as well as Magdalena Balazinska, Yoshi Kohno, and Beth Kolko. Gaetano's generousity and passion for improving the world continue to inspire me, and I wish that I could tell him how much of an impact that he made on me. Thank you to Anthony Poon: my classmate, undergraduate research buddy, and most importantly of all—my friend. My undergraduate research internship through the ODCSSS program at the University College Dublin with Aaron Quigley and Lorcan Coyle cemented my desire to go to graduate school. I also owe a debt of gratitude to the people in UCI's Computer Science department, where I started my journey through graduate school. I especially thank my former advisor, Nalini Venkatasubramanian, and Sharad Mehrotra for guiding me through the beginning of my journey in graduate school and for teaching me many of the broader concepts that I use to understand the technical aspects of Bitcoin and the blockchain. This understanding has helped me contextualize my qualitative findings.

Thank you to all of my friends that I have met outside of graduate school, both long-term and new, who have made my life so much better through their presence. There are far too many friends to list here, but I especially want to thank Alexis, Cassidy, Christine, Daniel, Dave, Hope, Ian, Jenn, Kay, and Louie.

Lastly, I have the deepest appreciation for my family—my partner, Mat; my in-laws, Karen, Kirsten, and Daniel; my parents, John and Shelagh; my extended family; and my pets. Your love, support, and encouragement mean the world to me—more than any words could ever express.

ABSTRACT OF THE THESIS

Algorithmic Authority of the Bitcoin Blockchain

By

Caitlin Lustig

Master of Science in Informatics

University of California, Irvine, 2018

Professor Bonnie Nardi, Co-chair

Professor Geoffrey C. Bowker, Co-chair

In this thesis, I expand on the concept of algorithmic authority, a concept that I introduced in earlier work to understand the role of algorithms in daily life. Algorithmic authority is the legitimate power of algorithms to direct human action and to impact which information is considered true. In contrast to much other work on algorithms in sociotechnical systems, I argue for more precise use of the word “algorithm”, as well as for the importance of studying algorithmic systems that do consist of “black box algorithms”. Through a study of the users of the cryptocurrency Bitcoin, I explore what it means to trust in algorithmic authority in an open source, decentralized system and contrast it with the authority of centralized and corporate software. My study utilizes data from my survey, interviews, and observation of the broader Bitcoin community. I examine the tensions between members of the Bitcoin community who would prefer to integrate

Bitcoin into institutions and those that saw it as a radical use of algorithmic authority. I describe how my participants preferred algorithmic authority to the authority of conventional institutions that they saw as untrustworthy. However, they acknowledged the need for mediating algorithmic authority with human judgment. I examine these tensions between how they would like Bitcoin to be used and how it is being used, and what those tensions can tell us about algorithmic authority. Lastly, I suggest future research directions for examining a wider range of algorithms and better understanding the Bitcoin community.

PREFACE

I sat in the back of the room at New York University's Algorithms and Accountability conference in 2015—it was a large room and, perhaps not so surprisingly, mostly filled. At this point, the interest in critical algorithms studies (though that area of research may not have been called that at the time) was picking up, and the room was inhabited by new media scholars, lawyers, information scientists, computer scientists, and journalists. I remember feeling as though I had "found my people" after searching for so long for a community that I fit into. Until graduate school, I was a computer engineer with a degree focus on hardware. Up until the time of the conference, I had often felt that I had thrown myself into the deep end when I began to transition into my current work, and I never fully felt comfortable identifying as an information scientist, although I also no longer felt comfortable identifying as a computer engineer either. The eclectic group of people gathered that day understood me, I thought, but I also had a nagging question at the back of my mind: *what do we mean when we say "algorithm"?* I remembered reading literature in the scholastic vein of this conference in 2012, and at that time I had felt that the literature misrepresented the concept of an algorithm. By the time I was in that room, I felt somewhat differently; although I did not fully understand what was meant by "algorithm" in critical algorithm studies, I understood and largely agreed with the critiques of algorithms that were presented at the conference. But, as I sat in the back, I overheard a disgruntled comment from programmers seated near me:

“*these people don’t know what algorithms are.”* The voice in my head asking “*what do we mean when we say algorithm?”* grew louder, and it has never fully gone away.

So, what *do* we mean when we talk about “algorithms”? While this question may seem prescriptive, it does not assume that there is a single definition of algorithm. Rather, it asserts that it is important to examine whether the sociotechnical systems research on algorithms is generalizable, when most of it refers only to machine learning algorithms. These algorithms are used in a variety of domains, such as medicine, search, and profiling, and so we must also ask: does it even make sense to talk about algorithms in a general sense? In my own research on blockchain protocols, which I have situated in the critical algorithm studies literature, I have struggled with whether it makes sense to talk about the blockchain as an algorithm. While some of my early participants did refer to the blockchain as “math” and as an “algorithm”, in recent years, as debates have heated up over how to make Bitcoin scalable, the word “protocol” has gained prominence in the Bitcoin community. However, there is still worth in connecting the blockchain to the critical algorithm studies literature, as research on the blockchain can interrogate the limits of the concept of “algorithm”, and gives a path for theorizing about algorithms that are dramatically different than the black box, largely invisible algorithms commonly studied in that area of research. Furthermore, discussing the blockchain as an algorithm provides a way to understand why we might take “algorithm” as a unit of analysis rather than code, protocols, or any number of other things.

Chapter 1. Introduction

In this thesis, I demonstrate the ways in which an algorithm can still have authority over a diversity of users who interpret the purpose and functionality of the software in a multiplicity of ways. I will describe new ways to understand the concept of an "algorithm" and discuss how algorithms gain authority over such a group of people. I call the emergent dynamic between algorithms and human actors "algorithmic authority". Algorithmic authority is defined as *the authority of algorithms to direct human action and to verify information, in place of relying exclusively on human authority*.

In this thesis, I use my empirical research (first described in Lustig & Nardi, 2015a) to 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. I examine these questions through a qualitative study of Bitcoin, a cryptocurrency that around the time that I finished my initial study had an exchange rate of $393.12 USD to one bitcoin (October 15, 2014), and around the time that I finished my thesis, $7,658.01 USD to one bitcoin (June 2, 2018)[1]. (See Figure 1 for graphical representation of Bitcoin price fluctuations.) The main algorithm that I will refer to is the *blockchain*. In this paper, I follow the convention of Bitcoin users by referring to the system as Bitcoin and the units of currency as bitcoin. Unless otherwise specified, when I refer to "*the* blockchain", I am generally referring to Bitcoin's blockchain. Although there

[1] Calculated using https://www.coinbase.com/charts

are countless technologies and other currencies that have their own blockchains as well, these technologies are currently mostly proof-of-concepts[2].

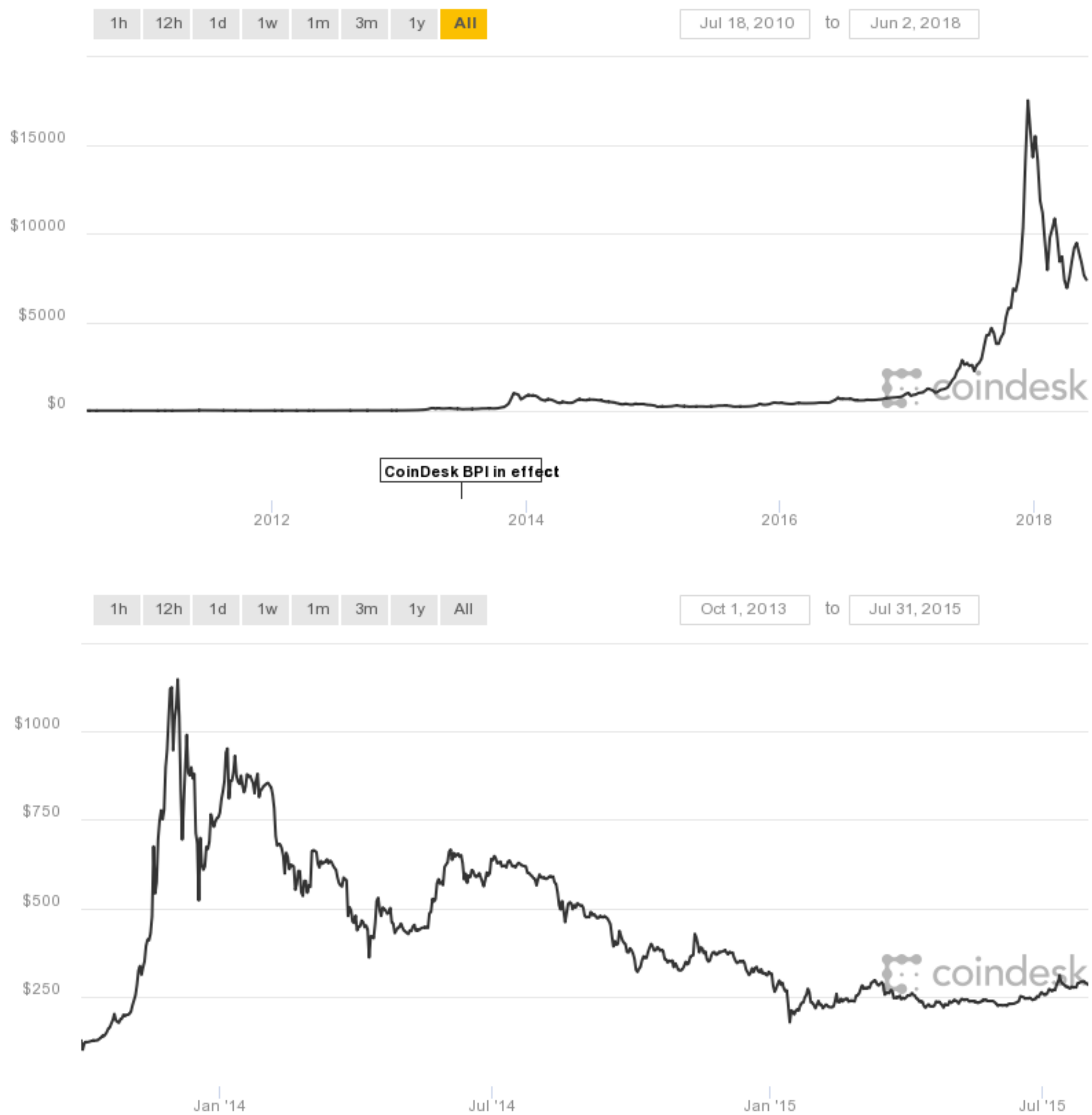

Figure 1: The price of Bitcoin compared to US dollars.
Prices shown were (a) from July 18, 2010 (early in Bitcoin's history) to June 2, 2018 (the time of the thesis was written); (b) from October 1, 2013 to July 31, 2015 (the time period in which the original study was conducted). Source: CoinDesk, https://www.coindesk.com/price/

[2] See Elsden et al. (2018) for an overview of the landscape of blockchain applications at the time this thesis was written.

I chose Bitcoin as an example of algorithmic authority because it is not managed by governments, banks, or even an organization, but by algorithms. These algorithms were developed by the Bitcoin open source community and used in the decentralized Bitcoin network. The algorithmic authority of the blockchain is notably different from many machine learning algorithms, which are perhaps the most discussed instances of algorithmic authority in both popular media and critical algorithm studies research. These discussions center on "black box" algorithms (generally these are algorithms that use artificial neural networks), that make decisions that are difficult for humans to interpret. Unlike Google's search engine optimization algorithms, which would be impossible to fully understand and predict even if the code was open source[3], Bitcoin's code is open source and its users often openly discuss its algorithms. They are so often discussed that Maurer, Nelms, and Swartz (2013) argue that the code is one of two things[4] that are "*practically all that Bitcoin enthusiasts ever talk about*" [emphasis in original] (p. 274) . Indeed, in my initial study, my user participants were well informed about the ways in which Bitcoin's code worked. My later study was focused more on Bitcoin developers and businesspeople, who were often concerned with how Bitcoin's code should be modified in order to make it better support their visions of an ideal future.

[3] Barocas, Hood, and Ziewitz (2013) state that many algorithm developers argue, "Even if you had Larry and Sergey [the co-founders of Google] at this table, they would not be able to give you a recipe for how a specific [Google] search results page comes about" (p. 6).

[4] Maurer et al. (2013) argue that Bitcoin enthusiasts also talk about the labor involved in mining bitcoin.

However, this thesis is not truly about Bitcoin. It is about algorithms. Bitcoin may not exist in the long-term future, or it may not exist in a way that represents the current desires of the Bitcoin community. Or, maybe it will exist and fulfill many of their hopes for the future. (As the Bitcoin community would say, perhaps it will go "To the moon!!! ┗(°0°)┛ "[5]) Even if Bitcoin becomes a footnote in history, the age of algorithms is upon us, and the concept of an algorithm in the context of large sociotechnical systems will endure. Bitcoin gives us a lens to concretely explore that which is otherwise seen as intangible and "unknowable"[6].

In the next chapter, I describe what algorithms are and why they are important. I expand on definitions from computer science, critical algorithm studies, and wider discourse, in order to develop the more inclusive definition of algorithm that I use in this thesis. I go on to explain how this definition relates to theories about authority and trust.

Chapter 3 describes why research on Bitcoin can help address some of the gaps in critical algorithms research. I briefly describe how Bitcoin works in order to give some background on the issues that mattered to my participants. This chapter

---

[5] ToTheMoonGuy, a reddit user who became famous in the Bitcoin community, explains this meme:

> ToTheMoonGuy has naught but a single Bitcoin to his name, but when Bitcoin finally reaches The Moon, we will know, for ToTheMoonGuy's 1 bitcoin will buy him his ticket. […]
>
> ToTheMoonGuy speaks out in both recognition and celebration of the greatest moments in Bitcoin. His conviction strikes fear in the hearts of central bankers, and his courage warms the soul of weary bitcoiners, even in the coldest episodes of oversupply (ToTheMoonGuy, 2018)

[6] Many thanks to Tao Wang for helping me to develop this framing about the importance of Bitcoin in the context of critical algorithm studies.

is not technical and simplifies some topics in the interest of clarity. I then go on to discuss related work on the Bitcoin community.

Chapter 4 discusses my methods. I conducted two studies, the first of which is primarily described in this thesis. This study was on the attitudes and values of the users of Bitcoin. In 2013, I conducted a survey of the Bitcoin community (primarily Bitcoin users), and from 2014-2015, I interviewed a subset of my survey participants. In my second study (2015-2018), I attended Bitcoin conferences and primarily researched businesspeople and developers in the blockchain ecosystem.

Chapter 5 focuses on how Bitcoin is a type of emergent algorithmic authority. I first discuss the limitations of my survey design and the demographics of the participants who took my survey. Next, I compare the language used by Bitcoin advocates with the language used to describe black box corporate algorithms in wider discourse to examine how different portrayals of algorithms give them authority. Finally, I argue that while my participants tended to distrust certain institutions, in some ways, blockchains may only gain authority if they become more corporate and centralized.

In Chapter 6, I examine the tensions between how my participants wanted Bitcoin to operate (e.g., in a decentralized manner), and how it functioned in practice. I analyze these tensions using the concept of an incomplete utopian project (as defined by Gregory, 2000).

In Chapter 7, I suggest directions for future research on Bitcoin and algorithms, and I summarize my main findings.

Chapter 2. The Importance of the Concept of an "Algorithm"

Algorithms have always been a crucial part of software development—they are "the fundamental entity with which computer scientists operate" (Goffey, 2008, p. 15). Beyond just shaping the behavior of software, algorithms have an increasingly critical role in shaping economics, politics, and behaviors, as well as, in some cases, perpetuating biases and discrimination. They impact our knowledge of the world, our work practices and agency, and how we are treated by sociotechnical systems. It is no wonder that the word algorithm has come into public discourse, and that over the last five years, the interdisciplinary "critical algorithm studies"[7] and FATML (fairness, accountability, and transparency in machine learning) areas of research have been created and quickly become increasingly important and visible. In critical algorithm studies, a broad range of disciplines—such as science and technology studies (STS), human computer interaction (HCI), law, computer science, and media studies—have become focused on researching algorithms as critical components of sociotechnical systems: their political and economic effects, methods of auditing them for fairness and bias, and their legal implications.

While in other work I have argued for more empirical studies that could bridge that gap between critiques of algorithms and the practices of users, I now argue that in addition to empirical research, one important step toward bridging

[7] See: the critical algorithms reading list compiled by Gillespie and Seaver (2016).

this gap will be to go back and re-examine what we mean when we say "algorithm" (Proferes, Centivany, Lustig, & Brubaker, 2017).

Developing more precise language to situate work on algorithms, while at the same time broadening the range of algorithms that we research, may help us address some of the difficulties of designing better sociotechnical systems (Wagenknecht, Lee, Lustig, O'Neill, & Zade, 2016). For example, how to address concerns like privacy and transparency will differ based on the application space (e.g., medicine versus social media), and more dialogue is needed between researchers in different application domains (Lustig et al., 2016). Furthermore, distributed systems have significant differences from more centralized systems in terms of how authority manifests. In order to expand our understanding of the diversity of algorithms, there are a number of questions we might ask: When we say "algorithm" are we only referring to machine learning? Does it make sense to make generalizations about algorithms in different application spaces? What differences are there between the ethical concerns in the design of algorithms in centralized and distributed systems? What are the differences between ethics of open source and closed source algorithms?

An examination of the definition of algorithm is necessary for contextualizing this thesis and addressing these questions, but it is not easy to define algorithms. Not only do different disciplines have varied definitions for algorithms, but even within mathematics and computer science—the primarily disciplines concerned with algorithms—there is some disagreement about the meaning of the word. The following sections briefly summarizes some of the definitions of algorithm in computer science, critical algorithm studies, and in corporate discourse. I end with discussing what algorithm means in this thesis.

2.1. In Computer Science

Perhaps the most succinct definition of algorithm is "logic + control" (Kowalski, 1979). Algorithms are simultaneously instructions (logic) and the action that carries out these instructions (control). Other definitions of algorithms (e.g., (Knuth, 1973; Stone, 1971)) elaborate on this idea further by arguing that algorithms: (1) must have a finite runtime; (2) must not require any thought in order to calculate (i.e., as long as one can follow instructions, one can execute an algorithm); and (3) must produce outputs that relate to the inputs that it was given. Berlinski (2001) playfully sums up this definition:

> **In the logician's voice:**
> *an algorithm is*
> *a finite procedure,*
> *written in a fixed symbolic vocabulary,*
> *governed by precise instructions,*
> *moving in discrete steps, 1, 2, 3, . . .,*
> *whose execution requires no insight, cleverness,*
> *intuition, intelligence, or perspicuity,*
> *and that sooner or later comes to an end.* [emphasis in original]
> (p. xiv)

These definitions tend to also describe an algorithm as a function that is computable by a Turing Machine (i.e., a machine that can calculate anything that can be calculated); however, there have been some researchers that argue that there are some algorithms that fall outside of this category and have capabilities beyond what Turing described (Blass & Gurevich, 2003).

2.2. In Critical Algorithms Studies

In the article, “Governing Algorithms: A Provocation Piece”, Barocas et al. (2013) question the popularity of the word “algorithm” in academic research on sociotechnical systems. They ask, “Would the meaning of the text change if one substituted the word ‘algorithm’ with ‘computer’, ‘software’, ‘machine’, or even ‘god’? What specifically about algorithms causes people to attribute all kinds of effects to them?” (p. 3). I also ask, if algorithms are the building blocks of software, then what is the discursive advantage to using “algorithms” as our unit of scale?

In recent research on algorithms in the social sciences, “algorithm” generally refers not to a singular algorithm, but to algorithmic systems. Algorithmic systems are “intricate, dynamic arrangements of people and code” (Seaver, 2013, p. 9). While computer scientists and mathematicians may sometimes speak of sorting algorithms and graph search algorithms, in this other discourse, the word algorithm consistently represents complex algorithmic systems that use Big Data to make decisions with real life consequences for humans. For example, Tufekci (2015)used “algorithm” to describe “computational processes that are used to make decisions of such complexity that inputs and outputs are neither transparent nor obvious to the casual human observer” and conceptualized algorithms as actants (i.e., despite not being alive, they have agency; see: (Latour, 2005)). In other words, algorithms such as “merge sort” do not fall under this definition, because even when used to sort Big Data, there is nothing specific about the use of merge sort that affects software in a way that impacts humans. Often cited examples of this kind of algorithmic system are Google’s search engine algorithms and Facebook’s News Feed algorithm.

In the following, I describe three types of algorithmic systems that demonstrate the importance of researching the social impacts of algorithms: public relevance algorithms, heteromation algorithms, and profiling algorithms. There are many more types of algorithmic systems that have significant influence over the lives of people, but I use these three as examples of the algorithms commonly discussed by critical algorithm studies researchers. Note that I do not discuss the technical aspects of these types of algorithms. Understanding the technical aspects of the algorithms can greatly help researchers identify technically feasible solutions that address the thorny ethical issues these algorithms raise; technical knowledge can give a greater understanding of how these systems were designed. However, in this thesis, I am primarily focusing on the discourse about algorithms, rather than the construction of algorithms.

Public relevance algorithms: David Beer (2009) describes how with the advent of Web 2.0, software became ubiquitous and participatory, and algorithms gained "the capacity to shape social and cultural formations and impact directly on individual lives" (p. 994). An example of the power of algorithms in everyday life is Google's suite of search and ranking algorithms, which influence the information users have access to and in turn may impact what they judge to be true (Introna & Nissembaum, 2000). Gillespie (2013) refers to these kinds of algorithms as "public relevance algorithms"—algorithms that "select what is most relevant from a corpus of data composed of traces of our activities, preferences, and expressions" (p. 168). Burrell (2016) points out that search algorithms are not necessarily machine learning algorithms; however, they are part of algorithmic systems that use machine learning algorithms for specific tasks like "detecting ads or blatant search ranking manipulation and prioritizing search results based on the user's location" (p. 3).

Heteromation algorithms: Algorithms not only impact how users constitute their knowledge of the world, but they also can act as employers or managers of users. This role of algorithms in shaping human behavior can be observed in technologies of *heteromation*, which are characterized by their use of humans as integral "computational components" to augment software algorithms (Ekbia & Nardi, 2014, 2017). Heteromation is a reversal of automation. Technologies of automation use computers to perform prohibitively expensive or difficult tasks for humans. Instead, heteromated technologies use humans to perform tasks for computers (e.g., Amazon Mechanical Turk (AMT); see: (Irani, 2015) for a discussion of algorithmic management in AMT). Heteromation uses computational systems to organize and manage laborers and to run computations on the work that the laborers perform. Although the type of work that the concept of heteromation encompasses is quite broad, heteromated systems typically involve human work as a necessary part of their algorithms.

Profiling algorithms: A third use of algorithms is to construct profiles based on the demographics and behavior of users or groups. Algorithms may then use these data to create user profiles based on categories, such as perceived race, ethnicity, gender, and interests. These categories are formed by computing the likelihood of a user belonging to a certain group based on how their online activities compare to others of that group (Cheney-Lippold, 2011)[8]. Through profiling, algorithms may inadvertently violate user privacy, and perpetuate inequalities and stereotypes. In recent years, there has been increased interest in research on how Big Data algorithms, particularly advertising algorithms, use profiling to perpetuate discrimination. Research on Google advertisements showed that searches for black-identifying names were 25% more likely to bring up advertisements that were suggestive of an arrest record than searches for white-identifying names (Sweeney, 2013). Studies found that gay men were shown advertisements for a particular nursing school more than men of other sexualities (Guha, Cheng, & Francis, 2010), and that men were shown Google advertisements for higher paying jobs more often than women (Datta, Tschantz, & Datta, 2015). An article on Facebook advertising revealed that Facebook had been constructing "Ethnic Affinity" categories for users based on their Internet activity (Angwin & Parris, 2016). Before Facebook changed their policies, these categories could be used to violate the US Fair Housing Act by only showing housing advertisements to certain ethnicities.

Profiling algorithms can also be used for predictions. For example, they are used to determine how likely someone is to pay back a loan or credit card, and this prediction is then used to automatically decide on the loan amount or credit limit. These algorithms do not necessarily reduce human bias; they may be trained on incorrect or incomplete data[9] and they may also develop unintentional biases

[8] See (van Otterlo, 2013) for an accessible technical description of profiling algorithms.

[9] Data is constructed, it is not "objective" truth. As Bowker (2005) argues, "Raw data is both an oxymoron and a bad idea; to the contrary, data should be cooked with care" (p. 184).

(Bruckner, 2018). For instance, they “may place a low score on occupations like migratory work or low-paying service jobs. This correlation may have no discriminatory intent, but if a majority of those workers are racial minorities, such variables can unfairly impact consumers' loan application outcomes” (Citron & Pasquale, 2014, p. 14). In other words, while these algorithms are designed to discriminate against individuals considered to be a high credit risk (e.g., individuals with low income), the algorithm may also make correlations between income and other factors, such as race, and begin to classify certain minority groups as high risk.

These three types of algorithms all possess different types of algorithmic authority—be it through prioritizing and displaying information, managing humans, or decision-making based on profiling.

2.3. The “Work” of Algorithms in Corporate and Wider Discourse

What work does the word “algorithm” do? I have explored what classifies a computational component as an algorithm rather than “code” or “a program” and what kinds of algorithms researchers in the critical algorithm studies area are concerned with, but further elaboration is needed on what the word evokes in wider discourse, particularly in the ways that it is used by companies that have developed algorithmic systems. Critical algorithm studies researchers engage with this wider discourse to examine the ways that corporations describe algorithms and their characteristics in order to promote certain perceptions of their software.

This question of “what work algorithms do” has been explored in Sandvig’s (2014) essay on “the algorithm”, which traces the history of the concept of “algorithm” in various discourses. He explains that what was once a concept that was primarily in the realm of technology and education is now defined through marketing. The corporate use of “the algorithm” has much in common with how the word “platform” has been used. In “The Politics of ‘Platforms’”, Gillespie (2010) deconstructs the multiple meanings that the word “platform” takes on when used by corporations to promote their product to three different audiences: advertisers, content producers, and users. He identifies four different images of platforms that these companies seamlessly project to simultaneously appeal to their three audiences: computational platforms, architectural platforms, figurative platforms, and political platforms. Platforms are portrayed as technologically innovative spaces where advertisers and content producers can raise up their content to make it visible to users; they are simultaneously portrayed as spaces that facilitate multiple viewpoints in an egalitarian manner. Similarly, I later explore how “algorithm” has been used by companies to project multiple images of “the algorithm” as both a set of abstract mathematical rules and as an artificial manager. They portray algorithms as simultaneously objective and neutral, natural, mysterious and opaque, authoritative, powerful, and automatic. I later return to these aspects to explain how they relate to perceptions and utilities of blockchains, which are typically open source and decentralized.

2.4. In this Thesis

In the previous sections in this chapter, I highlighted how algorithms are seen by computer scientists as lists of instructions that take input data and produce outputs; by social scientists as large systems that have influence over people's lives; and by corporations as marketing tools that demonstrate the supposed objectivity and power of their software.

In this thesis, I use the word "algorithm" to refer to an assemblage of the code (i.e., list of instructions) and of the human actors that facilitate the implementation and operation of this code. An assemblage is "a mode of ordering heterogeneous entities so that they work together for a certain time" (Müller, 2015, p. 28). This thesis uses "assemblage" somewhat loosely and does not delve into assemblage theory. Instead, I describe an algorithm as an "assemblage" in order to emphasize how in algorithmic systems, code and humans come together to perform tasks through an algorithm, but the relationship between these actants are configured in mutable ways. The configuration of the assemblage of every algorithm is unique, and even uses of the same algorithm differ over time and context. In other words, it is difficult to make absolute statements about agency of algorithmic systems.

In contrast to the definitions of "algorithm" that are implicit in the work of critical algorithm studies researchers, this definition of algorithm does include decentralized and open source algorithms, as well as algorithms that are not machine learning algorithms. It includes public relevance algorithms, heteromation algorithms, and decision-making algorithms. This broader definition allows us to not only talk about algorithms that primarily derive authority from the perceived trustworthiness of the corporations that develop them, but also about algorithms that gain authority from users' trust in the algorithm's perceived openness and decentralization. In other words, in order to trust corporate algorithms, such as Facebook's, users must partially place their trust in the corporation itself because the code is not visible; whereas, users of open source software, such as Bitcoin, place their trust in the algorithm precisely because its code *is* visible. When algorithms become more visible in "black box systems", such as through breakdowns or abuses (e.g., Cambridge Analytica[10]), companies are generally seen as less trustworthy—when an algorithm that was once invisible becomes visible, it is rarely perceived in a positive way[11].

Algorithmic authority, then, is about trust—trust that the code of an algorithm or the people that control it will behave in a manner that is predictable and reasonable. Trust is of particular importance in understanding how algorithms gain authority. I turn to Gambetta's (1988) 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. (p. 217)

---

[10] Cambridge Analytica was a political consulting firm that gathered data from over 50 million Facebook users, primarily without their consent or knowledge. These data were used to develop psychometric profiles and target advertisements to users in an attempt to affect the outcomes of elections (Metcalf & Fiesler, 2018)

[11] Star and Ruhleder (1996) state that one attribute of an infrastructure is that it is "visible upon breakdown" (p. 113). This thesis does not explicitly examine algorithms as infrastructure, but I have discussed blockchains as infrastructure in other work (Kow & Lustig, 2017).

Thrift (2005) stated that “software is best thought of as […] an expectation of what will turn up in the everyday world […] a means of sustaining presence which we cannot access but which clearly has effects, a technical substrate of unconscious meaning and activity” (p. 156). Software can shape our expectations and understanding of the world, but Thrift argued that though its effects may be visible, the relationship between the inputs to the software and the exact mechanisms used to process those inputs are largely invisible, creating a sort of “technological unconscious”. Users may trust in software because of some level of predictability, but they are vulnerable to not only the visible effects of software, but also to their invisible effects. I argue that because algorithms are an assemblage of humans and code, trust is not just about predictability of software—some users may place more trust in the code and others may place more trust in the humans who maintain or design the code. In other words, where users place trust and authority is not the same for all users and for all algorithms.

Weber’s theories about authority (1978) are useful for understanding the spectrum of types of authority. He described authority as leadership that is perceived as legitimate and without coercion, and he defined three kinds of authority: traditional, charismatic, and rational-legal authority. *Traditional authority* refers to authority that derives its legitimacy from precedents and social norms. It is authority that is inherited or is seen as something that has “always existed”. *Charismatic authority* refers to an authority that derives legitimacy from a leader with a charismatic personality; followers may believe that this leader has extraordinary abilities or divine powers. Charismatic authority tends to challenge traditional authority. *Rational-legal authority* refers to an "appeal to efficiency, and the rational fit between means and intended goals" (Coleman, 1997, p. 36). Weber presented authority as a dynamic concept; over time, the source of legitimacy of an authority may change. Traditional authority upholds the status quo, whereas charismatic authority challenges it. Rational-legal authority may challenge tradition but does so in a way that is more gradual than charismatic authority.

Which of these forms of authority do algorithms utilize? The authority of algorithms seems to derive most heavily from rational-legal ideals, but it is in no way limited to that type of authority. (Indeed, the religious language sometimes used to describe Bitcoin's creator points to some kind of charismatic authority by proxy for Bitcoin.) An algorithm must be represented as objective in order to gain legitimacy through rational-legal authority. Gillespie (2014) argues that for public relevance algorithms to be seen as legitimate, they must appear to be completely automated. In order to maintain the legitimacy of the "shape" of the algorithm, both technically and in terms of the values it represents, developers of the algorithm must describe it in a way that defends its impartiality. However, Gillespie points out that algorithms are often not completely objective and, furthermore, they are often not completely automated or "hands off". There are many things that search algorithms may find relevant to a query that are not displayed, be it for legal, moral, or commercial reasons. For example, Google "refuse[s] to autocomplete search queries that specify torrent file-trading services" (Gillespie, 2014, p. 181).

As stated earlier, algorithmic authority is defined as the authority of algorithms to direct human action and to verify information, in place of relying exclusively on human authority. This concept is not entirely new. Before I began writing about algorithmic authority, an astounding number of other phrases had already been developed to describe the authoritative aspects of algorithms: power through the algorithm (Beer, 2009); governing algorithms (Barocas et al., 2013); relevance algorithms and algorithmic objectivity (Gillespie, 2014); and algorithmic management (Irani & Silberman, 2013; Lee, Kusbit, Metsky, & Dabbish, 2015); as well as many more to describe the general social impact of algorithms: algorithmic identity (Cheney-Lippold, 2011); algorithmic culture (Hallinan & Striphas, 2014); algorithmic living (Boellstorff, 2013); and algorithmic invisibility (Tufekci, 2014). In addition, Clay Shirky (2009) also used the phrase "algorithmic authority" before I did. I developed my concept of algorithmic authority before finding Shirky's earlier use of the phrase; however, despite the similarity, my definition has some key differences. In a blog post, Shirky (2009) 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.'" (para 12). Shirky uses Google's PageRank algorithm as an example of how information can be generated automatically and trusted by most people as "legitimate". My use of the term algorithmic authority is broader than his, as well as most of the other terms I referenced in this paragraph; I argue that algorithms are not only given the authority to decide which information is true and to create and analyze categories, but also to direct heteromated human action. Previous work has generally not tied all of these uses of algorithms together.

Chapter 3. Bitcoin

In the following, I describe why Bitcoin is an important example of algorithmic authority, and briefly describe how it works and some of the related research on it.

3.1. Why Bitcoin?

I use Bitcoin as an example of algorithmic authority that is open source, decentralized, and heteromated—as opposed to the algorithms typically focused on by critical algorithm studies (e.g., online search algorithms, recommender algorithms, and targeted advertising algorithms). In the following, I describe some of the limitations of critical algorithm studies research and how researching open source software and peer-to-peer (P2P) systems, such as Bitcoin, could provide an alternative path for understanding algorithmic authority.

It is important to extend the discourse in critical algorithms studies because the prevailing focus on black box algorithms has multiple weaknesses:

1. It does not pay enough attention to the sense-making that users and workers do when they use algorithmic systems. Understanding these behaviors would help researchers better understand the work needed to support the users of these algorithms (Lee et al., 2015).

2. It has largely not focused on how algorithms are developed. It is surprising that, through infrastructural inversion[12], critical algorithm researchers have worked to reveal the power of algorithms in the world but have not extensively looked at the practices used to develop these algorithms. Examining open source algorithms, such as the blockchain, provides a better understanding of how algorithms that are completely transparent can still have authority. An implicit assumption in critical algorithm studies is that algorithms have power because users cannot challenge or understand them; however, this is generally not true of open source software.

3. It has focused on what is different about algorithms from other modes of control and authority, without enough focus on what makes them similar; there has been undue focus on how the decisions made by algorithms may not be questioned by users because they are black boxes, without placing this kind of decision-making into a historical context (e.g., Striphas (2010) on "algorithmic culture"). In other words, these arguments often suggest that there was a time when decisions made by authorities could be questioned, when people could get "real answers". However, they do not take into account the relations of power between individuals and corporations, and the decisions that are made behind closed doors. There are differences between decisions made by powerful humans and algorithms—certainly, the inability for any one person to understand the decisions made by complex

[12] First discussed in (Bowker, 1994), "infrastructural inversion" refers to "foregrounding the truly backstage elements of work practice" (Star, 1999, p. 380).

algorithms (Barocas et al., 2013) and algorithms' ability to automatically make statistical decisions based on attributes of "the crowd" (Citron & Pasquale, 2014), distinguish algorithms from previous decision-making processes. But without examining how algorithms are similar to these other modes of control and authority, researchers risk oversimplifying the relations of power between the developers of algorithms and their users.

Despite the large volume of research on algorithms, there is not always a sense of how and why the authority of algorithms forms and evolves, just simply that it exists. More empirical work in this area would give a better sense of how users come under the authority of algorithms, especially in the context of heteromated algorithms. Algorithmic systems can be challenging to empirically research, because the data they use are often private and the algorithms themselves are often black boxes. As described by Burrell (2016), algorithms may be seen as opaque for three reasons: (1) companies may keep their algorithms secret in order to prevent others from copying them or users from gaming their algorithms; (2) it may be difficult to understand the code without specialist knowledge; (3) the decisions made by an algorithm cannot be comprehended because as "a computer learns and consequently builds its own representation of a classification decision, it does so without regard for human comprehension" (p. 10). It is difficult to make critiques that lead to better policies, design guidelines, and methods of preventing or detecting unethical behavior when we cannot necessarily fully grasp many of the complexities of the algorithms that we study.

These critiques point to the importance of researching open source systems. In particular, more research is needed on algorithms used in distributed networks, especially peer-to-peer networks (P2P). P2P is widely associated with both a type of technical architecture and a certain ethos about how society should be organized that is markedly different from that of proprietary networks (Musiani, 2012). These technological networks may be portrayed as "distributed forms of management" (Galloway, 2004, p. 8). In 2005, Michel Bauwens, founder and director of The P2P Foundation, predicted that P2P would not just be a type of technical architecture, but also "a new human dynamic" that would upend old models of political economies. (However, what he refers to as "P2P political economy" might be better described as "commons-based peer production", as coined by Benkler (2006).) Bauwens describes a "third mode of production" in which "use-value [is produced] through the free cooperation of producers who have access to distributed capital" (Bauwens, 2005, Peer to Peer section, para. 4) through self-governed communities that "make use-value freely accessible on a universal basis, through new common property regimes. This is its distribution or 'peer property mode': a 'third mode of ownership'" (para. 6). Bauwens argued that this new kind of political economy would only be feasible because of P2P infrastructure. In this vision, peer-to-peer systems operate as stand-ins for traditional governance because they decentralize "not just features, but costs and administration as well" (Shirky, 2001, p. 20), and, despite the hierarchical nature of Internet protocols, the Internet is widely accessible to the public because of lower barriers to entry (e.g., computers becoming relatively affordable and Internet access becoming fairly ubiquitous in many parts of the world). Distributed communication protocols allow for “autonomous communication” and “autonomous content production that may be distributed without the intermediary of the classic publishing and broadcasting media” (Bauwens, 2005, The Infrastructure of P2P section, para. 2).

Similarly, Folkinshteyn, Lennon, & Reilly (2015) promoted the idea that Bitcoin’s development mirrors that of the World Wide Web (WWW). “In addition to its simplicity, [the WWW] has a deliberately decentralized nature. Nobody needs to ask permission to create a webpage and link to other websites. There is no central database or authority which needed to be updated or maintained” (p. 83), and they argued that, “the Bitcoin system allowed for the same in the currency space” (p. 85) in part because it is open source. The Bitcoin source code was originally published on Bauwen’s website, the P2P Foundation, and he later expressed his thoughts on Bitcoin, arguing that “this technology is potentially a game changer by bringing down the transaction cost for self-organization” through smart contracts and distributed autonomous systems (Bauwens, 2014, The Positive Aspects of Bitcoin section, para. 7). However, he also cautioned that Bitcoin could lead to more inequality. It may most benefit people with extreme libertarian views, “which allied with venture capital and the oligarchies that invest in Bitcoin, [would alter] the balance of power away from emancipatory and progressive political forces” (The Negative Aspects of Bitcoin section, para. 7). Bauwens argued that although Bitcoin is a distributed technology (with the goal of disintermediation; i.e., getting rid of the need for intermediaries), it may in fact lead to the rise of new centralized institutions. Historically, peer-to-peer systems without mechanisms for maintaining equality run the risk of being used as effective tools for large institutions to centralize control when there are no mechanisms for preventing them from co-opting the technology or for preventing these institutions from taking over the majority of the network.

These tensions between centralized and decentralized control make Bitcoin a particularly rich research topic. In the following, I describe Bitcoin and what makes it relatively unique from technological perspective. I do not go into great technical detail, and I have only included the information necessary to understand the basics of Bitcoin and the concepts that my participants discussed.

3.2. What is Bitcoin?

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 (Blendon & Benson, 2009). Overall, US Americans were pessimistic about the stock market and housing prices (Hurd & Rohwedder, 2010). In 2009, 48% of US Americans reported that they felt angry that the government was bailing out "banks and financial institutions that made poor financial decisions" (Pew Research Center, 2009). 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 (Trudell, 2012). Occupy protesters argued that the current way in which liberal democracies function is deficient (Razsa & Kurnik, 2012).

Like members of the Occupy Movement, at the time of my initial study many Bitcoin users were drawn to the currency because they wished to disrupt institutions by creating their own institutions governed by consensus. To understand what it means to "disrupt" an institution, I turn to Schumpeter's (2013) definition of "creative destruction": that which "incessantly revolutionizes the economic structure from within, incessantly destroying the old one, incessantly creating a new one" (p. 83). Bitcoin is appealing to some users because it not only provides an alternative to government-based fiat currency[13], but because they 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 (2008). It is widely believed that Satoshi Nakamoto is a pseudonym for the person or persons who created Bitcoin. In this thesis, I follow the convention of much of the Bitcoin community and refer to Satoshi as "he" and use his first name. Satoshi'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, Satoshi argued that

[13] Fiat currency refers to currency whose value is not derived from a commodity, but from an authority (usually a government). There have been some debates as to whether Bitcoin is a fiat currency, because while it is not a government-issued currency, it arguably not a commodity—there is no practical use for Bitcoin besides as a currency. Kaplanov (2012) argues that, "[u]nlike fiat currencies, whose value is derived from regulation or law and underwritten by the state, bitcoins have no intrinsic value and the only real value is based on supply and demand—what people are willing to trade for them" (p. 4). However, Grinberg (2011) argues that Bitcoin is fiat currency simply because it is not a form of commodity money. Bitcoin users themselves tend to frame Bitcoin as oppositional to fiat currencies, which suggests that they do not see it as a fiat currency. The confusion is complicated even more by some participants reporting that they do use Bitcoin as a commodity. In the US, Bitcoin is currently regulated as a commodity by the US Commodity Futures Trading Commission, but what Bitcoin "is" (e.g., a currency, a commodity, something else?) considered to be has not been consistent across governing bodies. The ways in which Bitcoin is used as a commodity are explored later.

electronic commerce is flawed because it has high transaction fees and affords consumers less privacy than cash transactions.

According to Satoshi, the methods taken to prevent *double spending* are the main cause of the shortcomings of electronic commerce. Double spending refers to online transactions in which "many copies of the same bitstring are spent at different merchants" (Hoepman, 2007, p. 152). 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 means that merchants may later lose money that they thought they had received. Therefore, 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. Satoshi (2008) argued 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" (p. 1). In response to these issues, Satoshi designed Bitcoin to solve the issue of double spending without mandatory transaction fees or loss of privacy.

Figure 2: Screenshot of the Bitcoin-Qt graphical interface for Bitcoin Core.
Source: "Screenshot of Bitcoin core v0.10.0 running on fedora 21" by Bitcoin Developers, 2015 (https://commons.wikimedia.org/wiki/File:Bitcoin-core-v0.10.0.png) distributed under an Expat/MIT license (https://commons.wikimedia.org/wiki/Category:Expat/MIT_License)_

Satoshi created Bitcoin as a currency and payment platform that is *pseudonymous*[14], *supports micro-transactions,* and *has no inherent transaction fees*. Bitcoin was designed with the idea that it would have the same affordances as cash, but in a digital format. While cash is typically regulated by a government, Satoshi's system relies on a distributed and decentralized P2P network to give it value through consensus and artificial scarcity. Bitcoin's network keeps a public, pseudonymous ledger of all transactions. This ledger is called the *blockchain* (Figure

[14] Researchers have shown that Bitcoin is not as anonymous as originally believed (e.g., (Reid & Harrigan, 2013)).

2). When a transaction is made (Figure 3), software on peers' computers verifies that the money has not been double spent by comparing it against this ledger.

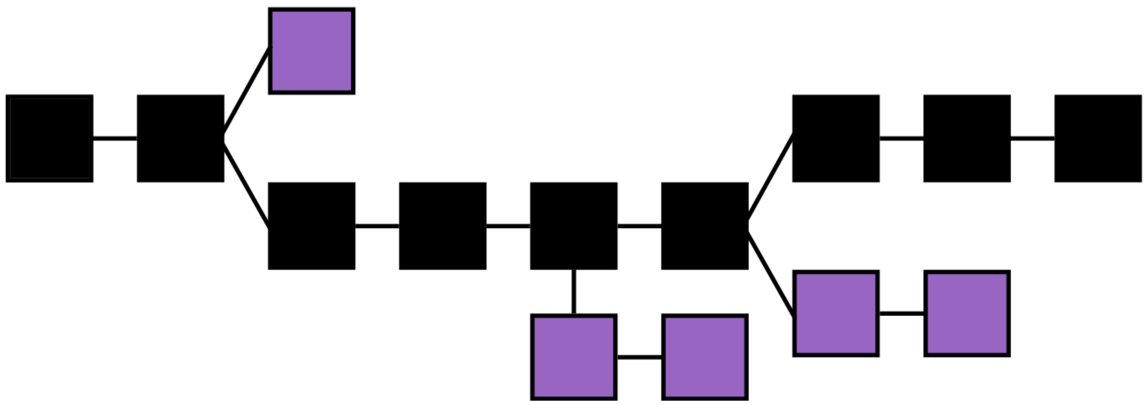

Figure 3: A graphical representation of a blockchain with forks.
Figure has been modified for visual clarity; the original was created by Theymos (https://en.bitcoin.it/wiki/File:Blockchain.png) distributed under a CC-BY-3.0 license (https://creativecommons.org/licenses/by/3.0/legalcode)

The blockchain mechanism has been described by numerous sources as "the main innovation of Bitcoin". 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 cryptographic hash functions, which make the blocks impossible to "forge". (Essentially, this mechanism means that instead of trusting a mint to make hard-to-counterfeit currency, Bitcoin users trust in cryptographic algorithms to create counterfeit-proof money[15].) 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 short time of each other, the Bitcoin network may be unable to immediately come to a consensus about which block should come next in the blockchain. In this situation, the

[15] Thanks to Dave Miller for this framing of Bitcoin's algorithmic authority.

blockchain creates a "fork". Whichever branch of the fork is longest becomes a part of the main blockchain and the other branches are discarded. In Figure 3, the longest chain is shown in black and the other branches are unused.

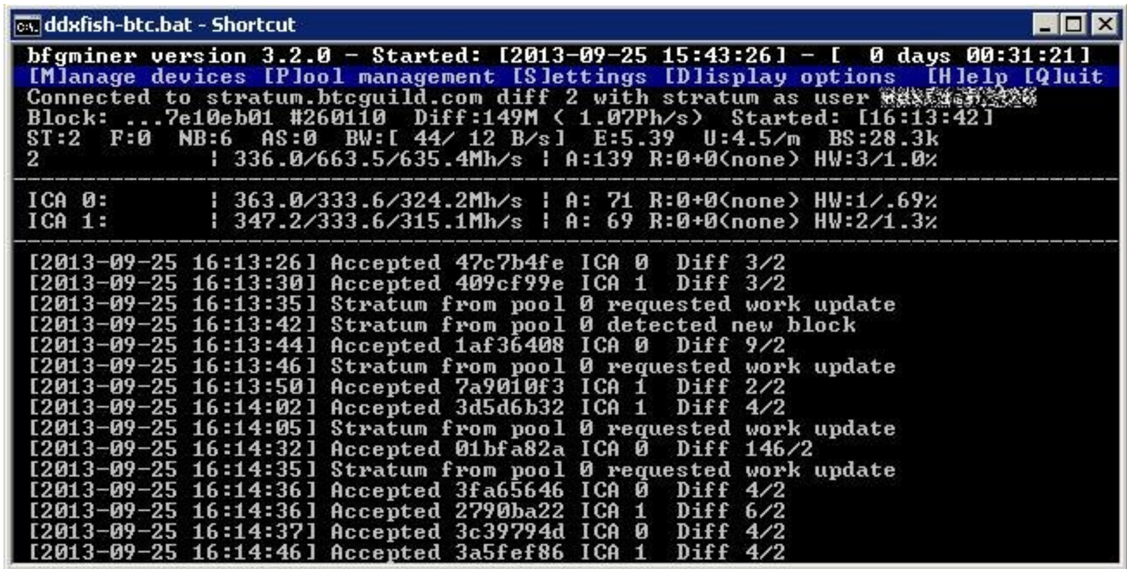

Figure 4: A screenshot of the bfgminer software.
Source: SourceForge (https://sourceforge.net/projects/bfgminer/)

In order to incentivize users to run this software (e.g., software shown in Figure 4), there is a random chance that the user will be rewarded new bitcoin for completing a calculation. Bitcoin users refer to the generation of new bitcoins as "mining" bitcoins. When bitcoins are mined, the verified transactions are bundled into a "block" and put into the blockchain. 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 some Bitcoin users wanted to make clear to me—this number could change if the community agreed to change the code.) As of May 2018, over 17 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% (referred to as "the halvening"). At the time of writing this thesis, this number is 12.5. Users have calculated that by the year 2140 all 21 million bitcoins will have been mined.

The method of consensus that Bitcoin uses is not without risks. The most commonly discussed attack on Bitcoin during my initial study is referred to as a "majority attack" or a "51% attack", in which a miner with the majority of the power in the network can mine blocks fast enough to produce a fork that includes blocks that prohibit or reverse transactions or double spend bitcoin. Bitcoin is vulnerable to many other types of attacks (see: ("Weaknesses - Bitcoin Wiki," n.d.), including attacks that only require 25% of the mining power (Eyal & Sirer, 2014). Therefore, centralization of mining power has significant security risks, which worried some participants, as mining has become more and more centralized over the years.

Bitcoin is hardly the first modern widespread alternative to fiat money, but it was the first to capture the public's attention. Bitcoin has been also 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. 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, at the time of my initial study, Bitcoin was 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. And unlike e-gold, Bitcoin has no infrastructural mechanism to determine the identities of users (Grinberg, 2011; Kaplanov, 2012).

The blockchain protocol also provides a kind of governance through code: anyone can join Bitcoin's distributed computing network, but the protocol has mechanisms to make it nearly impossible for actors to alter the ledger for their own gain. Thus, Bitcoin advocates have referred to the blockchain as "trustless" because they believe that they do not need to trust individual actors—they simply trust the network as a whole to come to the correct consensus. Bitcoin is also an international currency. For these reasons, Bitcoin has gained a reputation for being a subversive technology, and was, at some point in time, associated in the public's mind with illegal activity[16].

Other uses of the blockchain protocol include storing records of ownership (e.g., property or securities) and "smart contracts". Simply put, smart contracts are code stored on blockchains that execute when certain conditions are met. However, "smart contract" does not have a single definition, and the term has been used to describe "physical objects that change their behavior based on some data. More recently, the term has been used for the exact opposite: to describe computation on a blockchain which is influenced by external events such as the weather" (Greenspan, 2015, para. 1). The most promising uses for smart contracts come from

[16] While it is difficult to accurately survey Bitcoin users about their illegal activities, a 2013 survey showed that most users of Bitcoin did not use it for illegal purposes (Smyth, 2013), and this finding is also supported by my own data. In order to gain trust, I did not ask participants about illegal activities, but some participants volunteered their opinions about them in interviews and survey responses, which were largely negative.

the Internet of Things domain. One example is smart locks (e.g., those proposed by Slock.it)—locks with digital keys that are only valid for the duration that someone has paid to use a property, such as a recurring monthly rent payment or a one-time payment for a hotel room. If payment is not recorded on the blockchain, the smart contract automatically executes and makes it so that key no longer works. Machines in the Internet of Things might also use a blockchain to buy and sell things to one another, such as excess electrical energy, using a neutral platform that is not owned by any company and can be accessed by all machines running the same protocol. When organizations share the same ledger (i.e., blockchain), they cannot alter the transactions for their own gain and all parties can verify that transactions are correct. These uses of the blockchain are sometimes referred to as "decentralized autonomous organizations" (Buterin, 2014b), and they have sparked imaginaries of a world without the need for lawyers or governments, or even the need for humans in the service industry[17]. Buterin described this future in a Reddit comment:

> You wake up, and see that $17.27 was automatically deducted from your primary wallet, as you had authorized to happen every day, to pay the rent for your apartment; if you canceled the authorization, then, after a warning period, ownership in the land-registry contract would automatically transfer back to the landlord, and the door lock would no longer recognize signatures signed by your smartphone's private key as valid for letting you in. Of course, your landlord is bound by the same restrictions. If he shuts off his account that pays the local government $6.60 land-value tax per day, then he loses ownership and the contract automatically switches over so you are renting from the government

[17] While there are more practical uses of the blockchain to replace certain jobs, a humorous example of this imaginary comes from Maurer's interaction with a young programmer:

> I have to admit I didn't quite understand how a distributed ledger would benefit machine-led, automated construction. He shifted to another example: ice cream shops, which "self-replicate and own themselves… you could get rid of the cashier, too." But who will stock the shelves, I asked? "I guess robots could do that, too" (Maurer, 2016, p. 85).

> instead. The government itself is simply a large decentralized organization, and you can see in real time the $6.60 moving on the blockchain and eventually getting into an account to pay for a medical-research program trying to extend the human lifespan from 170 years to 230. The Internet that you are using to access this information is based on a decentralized and incentivized mesh-networking platform; you paid $0.0009 to access the information, but your laptop also earned $0.0014 transmitting other people's packets at the same time. You get into your Mastercar self-driving car to go to work (originally, all self-driving cars were made by Google, but Master Corporation, a decentralized autonomous entity that automatically uses a combination of futarchy and liquid democracy to determine how the company should spend its funds each day, proved that its governance mechanism was so efficient that it overtook Google on some core services within three years, and alt-Mastercorps took over most of its other operations). You get in, and Mastercar runs a [sic] optimized version of the A* search algorithm (for which James Wilbur automatically got a bounty of $782,228 worth of MSC from the Master Contract) to determine the optimal path to your primary workplace. Given that your self-tracking app has detected that you value your own time (or, rather, the delta between time spent in a car versus time spent at home or work) at an average of $14.18 per hour, the Mastercar's algorithm chooses a route that takes an extra eleven minutes in order to avoid road tolls and also on the way moves a shipment from one side of the city to the other. You drive out, and thirty minutes later you have spent $1.04 on electricity for your car, $1.39 on road tolls, but receive a reward of $2.60 for moving the shipment over. You arrive at work—a location which is a hybrid living/working space where 'employees' of five different alt-versions of Master Corporation are spending most of their time, except that you chose to live at home because you have a family. You then get to work, running simulations of a proposed new scalability algorithm for the now community/DAO-driven Ethereum 6.0. (Buterin, 2014a)

The concept of decentralized autonomous systems is inextricably tied to blockchain technology, as evidenced by the trajectory that proponents see for blockchain technology. Swan (2015) argued that blockchain technology will have three waves: Blockchain 1.0, Blockchain 2.0 (which, at the time of writing, is the most accurate description of the current state of the blockchain ecosystem), and Blockchain 3.0. In Blockchain 1.0, blockchains were simply used for currencies (e.g., Bitcoin). In Blockchain 2.0, code is stored on a blockchain that runs under certain conditions (e.g., smart contracts). By and large, these applications currently have low usage and are primarily “proof of concepts”. Blockchain 3.0, “articulates decentralized principles of governance and justice throughout society, underpinned by the diffusion of blockchain technology” (Elsden, Nissen, et al., 2018, p. 2). The difference between Blockchain 2.0 and Blockchain 3.0 is that the focus in 3.0 less about the blockchain itself, and more about the ideas that inspire the greater blockchain community and how blockchains might be used to create new kinds of infrastructures, new kinds of relationships between humans and machines, new ways of viewing the world, and new forms of governance.

Although this section largely discussed technical details of Bitcoin, there are obvious political implications for its design, namely, some advocates imagine using it to create a future with little centralized governance and an abundance of decentralized automated organizations leading to a future with “automata as authority” (Szabo, 1997). Bitcoin users have been drawn to the currency in part because they find human judgment flawed—humans can be corrupt and make errors, but algorithms, they reason, cannot. They argue that blockchain is more efficient and transparent than bureaucracies. These themes will be explored further in later chapters.

3.3. Related work

Other than this study, there have been few studies on the users of Bitcoin or blockchain technology. Bohr and Bashir (2014) note that, “Surveying a random sample of the Bitcoin community is nearly impossible as Bitcoin offers a lot of privacy to its user, the currency is not regulated by any centralized agency, and adoption of Bitcoin is still not widespread" (p. 95). There have been some regional studies of Bitcoin users and other actors in the blockchain space: entrepreneurs based in Copenhagen who are shaping the infrastructure of blockchain technology (Jabbar & Bjørn, 2017); developers, miners, entrepreneurs, and lawyers based in Southern California and Hong Kong (Kow & Lustig, 2017); Bitcoin users in Malaysia (Sas & Khairuddin, 2017); users in Hong Kong (Kow & Ding, 2016); and users in Indonesia (Gunawan & Novendra, 2017). Broader research on Bitcoin users includes (Baur, Bühler, Bick, & Bonorden, 2015; Fabian, Ermakova, & Sander, 2016; Lustig & Nardi, 2015a), surveys conducted in (Smyth, 2013, 2014) as well as further analysis of Smyth's 2013 survey in by Bohr & Bashir (2014), and community-led surveys such as (Bitcoin Student, 2014; CoinDesk, 2015; IceTurtle4, 2014). There have been multiple studies contrasting the opinions of users and non-users (Bashir, Strickland, & Bohr, 2016; Gao, Clark, & Lindqvist, 2016) and user opinions on the anonymity of Bitcoin (Fabian et al., 2016; Lustig & Nardi, 2015b). Some work has been conducted on specific events or debates in the history of blockchain technology, such as the DAO exploit (DuPont & Campbell-Verduyn, 2017) and the scaling debate (De Filippi & Loveluck, 2016). Other work that discusses 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., Meiklejohn, 2013; Reid and Harrigan 2013). Some researchers have also taken a historical look at the ideas that influenced Bitcoin's design (Barok, 2011; DuPont, 2014).

In what was perhaps the most relevant work when my initial study was conducted, Maurer et al. (2013) 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. 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" (p. 263). Maurer et al. suggested 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" (p. 268). Bitcoin was designed to prevent corruption, and consequently, users found the system more trustworthy than institutions such as governments and banks. Mallard, Méadel, and Musiani (2014) suggested that trust in Bitcoin is distributed through several sociotechnical mechanisms, one of which is the underlying algorithms of Bitcoin's code, in particular because it is a peer-to-peer system. To use a P2P 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.

Chapter 4. Methods

This thesis draws on two studies I conducted, but primarily uses data from the initial study; the second study will be examined further in future work and is primarily used here to add context and verification to my findings. The initial study consisted of two phases: a survey and a series of interviews. I also engaged in observation by actively reading forum posts, blogs, and articles written by community members. My findings in this study were derived using Grounded Theory methodology (Glaser & Strauss, 2009). The second study was focused on observation at conferences for different audiences (i.e., academics, developers, or businesspeople), as well as formal and informal interviews with attendees, and observation of the official Bitcoin developer mailing list (first called Bitcoin-development, now called bitcoin-dev). I received IRB approval for my research from the University of California, Irvine.

4.1. Survey

I posted an exploratory survey of 36 questions on BitcoinTalk.org (326,031 users at the time) and /r/Bitcoin (122,561 subscribed users at the time) in October, 2013. I 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 composed of questions rated on a Likert-type scale 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 510 survey participants, 124 left their addresses.

4.2. Interviews

I used the data collected from the survey to craft interview questions based on the themes that emerged from the responses. From the survey data, I noted that participants had diverse views on the future of Bitcoin and government regulation of Bitcoin. I used exploratory and semi-structured interviews to learn more about the diversity of views on those issues, and I iteratively refined the questions based on previous interviews. I contacted about a third of the survey participants for interviews in waves until over twenty participants agree to be interviewed. I did not contact survey participants who left short answers or did not answer a large number of questions. All interviewees were men; no women or nonbinary people offered to be interviewed. I 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. I also conducted five follow-up interviews with these participants (one in Winter 2015; the others in Summer 2015—two of these interviews were in person), and two with participants obtained through snowball sampling in Summer 2015, for a total of 29 interviews.

Figure 5: Frankenmint's ASICMiner Block Erupters.
Photograph by Stephen Lam for Reuters (Randewich, 2013).

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*." (See Figure 5 for a picture of one of Frankenmint's later mining rigs.) Original orthography and punctuation have been preserved for participants who communicated over instant message and email.

4.3. Observation

Over the course of my research, I read Bitcoin forums and blogs from November 2012 to mid-2018, to immerse myself in the Bitcoin community. I primarily read posts on Reddit. The forum and blog posts I read focused on the latest Bitcoin news, technical details of Bitcoin's implementation, and political economic theory. I 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. After the shutdown of Silk Road, articles in mainstream media took a more serious look at how Bitcoin could be used. I also briefly attempted to mine bitcoins, but did not have hardware that was powerful enough to yield any bitcoins.

I found that throughout this initial study Bitcoin users reached out to me—many were interested in the results of the research. Some participants sent links to articles or images they thought I would find interesting. One Bitcoin user even gave me a generous gift on Reddit for appreciation of my survey—0.05 bitcoins. At the time this was valued at around $8 USD, but at the time of the completion of this dissertation, May 8, 2018, is worth $467.00 USD[18]. This gift mirrored traditional ethnographers' experiences of receiving gifts from members of the communities they research. See Nardi (2016) for further detail about how my fieldwork resembled those of traditional ethnographers and the reactions from members of the Bitcoin community to my research.

During my later research (2015 to 2018), I also attended Bitcoin events, such as numerous academic events and workshops hosted by the Institute of Money, Technology, and Financial Inclusion; The State of Digital Money conference; The Blockchain Future event hosted by the OC (Orange County) Tech Hour; and Inside

[18] This money is still unspent and will only be used to further my research on Bitcoin (e.g., pay to attend Bitcoin-related conferences) or it will be donated if I cease to conduct research on Bitcoin in the future.

Bitcoins San Diego conference, which I attended with my collaborator, Yong Ming Kow. I attended the 2016 Financial Cryptography and Data Security conference, as well as the Bitcoin workshop held at the conference. This conference began in 1997 and is attended by prominent members of this sub-field of cryptography, and more recently has been attended by key developers in the Bitcoin and wider blockchain space. I have also followed email lists for Bitcoin researchers and the Bitcoin developer mailing list (bitcoin-dev). I was a teaching assistant for a course on Bitcoin taken entirely by non-users. I also observed online (e.g., /r/bitcoin and bitcointalk.org) and physical (e.g., a house inhabited solely by developers of Bitcoin and blockchain applications) spaces for members of the Bitcoin community. I collected data through audio and video recordings, photographs, screenshots, emails, instant message conversations, physical artifacts (such as a hardware bitcoin wallet), and field notes.

Chapter 5. Bitcoin as an Example of Emergent Algorithmic Authority

My findings examine the reasons Bitcoin users turned to algorithmic authority and the ways in which that authority was mediated by human judgment. My findings reveal some of the tensions and complexities of algorithmic authority. Participants' views on the blockchain were diverse—they viewed it as political or apolitical, centralized or decentralized, promoting resistance or reifying institutional hegemony. For each of these pairs, most participants' views were somewhere in between, but they tended to lean strongly in one direction or another. These views were further complicated by the difference in how participants wanted Bitcoin to function and the ways in which it was actually used. Exploring these tensions allows us to gain a greater understanding of the complexities of algorithmic authority, the multiplicity of ways in which algorithmic authority may manifest and be understood, and how this authority is continually renegotiated.

In the following sections, I contrast how algorithms gain authority in corporate settings with how the blockchain has authority in the Bitcoin community. I draw on academic discourse on algorithms more broadly and from my research on the Bitcoin community to make these comparisons. Section 5.1 describes the demographics of the people who took my survey and gives context about the broader blockchain community. In Sections 5.2 and 5.3, I contrast the authority of black box algorithms in corporate settings with that of the blockchain in two different contexts: algorithms portrayed as mathematics (Section 5.1) and algorithms portrayed as stand-ins for human labor (Section 5.2). In these two sections, I show that how the Bitcoin community and corporations tended to describe algorithms had much in common, although their portrayals of algorithms were based on different ideals and different types of authority. However, Section 5.4 discusses how some participants argued that in order to have authority, Bitcoin needed to be more like corporate algorithms, in that Bitcoin might need to become more regulated and integrated with other institutions.

5.1. Who Uses Bitcoin?

Bitcoin has gone through waves of adoption: cryptographers (2009-2011); libertarians and anarchists (2012-2014); and businesspeople and investors (beginning in 2015). My survey of Bitcoin users was conducted in 2013, towards the tail end of this second wave. By the time I attended blockchain conferences in 2015, I began to see a much larger presence from businesspeople and investors, who were primarily interested in Bitcoin because of they believed they could profit from it, although many first took notice of it because they held libertarian viewpoints.

The open source Bitcoin community has provided a wealth of public information for scholars, as its culture promotes active participation. In this thesis, I use the phrase “Bitcoin community” to primarily refer to the English-speaking community; this decision to focus on English-speakers was a pragmatic one, based on my own language competences. The larger Bitcoin community consists of many different kinds of actors such as users, entrepreneurs, investors, developers, miners, and legal experts. Many users are experts on Bitcoin and the blockchain in their own right even though they are not Bitcoin or blockchain developers. Looking through the writings of the Bitcoin community gives a sense of just how knowledgeable and invested (both financially and emotionally) the community is in Bitcoin and blockchain technology. The English language community has multiple sizeable subreddits (e.g., /r/bitcoin and /r/btc), online forums (e.g., Bitcoin Forum), IRC channels, blogs where lively debates take place in the comment sections, mailing lists (e.g., bitcoin-dev), events, books written by community members, and a community of researchers, both academic and non-academic (some work independently or for companies). The Bitcoin community is an example of a "recursive public", which Kelty (2008) defined as:

> a public that is vitally concerned with the material and practical maintenance and modification of the technical, legal, practical, and conceptual means of its own existence as a public; it is a collective independent of other forms of constituted power and is capable of speaking to existing forms of power through the production of actually existing alternatives. (p. 3)

This community is actively involved with shaping the trajectory of Bitcoin and the blockchain—in terms of its underlying protocols, the capabilities of the technology, and the values that the technology is designed to represent; and the community also determines its governance structure and distribution of power. Members of this community regularly produces what Mallard et al. (2014) termed "hybrid literature": technical proposals and research that are not written by academics, but carry the same weight in the community.

5.1.1. A note on survey design

In this thesis, I have used the original wording from my survey and other surveys that I reference (hence erroneously using "male" and "female" to refer to gender later in this thesis), although there are some demographics questions should have been worded differently. In this section, I briefly discuss the limitations of my survey design.

I began the demographics section with: "Please only give as much information as you are comfortable giving. All questions are optional. Your demographic data is for informational purposes only and will not be tied to your responses in any publications that will come out of this research." I asked questions about participants' age, gender, sexual orientation, religious beliefs, household income in US dollars, how their income compared to the average income in their country, highest level of education completed, and their country of residence. In the following, I describe some of the reasons for these survey design decisions.

First, I deliberately did not ask about ethnicity or race. International survey design guidelines suggest that designing surveys with questions about race and ethnicity are challenging across international contexts in which understandings of these concepts differ. The United Nations Statistics Division (2017) states that "[b]ecause the ethnocultural composition of a country can vary widely from country to country and due to the diversity in the approach and the various criteria for establishing ethnicity, it is recognized that there is no single definition or classification that could be recommended that would be applicable to all countries" (p. 205). There is evidence that there are international commonalities in conceptions of ethnicity and race that can be leveraged to develop survey questions about ethnicity and race (Morning, 2008), but for this survey I chose to simply ask about the country that the participants lived in.

Second, I regret using "male", "female", and "other" for my options for gender (participants, were, however, allowed to pick more than one option and given the option to describe their gender further if they selected "other"). I should have used "woman" and "man" because those words are associated with gender; whereas, "female" and "male" are associated with sex. Furthermore, "other" literally others non-binary people. Thankfully, one participant did call me out on my wording in their response. See Jaroszewski et al. (2018) for suggestions on how to better word survey questions about gender, especially for communities that have the potential for responding negatively to more inclusive wording. As I describe later, at the time that I conducted my survey, some parts of the Bitcoin community were known for not being inclusive of women.

Third, some participants took offense that I asked about sexual orientation. All demographic questions were optional, so as to not cause discomfort for participants. My intent in asking about sexual orientation was to be thorough and ask about major categories of identities even if there was not an obvious connection to how they might perceive or use Bitcoin. Because I used Grounded Theory methodology, I wanted to leave as many avenues for inquiry open as possible. However, by this logic, the survey should have included questions about marital status, occupation, and any number of other things.

Fourth, I asked participants how their income compared to the average income in their country because it was difficult to make inferences about economic class based on their income as reported in US dollars. While this question was useful for understanding participants' general economic status, asking about their income compared to the general income in their region would have given a more exact answer. For example, someone in San Francisco, CA, USA may make much more than the average income in the United States, but they may identify as middle class because the cost of living is high in San Francisco.

Lastly, my questions about political beliefs were not based on any standards for survey design. Participants were asked, "Which political outlooks best describe you? Please select one or more. These descriptors may not match the language you would use to describe yourself. The next question gives you a chance to answer in your own words." I provided them a list of common political labels and allowed them to select more than one: anarchist, communist, green, left-wing, libertarian, moderate, right-wing, and socialist. I then asked participants: "Please describe your political views in a short sentence." I phrased my questions to avoid referencing political parties, although in some countries some of these labels do have parties associated with them, such as green and libertarian. However, I recognize that these labels are skewed towards what are generally considered left-wing labels. I had difficulty finding a list of standard political ideologies that was appropriate for an international survey.

5.1.2. Survey results

As shown in Table 1, the Bitcoin users who responded to my 2014 survey were predominantly US American (51%), male (96%), libertarian (60%), and between 25-34 years of age (50%). 63% had bachelor or graduate degrees. Participants were relatively affluent; only 27% self-reported making less money than the average person in their country. While gathering demographic data was not the main focus of this study, it has been included here in order to give readers a better sense of the background of participants and how that background might have informed their views.

When I shared some preliminary results with the /r/bitcoin community, I was asked by users if the demographics of Reddit might be skewing the data. A Reddit user (who later deleted their account) responded with:

> Everything about this confirms people's beliefs about /r/Bitcoin. And the majority demographic being 25 and 34 year old, heterosexual, atheist or agnostic, American, and male is extremely reflective of reddit in general. I suppose an interesting question would be if this study is reflective of all Bitcoin users. I'm pretty sure it is.

I did find that participant demographics were similar to those of Reddit as a whole. According to a 2011 survey (Reddit Originals), Reddit users tended to be male (78%), young (84% were between 18 and 34), and US American (64%). However, the Bitcoin community had a significantly higher proportion of males, was more geographically dispersed, and a bit older than Reddit users.

Table 1: Demographics of Bitcoin

Demographic Category	Percentage
Gender (allowed to pick multiple options)	
Male	96.92%
Female	2.09%
Other	1.86%
Age	
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%
Income in US dollars	
$0-$24,999	23%
$25,000-$49,999	22%
$50,000-$74,999	15.4%
$75,000-$99,999	10.1%
$100,000-$124,999	11.4%
$125,000-$149,999	5.3%
$150,000-$174,999	3%
$175,000-$199,999	1.3%
$200,000 and up	8.4%
Self-reported income	
Higher than national average of participant's country	44.71%
Around the national average of the participant's country	27.04%
Less than the national average of the participant's country	27.88%
Education	
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%
Political beliefs (allowed to select multiple options)	
Libertarian	59.25%
Moderate	36.25%
Anarchist	27%
Left-wing	25.25%
Green	18%
Socialist	11%
Right-wing	8.25%
Communist	2.5%

Demographic Category	Percentage
Religion (allowed to select multiple options)	
Atheist	47.5%
Agnostic	33.81%
Christian	17.9%
Other	11.11%
Buddhist	6.86%
Jewish	2.13%
Muslim	1.42%
Hindu	0.95%
Sexual orientation	
Straight or Heterosexual	90%
Gay, Lesbian, or Homosexual	2.1%
Bisexual	3.5%
Other	4.2%

The preponderance of males in my survey was not a fluke—in 2014, a survey of Bitcoin users found that 93% of respondents were male (Smyth, 2014). This was a slight improvement on the gender imbalance seen in a 2013 survey which had found that 95% of the respondents were male (Smyth, 2013). Speculation about why Bitcoin is overwhelmingly used by men is beyond the scope of this thesis; however, the Bitcoin community at the time was not known for being particularly feminist. Two men that I interviewed did relate stories about how they had tried to speak up in favor of feminist issues on /r/bitcoin and BitcoinTalk and received very negative reactions from other users.

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 1% or more 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: Switzerland, France, Singapore, Russian Federation, Poland, Belgium, Czech Republic, New Zealand, Spain, Italy, India, Ireland, Austria, Slovenia, Greece, Philippines, Argentina, Romania, Denmark, Croatia, China, Serbia, Israel, Brazil, Portugal, Japan, South Korea, Belarus, Malaysia, Slovakia, Mexico, South Africa, Moldova, Hungary, Lithuania, Taiwan, Thailand, Ukraine, and Benin.

Of the initial 22 interview participants, 13 were from the US, two from Australia, two from Germany, one from Argentina, one from Canada, one from Croatia, and one from India. One was a US American who was living in China at the time of our first two interviews (and we met in person for a third interview after he moved back to the USA). The survey participants located in the USA were in California (2), Colorado (1), Florida (2), Indiana (1), Maryland (1), Massachusetts (2), Minnesota (1), New York (1), and Utah (2).

Participants reported a number of uses for bitcoin, including selling items without fear of chargebacks, moving large amounts of money to different accounts quickly, investing, trading against other currencies, donating, and making international purchases. Only 69% of participants reported making Bitcoin transactions at least a few times a month; this finding was similar to that of surveys that were conducted around the time that I conducted mine. Those surveys found that roughly 30%-40% of participants did not report spending bitcoin (Bitcoin Student, 2014; IceTurtle4, 2014; Smyth, 2013). Few of my participants were miners—7% mined as a serious venture although 56% of participants had attempted mining at least once (similar to Smyth's (2013) findings).

I found that the views of the wider blockchain community ranged from that of the blockchain as an invisible and largely apolitical infrastructure for simply recording data and providing additional security and privacy measures to data storage—to that of the blockchain as a decentralized political tool for stopping government corruption, automating jobs across a wide range of sectors, and transforming organizational structures. In the next section, I describe how the concept of "algorithms as math" can support these conflicting views, as well as support both open source and more corporate agendas[19].

5.2. Algorithms as Math

When algorithms are represented as mathematical rules by corporations, they are portrayed as objective black boxes. This portrayal makes it difficult to understand the nature of agency and accountability in algorithmic systems. This description of algorithms is also problematic in that it provides justification for discrimination. While the blockchain is often also portrayed as objective

[19] Open source software can also be corporate, but here I am discussing software systems that are more aligned with type of one organizational structure than the other (i.e., open source or corporate).

mathematics, it differs from this typical portrayal in two key ways: it is transparent (all data is public) and it does not utilize personal or demographic information. For the Bitcoin community, objectivity positions Bitcoin in opposition to existing institutions because it suggests to some that human-run institutions could be replaced by automatic decision-making made by blockchains.

5.2.1. Algorithms may gain authority by seeming objective and natural

Companies commonly portray algorithms as completely autonomous bits of code, free from human intervention. This portrayal obscures the decisions and labor required to design algorithms; thereby hiding the roles of programmers, infrastructural and technological constraints, and stakeholders:

> When algorithms are mentioned at all, platform providers often encourage the notion that their algorithms operate without any human intervention, and that they are not designed but rather "discovered" or invented as the logical pinnacle of science and engineering research in the area. (Sandvig, 2014, Commercial Depiction of "The Algorithm" section, para. 3)

In this presentation of algorithms, they are seen as laws of nature or mathematical theorems that have only recently been discovered. And like nature and mathematics, they are portrayed as objective and politically neutral. This description is particularly common for Bitcoin; a speaker at a Bitcoin conference that I attended described Bitcoin as "*the sun and the stars—it is a force of nature, it exists*". As described further in Section 5.2.2., Bitcoin users often frame the blockchain as trustworthy because it is "math".

In framing algorithms as discoverable and objective, the people and organizations involved in developing the algorithm may be portrayed as unaccountable for the actions of the algorithm. This framing not only distances those developers from the algorithm, but also divorces the algorithm from the "practice that enlivens algorithms and activates their consequences" (Orlikowski & Scott, 2015, p. 211). In some cases, algorithms may be seen as reducing the accountability of companies, while at the same time providing users some measure of confidence in the software produced by these companies:

> More than mere tools, algorithms are also stabilizers of trust, practical and symbolic assurances that their evaluations are fair and accurate, free from subjectivity, error, or attempted influence. (Gillespie, 2014, p. 179)

The notion that algorithms are free from subjectivity is alarming when taken with another way that algorithms have been described: as ways to limit people's choices, frequently in ways that are invisible to the people whom they have control over, and are discriminatory against marginalized groups of people. If one believes that algorithms are objective and natural, then discrimination—that is institutionalized through existing social structures and further reified through algorithms that are considered to be free from bias—might be seen as simply part of the natural state of the world. Researchers (e.g., (Citron & Pasquale, 2014; Tufekci, 2015)) suggest that even when companies try to make algorithms blind to racial and sexual demographics, algorithms still make discriminatory decisions based on variables correlated with these demographics. Algorithms may also produce biased results when users train an algorithm through problematic actions (e.g., users select certain problematic advertisements which might cause an algorithm to promote those types of advertisements) or through poor initial training data.

The Bitcoin blockchain has no demographic data with which it can generate discriminatory results. However, blockchain applications tend to disproportionately benefit those who already have large amounts of financial capital—early adopters and people who can afford expensive hardware to maintain a significant share of the computing power in the peer-to-peer network. Thus, even without demographic data, many algorithms benefit already privileged groups of people.

When taken as mathematical rules, critical algorithm researchers frame algorithms as opaque, black boxes (Striphas, 2010) that are too difficult for any one person to fully understand; further complicating the issue of who (users, developers, or the technology itself) can be held responsible when they act in unintended and harmful ways. Some corporations might argue that users should be held responsible because they provide data for algorithms to use. By utilizing "the crowd" to make recommendations or decisions, corporations can disavow some level of responsibility (Striphas, 2010).

Furthermore, companies often develop new features and apply these new algorithms to user data in ways that the user could not have expected[20], suggesting that algorithms developers need to make fundamental changes to their design practices to take into account users' original intentions with shared data. Eric A. Meyer, a famous web design consultant and author, described this situation in a

[20] The output of algorithms can also be used by third parties in unexpected ways—for example, by an application which allowed websites to block people from accessing websites based on their genetic traits as determined from their 23andme data (Clark, 2015), or how police used a public genealogy database to catch the "Golden State Killer" through connecting DNA evidence to the DNA of relatives who had used a genealogy site (Kolata & Murphy, 2018).

widely shared blog post on the “algorithmic cruelty” of Facebook’s then-new “Year in Review” feature (2014). This feature was meant to remind users of the good things that happened in the last year; however, the algorithm displayed a picture of his daughter who had died earlier in the year as its cover photo. He explained that designers are not used to developing algorithms for situations such as his:

> Algorithms are essentially thoughtless. They model certain decision flows, but once you run them, no more thought occurs. To call a person “thoughtless” is usually considered a slight, or an outright insult; and yet, we unleash so many literally thoughtless processes on our users, on our lives, on ourselves. (para. 9)

Meyer’s experience demonstrates a power imbalance inherent in public relevance algorithms. Many algorithms are largely invisible, but part of Facebook’s power is also that it can selectively make things visible—it can raise content up as “a reward for interaction” (Bucher, 2012) and use the “threat of invisibility” as a means of governing users and advertisers, forcing users to participate more if they want their content to be seen. Algorithms can also make visible things that we did not even know about ourselves and determine sensitive information that we might rather keep hidden (Tufekci, 2015). When we view algorithms as black boxes, this asymmetry between algorithmic visibility and user visibility seems unavoidable—algorithms will know more about us than we can know about them—rather than viewing them as something that is designed and, therefore, can be changed.

For Bitcoin, some of the power imbalance between humans and code is not as extreme due to the transparency built into the blockchain, in which all information is pseudonymous but public, and the code is open for anyone to examine and debate. Although Bitcoin users’ trust was also predicated on the impartiality of code and they used much of the same language about objectivity as corporations did, Bitcoin's authority manifested quite differently from that of corporate algorithms.

5.2.2. Algorithms may gain authority because they are seen as more trustworthy and authoritative than existing institutions

In this section, I further examine the reasons that Bitcoin users preferred algorithmic authority over the authority of existing institutions such as governments or banks. Like the corporate discourse, participants focused on the objectivity of math, but for many in the Bitcoin community, math also took on a quality of resistance—it allowed them to trust the objectivity of Bitcoin rather than trust in the institutions and corporations they felt had failed them. Beer (2009) argued that "algorithms are carving out new complex digital divides that emerge in unforeseen and often unnoticed ways in the lives of individual agents" (p. 999) and that it will be difficult to identify and research the ways in which people resist these algorithms. However, in a reversal of Beer's concern, in this section I explore the ways in which *algorithms can explicitly and visibly act as resistance* to institutions. This is not to say that Bitcoin is an inherently resistive technology, but that it has the capacity to be used or, at the very least, be seen in that way.

Some Bitcoin users were drawn to the currency because of their dissatisfaction with current economic practices, particularly with how governments can increase their money supply, which generally causes inflation[21]. One survey

[21] While economists generally view some inflation (around 2%) as ideal for price stability (Bernanke, Laubach, Mishkin, & Posen, 2001; Board of Governors of the Federal Reserve System, 2015), these participants came from many countries, some of which had high rates of inflation at that time. Furthermore, not all participants agreed with mainstream economists.

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, told me about how he had worked at a bank for years, and felt that banks did not act in the best interest of the people. 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 the United States and Canada and they felt that the infrastructures and governments in their countries were functional, but did not align with their morals. For them, Bitcoin was seen as the potential for financial freedom from the forces governing fiat currency, which they felt they had little to no control over. 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 had a more practical purpose. Franco, a participant in Argentina, explained that in his country, the official exchange rate between US dollars and Argentine pesos was much worse than the black market exchange rate. He was employed by a US 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 US American living in China at the time of our first interview, explained that he used Bitcoin to get 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 their needs.

Some participants viewed Bitcoin as more trustworthy than governments because they considered Bitcoin to be apolitical. Survey participants described it as:

> "It's a technological solution to the problems with money. Money is about trust and math is much more trustworthy than humans."
> "[Bitcoin is] currency and transactions based on Math instead of personal interests."
> "No trust involved. I trust math more than any government or central authority."
> "It's simply more fair."

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 put misinformation on a blockchain[22] and try to spread it for their own gain, a majority of peers could choose to prevent it from

[22] Bitcoin's blockchain is primarily designed to store monetary transactions; however, some other blockchain technologies use blockchains to store a wider range of information.

making its way into the main blockchain. In other words, the wisdom of the crowd could prevent misinformation from spreading. Ken, a participant who dabbled in Bitcoin microfinance had a similar opinion, "*bitcoin is pure capitalism, plain and simple. It's property (thanks IRS) you can exchange for other property, without asking anyone's permission or paying anyone but the people who keep the network running (miners). Capitalism exists in every type of political environment, whether open or underground. […] Anarcho-capitalism is a politcal philosophy, and it happens to be one that's very compatible with a currency like bitcoin, since no central authority is necessary to issue it […] I consider it an apolitical currency, as is any cash.*" For Ken, Bitcoin was a capitalist project, but in his view, capitalism is separate from politics.

As Ken demonstrated, "apolitical" may refer to being non-partisan, or in the case of Tom, it may refer to being perceived as being grounded in a factual concreteness. In some of these interviews, there was a utopian sense that software could be developed without political biases or prejudices. For participants who had this view, Bitcoin was a versatile technology that could support many different political viewpoints, and the focus of their interest was on Bitcoin's technological aspects, rather than any explicitly political aspect.

For the participants who viewed Bitcoin as a political project (and even for many of the ones that did not), Bitcoin provided not only an alternative to institutions that they disliked, but also a possibility for overthrowing them. Some participants imagined a future in which Bitcoin would be the global currency, uniting people across the world, and ridding them of the tyranny of banks. For these participants, Bitcoin held much of the same appeal as the early Internet did. They were excited to be early adopters of a technology that they believed could transform the world and to have a hand in shaping its future. Some saw futures in which blockchains and smart contracts could replace corporate boards and governments, and provide a platform that could automate certain types of labor and management.

5.3. Algorithms as Stand-ins for Human Labor

Algorithms are sometimes represented as ways to transform work practices. When algorithms are represented as artificial managers, they are seen as a replacement for humans—completely autonomous and authoritative. The blockchain is often portrayed in this way, although Bitcoin users are cognizant of the work done by the Bitcoin peer-to-peer network. This section demonstrates that it is impossible to fully separate algorithms from humans—algorithms require some level of human intervention. Bitcoin's blockchain does manage a ledger and have authority over it, but in order to function, Bitcoin also requires human intervention and participation through mining and governance of the open source community.

5.3.1. Algorithms change the organization of human labor

Algorithms are increasingly being portrayed as stand-ins for human workers, particularly managers. There are now algorithmic journalists who produce content that is virtually indistinguishable from those written by humans (Carlson, 2015); algorithmic taxi dispatchers in the form of Uber (Lee et al., 2015); and algorithmic accountants and mints in the form of Bitcoin. In the case of each of these three systems (i.e., algorithmic journalists, Uber, and Bitcoin), algorithms are portrayed as automatically producing content and making decisions. However, research has begun to expose the ways in which these algorithms are more than just code—they are also reliant on human judgment and labor. In response to *The New York Times* article, “If An Algorithm Wrote This, How Would You Even Know?” (Podolny, 2015), a prominent figure in the Amazon Mechanical Turk (AMT) community, “spamgirl” (2015), wrote:

> Many of these articles will be "double checked" by microtaskers who ensure it reads well, giving it a tweak or two for a few cents. We're also the people who are training these algorithms to do a good job, and whenever an issue crops up, we're the ones providing the data needed to fix it. […] *Algorithms aren't really just computers spitting out text, they're a complex interaction between man and machine from which you cannot remove the man*. [emphasis added] (para. 3)

Amazon Mechanical Turks’ “artificial artificial intelligence” (coined by Amazon) is one method for giving algorithms the appearance of complete autonomy. Human labor is involved in Uber and Bitcoin as well. Uber drivers must rely on sense-making activities to understand how to interact with an algorithmic system that assigns them to passengers, manages their fare rates, and evaluates their performances. Lee et al. (2015) found that once drivers understood the system they could attempt “workaround strategies that helped them maintain control that the automated assignment did not support as part of the existing system functionality” (p. 1606-1607). Bitcoin users also relied on their judgment to determine which Bitcoin applications were safe to use and how to protect their assets. Blockchain technology also requires users to contribute their power to the peer-to-peer network. Despite the necessity of these interventions, this (human) work is largely invisible, and algorithms are typically seen as the only actants with authority in these systems.

Ekbia and Nardi (2014) define these algorithms as examples of "heteromation". They position heteromation as a form of production that is the inverse of automation:

> Technically, there has been a shift from technologies of automation, such as banking, retail, and manufacturing, the aim of which was to disallow human intervention at nearly all points in the system, to technologies of what we call heteromation that push critical tasks to end users as indispensable mediators. (What is heteromation? Section, para. 1)

Amazon Mechanical Turk is one of the most emblematic applications of heteromation. In AMT, "humans [are] rendered as bits of algorithmic function" (Ekbia & Nardi, 2014, Mechanical Turk: Micropayments for microtasks section, para 6.). AMT workers are generally recruited to perform tasks that cannot easily be performed by artificial intelligence algorithms (Irani, 2015). Requesters also use algorithms to manage workers through a sort of "automated management", by determining which tasks to show workers and helping them select tasks they would be best suited for. The employers trust AMT to produce good results because the filtering mechanisms for selecting workers are automatic and sophisticated.

For AMT requesters, the algorithm obscures the hybrid system of humans and code that are performing labor. Although requesters are aware that they are employing humans, AMT strips away much of the human aspect of this work by portraying humans as nameless computational components with which requesters do not need to interact with directly:

> Sociotechnical assemblages black box the complex politics of management into familiar acts of writing code and manipulating spreadsheets. By rendering the requisition of labor technical and infrastructural, the design of AMT limits the visibility of workers, rendering them as a tool to be employed by the intentional and expressive hand of the programmer (Irani, 2015, p. 730).

AMT requesters must trust both the filtering algorithm and their workers, even if they are rendered largely invisible by the code. Similarly, Bitcoin users must trust both the code and the miners who invisibly maintain the Bitcoin network.

Heteromation is similar to Vitalik Buterin's description of decentralized autonomous organizations (DAOs), a common concept in the large blockchain ecosystem. Buterin is a kind of celebrity in the Bitcoin community, and, among other things, he is co-founder of Ethereum (a famous blockchain-based platform/virtual machine for decentralized applications) and the co-founder *Bitcoin Magazine*. For Buterin (2014), DAOs have "automation at the center, humans at the edges" (Decentralized Autonomous Organizations section, para. 7). Buterin argues that Bitcoin is an example of a DAO. The concept of heteromation differs from that of DAOs, as heteromation's focus is on algorithms that are generally created and used by corporate entities. The corporations employing heteromation algorithms often pay workers with affective rewards or small amounts of money for their work. Most applications of the blockchain operate similarly to Bitcoin and therefore also require humans to offer their computational power to a peer-to-peer network. While the blockchain has much in common with most other heteromated systems, it is not a corporate venture in its main instantiation (Bitcoin) and, unlike most heteromated systems, some users do reap large economic benefits from the blockchain (e.g., through market speculation and through mining ventures). However, like other heteromated systems, Bitcoin does require mediation through human judgment.

5.3.2. Algorithmic authority is mediated by human judgment

Here, I 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 required 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. In this section, I will explain the main ways in which the Bitcoin community relied on human judgment.

In the absence of any formal centralized human authority, I found that Bitcoin users have to spend time and effort to discern which instances of human authority are legitimate. Most of the initial interview participants reported frequently spending 2-3 hours a day reading up on Bitcoin or communicating with other Bitcoin users. Jonathan was a participant who no longer felt that he had time to spend on Bitcoin, which perplexed me—what does it mean to spend time on a currency? When asked, he 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 participants explained that they spent time on it because 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.

Figure 6: Protester in front of MtGox's office.
Kolin Burges, a software developer from London, UK flew to Tokyo, Japan to protest in front of MtGox's offices. Source: The Wall Street Journal (Mochizuki, 2014).

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 bitcoin on the exchange's server suddenly lost their bitcoins. The closure was particularly notable because MtGox, founded in 2010, was handling 70% of all

Bitcoin transactions by 2013 (Vigna, 2014). The owners of MtGox claimed that $480 million USD of bitcoins had gone missing (Dougherty & Huang, 2014). Protesters came to MtGox's headquarters in Tokyo, Japan to confront the CEO, Mark Karpelès (Figure 6), who was later charged with embezzlement (Gibbs, 2017).

Participants argued that MtGox should have had more organizational oversight. Frankenmint, a participant whose sole source of income at the time was Bitcoin mining and investing, 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 cryptocurrencies, stated, "*I also feel bad for the people who trusted Gox and didn't understand the implications of that trust*." Earlier in this thesis, I had defined trust as the ability to reasonably predict the actions of other actors. A number of participants stressed that the world of Bitcoin is quickly evolving—bugs in the software are found, businesses shut down quickly or turn out to be scams, and regulations change. They were unable to completely trust in the supposed infallibility of Bitcoin's code or trust in the humans involved in its ecosystem.

Most participants had at some point been scammed out of bitcoins or had made an investment that was not successful. They observed that with enough experience and time, it was not difficult to tell which services were trustworthy and which were scams. One participant wrote, "*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].*" For example, Bitcoin users would share information when they suspected that a service or person was a fraud.

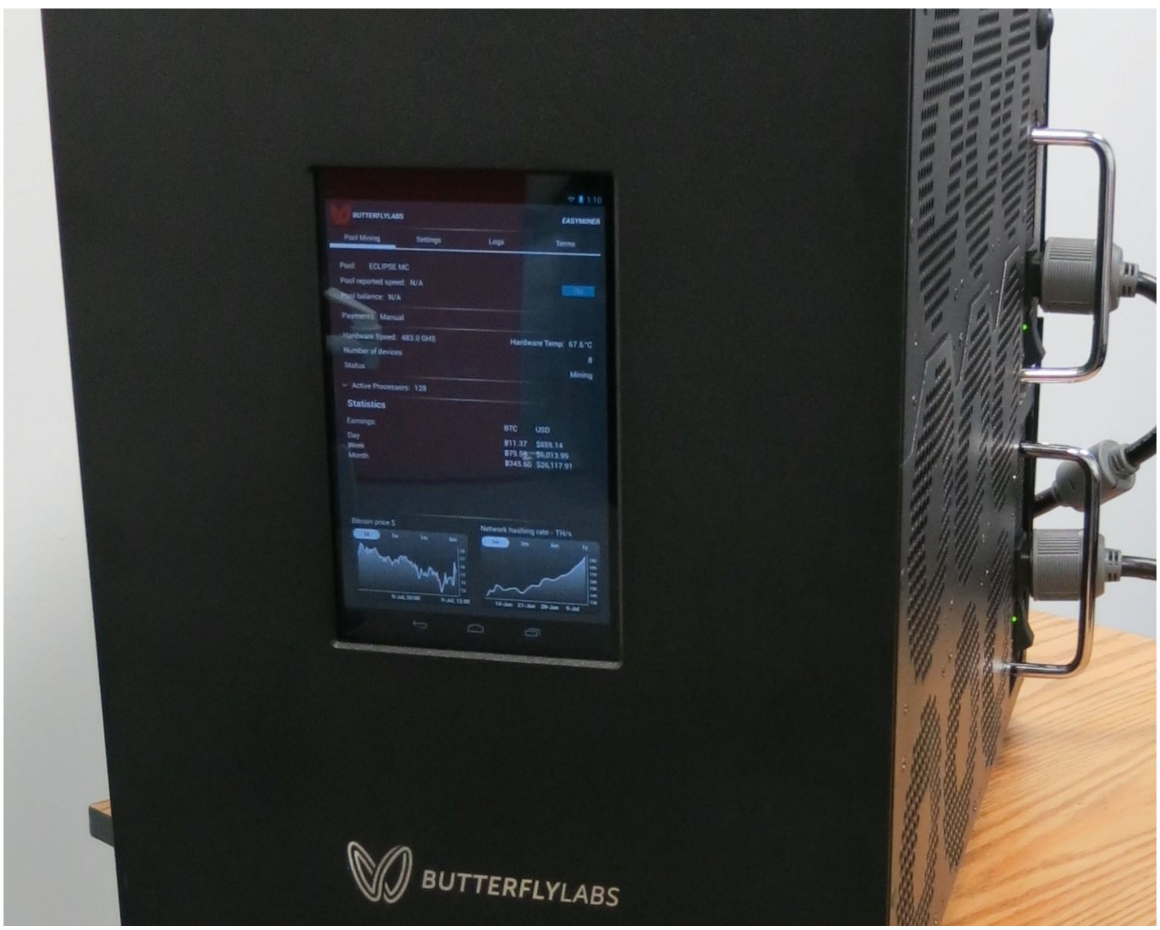

Figure 7: A Butterfly Labs miner.
Source: CoinDesk (Cawrey, 2013).

Fraud has unfortunately been a serious issue in the Bitcoin community because the transactions are irreversible and pseudonymous; in other words, once someone has conned a user into giving away their bitcoin, there is no way to for them to get it back. As a result, reputation is extremely important in the Bitcoin community, which means that in practice, Bitcoin users cannot always be pseudonymous. For example, one participant said that he had contributed to a microfinance site that took all loans in bitcoins, and he tried to only loan to people whom he thought would repay him. However, he did not have great success. Another example comes from Tom, who had pre-ordered Bitcoin miners from Butterfly Labs (example shown in Figure 7), a company whose mining hardware was popular among Bitcoin miners and thus it seemed legitimate. At the time of our interview, he, and countless others, found that his order never materialized. Butterfly Labs was shut down by the US Federal Trade Commission about five months after our interview, and it was later alleged that they used the unshipped hardware to mine for their own gain before delivering it to customers, sometimes past the point at which the hardware was competitive with others on the market (Farivar, 2016). Some users felt that others should take the perspective that Bitcoin was a high-risk experiment and did not express much sympathy for people who lost money through user error or scams.

Participants also 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 may have been stolen.

It was not just Bitcoin-related software that needed human judgment and intervention—Bitcoin miners have had to step in to prevent Bitcoin itself from facing serious problems. When version 0.8 of the 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. Buterin (2014) 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. Buterin pointed out that this "attack […] was seen by the community as legitimate" (Decentralized Autonomous Organization section, para. 5). According to Buterin's argument, the Bitcoin community saw this temporary centralization of power as more legitimately authoritative than Bitcoin's algorithms, which they had to "attack".

In a more general sense, some participants saw centralization of human resources as a necessary evil. For example, they felt that the Bitcoin Foundation was necessary for Bitcoin to be taken seriously. The Bitcoin Foundation was the unofficial public face of Bitcoin in the USA, and it interfaced with the United States government to help shape the laws that govern Bitcoin. One survey participant expressed that he didn'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*." Other participants disliked the Bitcoin Foundation because they felt that it did not represent their interests and only reflected US American concerns about government regulation of Bitcoin. Since my interviews, there have been a number of controversies about board members of the Bitcoin Foundation and the management of the foundation. However, high-profile advocates have played an important role in helping Bitcoin gain more adoption and interest from corporations.

5.4. In order to have authority, open source algorithms need institutional support and may need to adopt a level of centralization or corporatization

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 I noted earlier, Weber stated that legitimacy is a requirement for authority. While participants felt that Bitcoin had legitimate authority, they found that they sometimes had trouble convincing others of its legitimacy. Bitcoin may have rational-legal authority (and, for some people, it may have charismatic authority if they find Satoshi a compelling figure), but it does not have Weber's third type of authority: traditional authority, which may be a major drawback for some individuals. (However, some users do liken it to the Gold Standard, which may evoke traditional authority.) One participant told me that he tried to give away small quantities of bitcoin to people who he thought might find it compelling, but they almost always refused him.

Figure 8: A Bitcoin sign displayed in a shop in Montréal, Québec, Canada. April 27, 2018.

Legitimacy and authority were important to participants, because without them, participants were limited in what they could do with Bitcoin due to poor institutional support for the currency. Participants reported that brick-and-mortar businesses that accepted bitcoin were few and far between. (See Figure 8 for an example of such a business.) While some participants made purchases with bitcoins at such businesses, primarily restaurants and gas stations, most made their purchases online. Of the participants who tried to use bitcoin at brick-and-mortar businesses, most reported some difficulty in completing the transaction. For example, Franco tried to pay for a meal at a restaurant that proudly advertised that they accepted bitcoins, but no employees knew how to charge him. They ended up calling the restaurant's owner and walking through the transaction over the phone.

One method of using bitcoin at businesses that did not accept the currency was to use a website such as gyft.com to buy gift cards. Gyft.com uses the service BitPay to accept Bitcoin transactions and automatically transfers bitcoins into local fiat currency. This method of paying for goods with bitcoins show that participants were unable to avoid using fiat currency completely—not due to hypocrisy but rather the difficulty in doing so (see (Hill, 2014) and (Pitcher & Lebaron, 2015) for examples of people have tried to use Bitcoin for all purchases)[23]. This peculiar transformation of fiat currency to bitcoin in order to turn it back into fiat currency again exemplifies the complicated relationship between Bitcoin and fiat currency. For some Bitcoin users who purchased gift cards, it was for the novelty of the experience—many participants described Bitcoin as "fun"—but for others, it was a show of support for the currency.

[23] I have tried to pay for meals with bitcoin on at least four different occasions—once in San Francisco and three times in San Diego. At these restaurants, I was either told that they did not accept bitcoin anymore, that the machine that they used was out of order, or they denied ever accepting bitcoin.

As a result of this poor institutional support, many Bitcoin users simply amassed bitcoins. Keith, a participant who had written white papers on future uses of the blockchain and similar technologies, stated, "*I believe Bitcoins are a commodity trying to function like a currency. In reality Bitcoins are more like bearer shares but the Bitcoin community wants it to act like a currency*." One participant, Misal, wrote about the complexities of using bitcoin in India. What Misal observed in India corresponded with what I heard from participants in other regions of the world as well. He wrote, "*In the Indian ecosystem, bitcoin is still just a holding asset – this is not going to help the Indian bitcoin community to grow. In India If people wants to make it a sustainable currency in the longer run, then there should be an intrinsic value to it. And that comes when people start using that currency*." Some participants who held onto the currency viewed it like a stock—they "worked" for Bitcoin by mining, and they were paid in company stock. It was in their best interest to promote their company, because it would increase the value of their stock. This behavior demonstrates the difference in how some users used bitcoin (as something other than a currency) and the stated values of most participants in the first study.

As noted earlier, many participants reported spending multiple hours a day on Bitcoin; however, it was uncommon to find participants who actually made frequent transactions. In a survey of Bitcoin conducted by a community member, IceTurtle4 (2014), 29% of respondents reported that they had never purchased anything with Bitcoins, and 62% had not purchased anything with bitcoins in the last 30 days. However, only 6% did not have any bitcoins, suggesting that most of the users who had not spent bitcoins were in possession of them, but were unable or unwilling to spend them. While some bitcoins may be lost to people whose wallets they no longer remember the password for, people who no longer use bitcoin, or people who treat bitcoin as a long term investment—it was also the case that some Bitcoin users held onto bitcoins in the hopes that in the future there would be a better infrastructure in place for using them.

In addition to Misal, there were other participants who lamented the fact that it was not more useful in their regions of the world. However, they did not feel that it was a problem with Bitcoin itself; integrating Bitcoin into other institutions was crucial, either through laws or third-party applications. For this reason, one participant argued that regulation is *"[n]ecessary, unavoidable, and not so onerous as it has been made out to be. I think the major governments of the world recognized right off the bat that this couldn't be contained, so their moving to integrate it.*"

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: 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 allows for pseudonymous transactions, it has been used as a currency of digital black markets, the most well-known being the now defunct Silk Road, which was primarily a marketplace for drugs until it was shut down by the FBI in 2013. However, most of my participants were adamantly against using Bitcoin for illegal purchases because they felt that the association would undermine Bitcoin's legitimacy and authority 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 although he had been interested in Bitcoin when he had first heard of it, he did not try it at first because he thought that it was only good for black market purchases; he did not want to be associated with illegal activity.

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 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."*

However, some participants were not worried about seeming extreme; instead, they were concerned about negative effects from appealing to larger institutions.

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. While at the time of writing this thesis, Bitcoin itself has not garnered much use by centralized, commercial entities, many companies are now considering using blockchain technology to make certain tasks more efficient. Insurance companies have expressed interest in using blockchains for the insurance market because they are unalterable and transparent (Mainelli & von Gunten, 2014). Governments have identified blockchains as an efficient way of managing property records; for example, the Honduran government may be developing a blockchain solution with the blockchain company Factom to manage land title records in order to create a solution to ongoing issues with corruption and mismanagement[24]. A report from Santander Bank's InnoVentures group suggests that if banks adopt the blockchain or a similar type of distributed ledger, it "could reduce banks' infrastructure costs attributable to cross-border payments, securities trading and regulatory compliance by between $15-20 billion per annum by 2022" (Belinky et al., 2015, p. 15). R3 is a consortium of over 200 financial companies and banks that have come together to research and develop blockchain technologies. Microsoft has developed a "Blockchain as a Service" (BaaS) platform for its cloud

[24] Although it was initially announced that Factom had made a deal with the government, the validity of this claim has come into question, as well as whether this project will be completed (as of May, 2018). Nevertheless, this project provides a compelling example of how smart contracts could be used.

computing service Azure, as a mechanism for developers to easily test and deploy blockchains, and there are a number of other large technology companies (e.g., IBM and Amazon) who also have their own BaaS platforms.

In addition to non-Bitcoin blockchains being considered for use in centralized organizations, the infrastructure of Bitcoin itself has become increasingly centralized, as demonstrated by the dramatic difference between mining farms shown in Figures 9 and 10. Keith argued that Bitcoin will eventually evolve into the same centralized capitalist institutions that many Bitcoin users at the time opposed, "*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 cryptocurrencies] in competition.*" Colin, who ended up deciding to stop using and mining bitcoins three months after our interview, asked, "*How does the individual miner compete with the corporate mining farms? – well, they don't, do they?*"

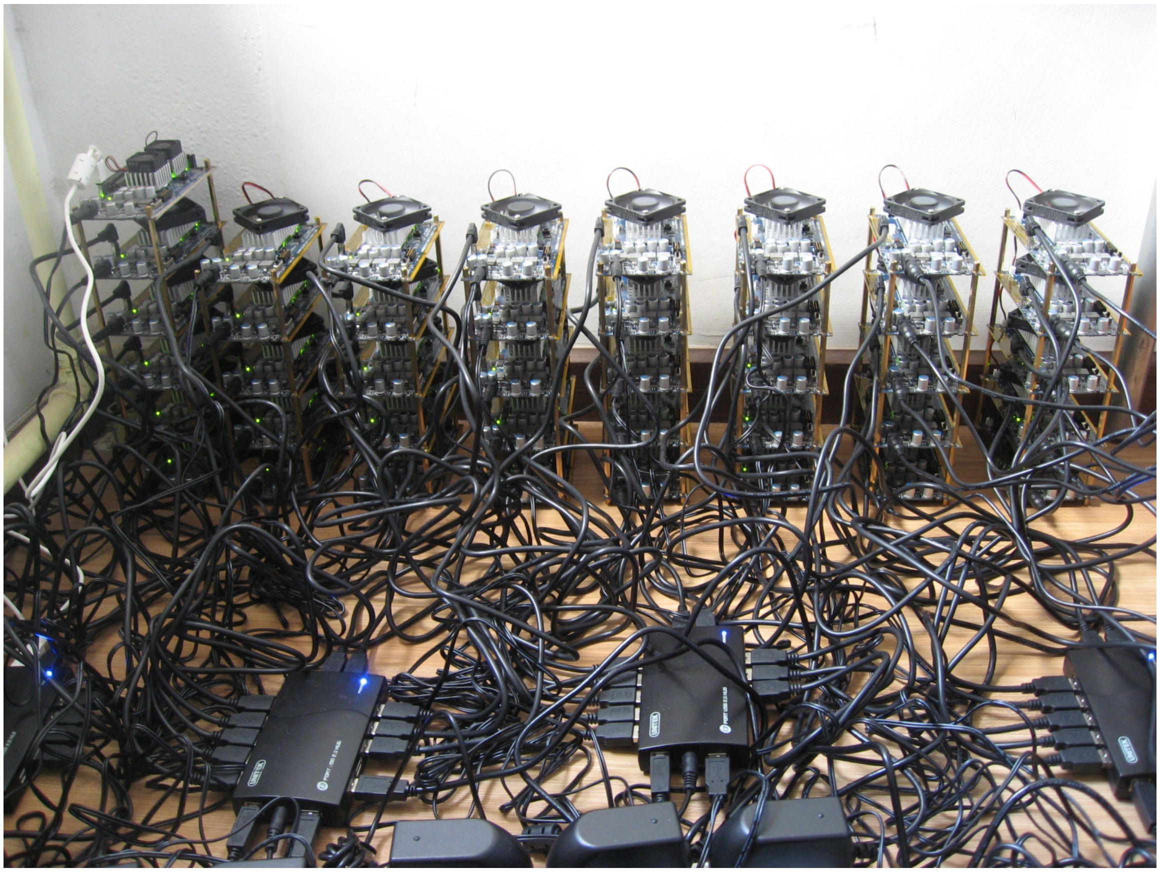

Figure 9: Bitcoin miners in 2015.
Photograph "Icarus Bitcoin Mining rig" by Xiangfu, 2015 (https://commons.wikimedia.org/wiki/File:Icarus_Bitcoin_Mining_rig.jpg) distributed under a CC-BY-SA-4.0 license (https://creativecommons.org/licenses/by-sa/4.0/legalcode)

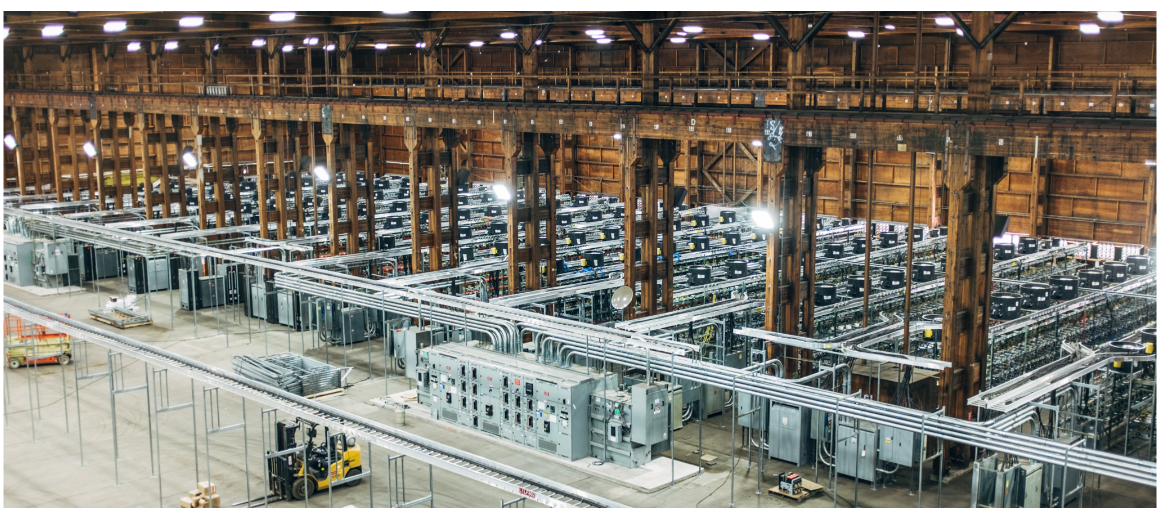

Figure 10: Bitcoin.com Pool's large-scale mining farm in 2017.
Source: pool.bitcoin.com, 2017 (https://pool.bitcoin.com/)

Since Bitcoin's inception in 2009, it has become increasingly difficult for the average person to mine bitcoin. Up until the middle of 2010, bitcoin mining could be done with a home computer with CPUs (central processing units); from then until the middle of 2011 it was something that one could only do with computers built with many GPUs (graphical processing units) or FPGAs (field programmable gate arrays) (Figure 9); and from 2013, it only became profitable to mine with specialized hardware referred to as ASICs (application specific integrated circuits), which were designed for the sole purpose of mining bitcoin (Figures 5, 7, and 10) (Velasco González, 2016). Taylor (2013) described the typical profile of Bitcoin miners around the time that ASICs were introduced:

> 1. High school and college students making use of cheap electricity and/or hardware from their parents or universities;
> 2. Gamers who subsidize their game machines by running GPU bitcoin mining codes on them when not in use;
> 3. Extreme hobbyists that buy multiple machines ("mining rigs") until they max out the cooling capacity of their basements (and/or the tolerance of their spouses);
> 4. Hackers deploying botnets robbing computation from networks of zombie machines;
> 5. Online collaboratives that raised funding to purchase mining hardware and share in profits, and
> 6. Companies that raised funding from Bitcoin enthusiasts via an IPO [initial public offering] on a BTC-denominated non-SEC [US Securities and Exchange Commission]-regulated online stock exchange, and are designing ASIC hardware to mine BTC and distribute dividends. (p.2)

With the proliferation of Bitcoin mining, this profile has changed considerably. There are now huge mining farms (see: Figure 10) in places where electricity is cheap (e.g., hydroelectric power, geothermal power, and coal, or, in the case of Venezuela, subsided by the government) and often in excess, such as East Wenatchee, Washington, USA; China; Venezuela; and Iceland (Chun, 2017; Hern, 2018; Hileman & Rauchs, 2017; Roberts, 2018). It is calculated that 58% of the mining farms with 1% or greater of the power in the Bitcoin network are located in China (Hileman & Rauchs, 2017). ASICs have lower electricity requirements than the other forms of mining, but Bitcoin mining has been calculated to consume roughly as much power as the country of Chile (Digiconomist, 2018; Vries, 2018). However, it is very difficult to know whether these calculations are correct; others have calculated that the actual electricity usage is about half the rate that the Bitcoin Energy Consumption Index suggests (Bevand, 2018). Regardless of the exact number, bitcoin mining consumes a staggering amount of energy[25]. ASICs are also completely useless once they break and cannot be recycled, raising concerns about e-waste. The design of the blockchain introduces the notion of artificial scarcity of Bitcoin, but the design of the hardware level of Bitcoin is driven by the idea of "superabundance" which is "underpinned by the idea that digital resources are not bounded" (Velasco González, 2016, Hardware Layer: Energy E-waste, and Efficiency section, para. 8). This perceived divorce from the materiality of mining permeates many of the discussions in the Bitcoin community.

The centralization of mining has other environmental risks because of the power that large miners have to determine the future of the network and their unwillingness to considerably change the algorithm of Bitcoin to one that is more energy-efficient. "40% of large miners rate their influence over protocol

[25] Some Bitcoin advocates argue that a high energy consumption may be not be a bad thing, because it means that Bitcoin is more secure. They contend that when there is high computing power in the network, it is more difficult for any actor to take control of it.

development as very high, compared to only 16% of small miners" (Hileman & Rauchs, 2017, p. 41), and yet:

> a quarter of small miners are open to the possibility of switching to another, less energy-intensive consensus algorithm in the future – no large miner agrees with this statement, though. Changes to the consensus algorithm may lead to a loss of investment in mining equipment that is specifically designed to only perform the calculations required by the current [proof-of-work] algorithm. (p. 100)

Miners are aware of the risk to the environment, but "39% of small miners and 73% of large miners state that the benefits of having a secure distributed computer network outweigh the environmental costs" (p. 99), and they believe that "for now most agree that [reducing the carbon footprint of mining] is a minor concern compared to other challenges that cryptocurrency systems currently face" (p. 100). Some other cryptocurrencies and blockchains use different consensus algorithms than Bitcoin's that are designed to make it more difficult for mining to be centralized and use less electricity (e.g., Litecoin's scrypt algorithm and Ethereum's proposed use of the Casper proof-of-stake protocol).

For many participants, it was blockchain technology, not Bitcoin that they had high hopes for. 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 cryptocurrencies 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 institutions they rejected, alternatives were essential, and the concept of the blockchain itself was what held authority.

Chapter 6. Tensions Between Reality and Ideals

My findings showed considerable variance in how participants viewed Bitcoin and the blockchain. One participant imagined a future in which cryptocurrencies would be used to provide a universal basic income, whereas another participant viewed Bitcoin as a tool to promote the vision of libertarianism espoused by US politician Ron Paul. Some participants were crypto-anarchists. There were participants who found the pseudonymity of Bitcoin to be extremely important and other participants who disliked its pseudonymous aspect. There were participants who wanted more government regulation of Bitcoin and others who hated the idea of any government regulation whatsoever. Many participants had certain demographic characteristics in common, but they clearly had varying political views. Most held beliefs that could broadly be described as libertarian, but those beliefs were articulated in different ways among participants.

In the following, I briefly review the tensions between the ideals of different members within community, as well as the tensions between ideals and the reality of Bitcoin during the time of my study:

- *Political or apolitical:* Some participants saw Bitcoin's algorithms as apolitical and incorruptible tools. As a result, they preferred them over the practices of existing institutions which were governed by corruptible human beings. However, some participants saw this departure from traditional institutions as a political choice. For some participants, it was meaningful to distinguish whether they felt that the project was political or apolitical because the distinction aligned them with certain viewpoints on Bitcoin's purpose.

- *Centralized or decentralized:* Despite the consensus among the participants that human-led institutions are less trustworthy than those run by software, some participants also argued that some level of human oversight and judgment was necessary for Bitcoin to function smoothly. These participants were not necessarily arguing for hierarchical governance, but rather governance through consensus on major decisions and a neo-liberal sense of personal accountability. The role of human intervention in the operation of Bitcoin was debated among users and some felt that certain methods of intervention were contradictory to Bitcoin's decentralized values.
- *Promoting resistance or reifying institutional hegemony:* Many participants argued that existing institutions—the same ones that many of them rejected—needed to support Bitcoin for it to gain widespread adoption. While some participants indicated that widespread adoption would ultimately be positive for Bitcoin, others were concerned that adoption would cause Bitcoin to become like the very institutions they opposed. For participants who raised these concerns, the authority of the blockchain was decoupled from the authority of Bitcoin, and they said that they would start using another cryptocurrency if Bitcoin became more centralized.
- *Contradictions between desires and reality:* Participants held many utopian ideals and hopes for the ways that Bitcoin could change the world. However,

many acknowledged that the social norms and regulations around Bitcoin were still being developed. It was often compared to the Wild West or the early days of the Internet, and while they believed its transformative power for economic systems could be as great as the Internet was for telecommunication systems, it was unclear when and how that shift would happen. Many participants admitted that they did not even use Bitcoin as a currency because they had nowhere to spend it. For some, Bitcoin was more like a stock or a commodity.

Algorithmic authority is always made up of trust in both code and humans, which are part of an algorithmic assemblage; however, algorithmic authority is not always derived from trust in all parts of an assemblage. Rather, it may primarily come from the perceived trustworthiness of just one part of this assemblage (i.e., the code or the humans). These two types of algorithmic authority (i.e., code and human) are demonstrated in the tensions listed above. It was not that different factions of actors in the blockchain community wanted the blockchain to have less authority, but rather that they placed their trust in different actants.

6.1. Authority and utopia

As described in Chapter 5 (and summarized in Table 2[26]), my participants were on a spectrum between two poles: those that hoped that Bitcoin could provide a new disruptive authority and those that felt that Bitcoin was only valuable to the

[26] Thank you to Hope Sisley for suggesting that I add the bottom row of the table.

extent that it could be utilized and integrated into existing institutions. For participants who were concerned with Bitcoin as a disruptive technology, the appeal of Bitcoin was based on utopian visions of a technology unhindered by centralized institutions or human judgment. For them, the blockchain algorithm was at the heart of the disruption; Bitcoin itself was just one application of the blockchain.

Table 2: Summary of tensions between utopian ideals and reality

Utopian ideals	Reality
Bitcoin's algorithms are valued because they do not require trust in humans.	In practice, Bitcoin still requires human oversight and mediation.
Bitcoin's algorithms are valued because they are independent from institutions that are corrupt or imperfect.	In practice, Bitcoin still requires some degree of institutional support.
Bitcoin is accessible to everyone who wishes to use it and will promote a more egalitarian society.	Bitcoin mining and politics are increasingly dominated by corporate-like entities rather than individuals.

The utopian vision that inspired Bitcoin is an example of an *incomplete utopian project* (Gregory, 2000). Gregory argued that utopian projects are characterized by persistence: "utopian projects outlive any particular attempt at realization, nor is any particular failure sufficient to spell the end of a utopian quest" (p. 198). The diversity of alternate technologies that are based on blockchain technology could provide the heterogeneity needed to continue with the utopian visions of participants if Bitcoin fails to live up to their expectations.

Indeed, the growing centralization of Bitcoin's governance points to the impossibility of its ever living up to the utopian ideals of the Bitcoin community. While it is true that some participants were in favor of some forms of regulation, they largely viewed it as a necessary evil and not as a desirable future for Bitcoin. Similarly to how participants had different definitions of what it means to be (a)political, Bitcoin users understood centralization in different ways.

While it is true that Bitcoin's protocols operate in decentralized ways, many other aspects of Bitcoin are not as decentralized as they seem at first glance. The failure of Bitcoin to be fully decentralized was demonstrated by temporary configurations of centralized power, such as the group of miners who decided to fix the issue with version 0.8, as described earlier. One user wrote about this incident on /r/bitcoin, "*centralization was kind of important in mitigating this issue. we had big pools of miners able to do as needed instead of individuals. we also had a dev team we depended on to guide us through*." Another user replied, "*It only needed centralization of leadership, rather than centralization of authority. We didn't need a central authority mandating a certain change. We just needed a central authority suggesting a change that others can choose to heed or ignore*." For this person, centralization implied a coercive form of authority that was undesirable. Weber (1978) distinguished authority from power by arguing that authority is supported by legitimacy, whereas power is supported by coercion. If we use Weber's terminology, then the second commenter was arguing that centralization is not always coercive, but can be legitimately authoritative.

Bitcoin's code may be open source, but it is still produced in a hierarchical way. At the time of writing, there are few programmers who actively work on the code. When I worked on my first study, I calculated that, as of October 14, 2014, 73.6% of the code was committed by only eight developers out of 252 contributors[27]. This sort of hierarchy is not uncommon in open source software:

> Commons-based peer production, observe Benkler and Nissenbaum [2006], emerges in environments driven by collaborative efforts and results from the meeting of free individuals allergic to 'managerial hierarchies'; but, as often happens with human things, the shattering of old hierarchies ends up producing new ones, as blatantly revealed by the statistical measures of online activities and by their compliance with the '80/20 rule' of power law distributions[28]. (Miconi, 2012, p. 93)

It may be that Bitcoin, and other algorithms that are seen as subversive, may only have authority as long as they are seen as such. As soon as they replace the old ways of doing things, these algorithms are no longer disruptive technologies, but instead are the new technologies to be disrupted. In Weberian terms, these algorithms may no longer be examples of charismatic or rational-legal authority, but become examples of traditional authority, which are in their nature conservative and resistant to change. Keith Hart (2014) spoke to the ways in which Bitcoin-related services are much more traditional than they first appear:

> Bitcoin—like neoliberalism that it mimics, dreams of markets and money without politics or the state. This dream is an illusion. If you don't accept that markets and money depend on politics, then the politics go underground. In the case of Bitcoin, 80% of all transactions were taking place with MtGox. It operated control over Bitcoin in a way that any central bank would desire, but could not realize.

As Hart suggests, Bitcoin may be more traditional than its users would desire. Yet Bitcoin may have authority simply because the values in the code can be interpreted in so many different ways by users. For some users, Bitcoin may be

[27] Calculated by using bitcoin.org/development

[28] The Pareto principle, created by quality management pioneer Juan M. Juran, states, "80 percent of consequences stem from 20 percent of causes" (Bunkley, 2008, para. 3). And indeed—in late 2014, I calculated that 20% of the Bitcoin contributors were committing exactly 80% of the code.

appealing because of its incompleteness, and, as Barocas et al. (2013) argued, the difficulty of understanding algorithms makes it easy to attribute all kinds of values and effects to them. Similar to the corporate rhetoric that uses “the algorithm” to appeal to a number of different audiences, Bitcoin may be able to appeal to different audiences because the politics of its creator were never explicitly stated. Satoshi, who left the project in 2010, likely had libertarian or anarchist motives, but his motives are still debated a decade after the Bitcoin white paper was disseminated.

At the time of my first study, my research suggested that these potential deterrents from using Bitcoin (i.e., ambiguity about purpose, mismatch between reality and ideals, and the diversity of views in the Bitcoin community) were not enough for participants to abandon the currency or their utopian ideals. These tensions were not serious threats to the community because there had not been any major conflicts about changes to the code, which was ultimately one thing that the entire community trusted.

However, in recent years, the scaling debate (which began in earnest in mid-2015) has shown that differing values have had real consequences on the cohesion of the Bitcoin community. As Bitcoin has become more popular, the community has been concerned with how to scale Bitcoin in order to support a larger volume of transactions. Community debates about how to change the code have at times been centered on how to best scale Bitcoin in order to support certain visions of the future. There has been increasing tension between people who have different ideas about what governance of the code should look like and how much power the developers (as opposed to the larger community) should have to make major decisions about the code. Furthermore, Bitcoin mining has become increasingly centralized, and it has become extremely difficult for the average person to mine successfully because the cost of competitive hardware is so high and the cost of electricity to run mining machines in some regions makes it prohibitively expensive.

Ultimately, there is a growing rift between those that have placed the majority of their trust in the blockchain as transparent, visible, and revolutionary code, and those that have viewed it as technology that could gain support from more conventional institutions and eventually become (invisible) infrastructure.

6.2. Authority and Trust

At the beginning of the thesis, I argued that trust in an actor comes from being able to predict how that actor will behave, something that is easier with an 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 has been expanded on by Andreas Antonopoulos, a famous advocate and author in the Bitcoin community, in the article, "Bitcoin security model: trust by computation" (2014). Antonopoulos 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" (para. 4). According to Antonopoulos, as long as over half of the computing power is controlled by what Satoshi referred to as "honest nodes" (i.e., network nodes that will not try to manipulate the blockchain for their own gain), 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. Antonopoulos' concept of why users trust the Bitcoin network suggests that Bitcoin is a heteromated system in which it is *essential* for human actors to offer their computing power (through mining) to the system, in order to make the system trustworthy.

A similar perspective on trust was offered by Maurer et al. (2013), 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" (p. 273). 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. The distinction between network (Antonopoulos) and code (Maurer et al.) is an important one, in that one implies a trust in the wisdom of the masses and the other implies trust in technological processes, respectively.

I 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 or in the network. Bitcoin's code is subject to change, and on rare occasions it has had serious errors (such as the issue with the 0.8 version of the software). Problems in the code can prevent the network from behaving correctly. 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 perform other tasks that became heteromated.

The Bitcoin community contributed to the functioning of Bitcoin in heteromated ways beyond computing power; they helped maintain the code, avert crises, and assess the trustworthiness of Bitcoin organizations and companies. 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, in part because they had difficulty trusting others. Therefore, trust in Bitcoin required trust in more than just the code or the network, but also trust in the ecosystem of services offered for the currency.

At the time of this study, there was little regulation of Bitcoin and so participants were at greater risk when using third party applications and services, and researching them 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 might 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.

People confer authority on an algorithm when they feel that they can trust the assemblage of actors associated with the algorithm. In the case of Bitcoin, developing this trust is difficult in the absence of formal centralization or rules that can prevent fraud or theft. Developing this trust without centralization is time consuming and may not scale well as both the Bitcoin user base and the number of Bitcoin related applications grow.

Chapter 7. Conclusion and Future Work

More research is needed to better understand the ways in which algorithmic authority can best be used to empower users, and whether certain aspects of technologies like Bitcoin—such as transparency, openness, and decentralization—could prevent some of the ethical problems that are inherent in closed source algorithms and could perhaps make it easier to successfully audit algorithms for bias. My hope is that those in the critical algorithm studies field will take up research on a broader range of algorithms in order to explore these questions.

As Bitcoin evolves, more research will also be needed to understand the relationship between the centralized institutions that so many of its users oppose and the decentralized algorithmic authority of Bitcoin. More work is also needed to learn about the current users of Bitcoin—there is little research, particularly recent research, on the users. The Bitcoin community has changed considerably over the years, and more interviews and surveys must be conducted to understand the values of current users and how these users place authority in the blockchain.

In this thesis, I examined the concept of algorithmic authority and discussed the ways in which Bitcoin users trust in the code and in their own judgment. I described how algorithmic authority does not just reside in code, but in a diversity of sociotechnical actants. However, I found that my participants were of two minds about the potential algorithmic authority of Bitcoin. One group hoped that Bitcoin and the blockchain would provide a new disruptive authority. The other group felt that Bitcoin is only valuable to the extent that it can be utilized and integrated into existing institutions. For participants concerned with Bitcoin as a disruptive technology, 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. If Bitcoin fails to live up to user expectations, the diversity of blockchain technologies could provide the heterogeneity needed to support their utopian dreams. Whether or not Bitcoin exists in the future, it has provided a valuable lens for understanding the authority of algorithms; perceived, endowed, and actual.

References

Angwin, J., & Parris, T., Jr. (2016, October 28). Facebook Lets Advertisers Exclude Users by Race. Retrieved November 1, 2016, from http://arstechnica.com/information-technology/2016/10/facebook-lets-advertisers-exclude-users-by-race/

Antonopoulos, A. (2014). Bitcoin security model: trust by computation - O'Reilly Radar. Retrieved October 4, 2015, from http://radar.oreilly.com/2014/02/bitcoin-security-model-trust-by-computation.html

Barocas, S., Hood, S., & Ziewitz, M. (2013). *Governing Algorithms: A Provocation Piece* (SSRN Scholarly Paper No. ID 2245322). Rochester, NY: Social Science Research Network. Retrieved from http://papers.ssrn.com/abstract=2245322

Barok, D. (2011). Bitcoin: censorship-resistant currency and domain name system to the people. *Piet Zwart Inst*.

Bashir, M., Strickland, B., & Bohr, J. (2016). What Motivates People to Use Bitcoin? In *Social Informatics* (pp. 347–367). Springer, Cham. https://doi.org/10.1007/978-3-319-47874-6_25

Baur, A. W., Bühler, J., Bick, M., & Bonorden, C. S. (2015). Cryptocurrencies as a Disruption? Empirical Findings on User Adoption and Future Potential of Bitcoin and Co. In M. Janssen, M. Mäntymäki, J. Hidders, B. Klievink, W. Lamersdorf, B. van Loenen, & A. Zuiderwijk (Eds.), *Open and Big Data Management and Innovation* (pp. 63–80). Springer International Publishing. https://doi.org/10.1007/978-3-319-25013-7_6

Bauwens, M. (2005). The political economy of peer production. *CTheory*. Retrieved from http://www.ctheory.net/articles.aspx?id=499

Bauwens, M. (2014, September 9). A political evaluation of bitcoin. Retrieved January 12, 2018, from https://blog.p2pfoundation.net/a-political-evaluation-of-bitcoin/2014/09/09

Beer, D. (2009). Power through the algorithm? Participatory web cultures and the technological unconscious. *New Media & Society*, *11*(6), 985–1002.

Belinky, M., Rennick, E., & Veitch, A. (2015). *The Fintech 2.0 Paper: rebooting financial services*. Santander InnoVentures.

Benkler, Y. (2006). *The Wealth of Networks: How Social Production Transforms Markets and Freedom*. Yale University Press.

Berlinski, D. (2001). *The Advent of the Algorithm: The 300-Year Journey from an Idea to the Computer* (1 edition). New York: Mariner Books.

Bernanke, B. S., Laubach, T., Mishkin, F. S., & Posen, A. S. (2001). *Inflation Targeting: Lessons from the International Experience*. Princeton University Press.

Bevand, M. (2018, March 21). Serious faults in Digiconomist's Bitcoin Energy Consumption Index. Retrieved June 4, 2018, from http://blog.zorinaq.com/serious-faults-in-beci/

Bitcoin Student. (2014, July 23). Results of a 3,000+ person Bitcoin survey [Tumblr post]. Retrieved May 9, 2018, from https://bitcoinstudent.tumblr.com/post/92669241028/results-of-a-3000-person-bitcoin-survey

Blass, A., & Gurevich, Y. (2003). Algorithms: A quest for absolute definitions. *Bulletin of European Association for Theoretical Computer Science*, *81*.

Blendon, R., & Benson, J. (2009). America's Response to a Deep Recession. *Challenge*, *52*(4), 32–52. https://doi.org/10.2753/0577-5132520404

Board of Governors of the Federal Reserve System. (2015, January 26). The Fed - Why does the Federal Reserve aim for 2 percent inflation over time? [FAQ]. Retrieved June 3, 2018, from https://www.federalreserve.gov/faqs/economy_14400.htm

Boellstorff, T. (2013). Making big data, in theory. *First Monday*, *18*(10). Retrieved from http://firstmonday.org/ojs/index.php/fm/article/view/4869

Bohr, J., & Bashir, M. (2014). Who Uses Bitcoin? An exploration of the Bitcoin community. In *2014 Twelfth Annual International Conference on Privacy, Security and Trust* (pp. 94–101). https://doi.org/10.1109/PST.2014.6890928

Bowker, G. C. (1994). *Science on the Run: Information Management and Industrial Geophysics at Schlumberger, 1920-1940*. MIT Press.

Bowker, G. C. (2005). *Memory Practices in the Sciences*. MIT Press.

Bruckner, M. A. (2018). The Promise and Perils of Algorithmic Lenders' Use of Big Data. *Chicago-Kent Law Review*, *93*, 3–60.

Bucher, T. (2012). Want to be on the top? Algorithmic power and the threat of invisibility on Facebook. *New Media & Society*, *14*(7), 1164–1180.

Bunkley, N. (2008, March 3). Joseph Juran, 103, Pioneer in Quality Control, Dies. *The New York Times*. Retrieved from https://www.nytimes.com/2008/03/03/business/03juran.html

Burrell, J. (2016). How the machine 'thinks': Understanding opacity in machine learning algorithms. *Big Data & Society*, *3*(1), 2053951715622512. https://doi.org/10.1177/2053951715622512

Buterin, V. (2014a). Hi, we are the Ethereum Project Team. Ask us anything! • r/IAmA [Reddit comment]. Retrieved June 4, 2018, from https://www.reddit.com/r/IAmA/comments/2bjmgb/hi_we_are_the_ethereum_project_team_ask_us/

Buterin, V. (2014b, May 6). DAOs, DACs, DAs and More: An Incomplete Terminology Guide. Retrieved October 4, 2015, from https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/

Carlson, M. (2015). The Robotic Reporter. *Digital Journalism*, *3*(3), 416–431. https://doi.org/10.1080/21670811.2014.976412

Cawrey, D. (2013, July 22). Inside Butterfly Labs: The ASIC bitcoin mining arms race. Retrieved June 2, 2018, from https://www.coindesk.com/inside-butterfly-labs-the-asic-bitcoin-mining-arms-race/

Cheney-Lippold, J. (2011). A New Algorithmic Identity Soft Biopolitics and the Modulation of Control. *Theory, Culture & Society*, *28*(6), 164–181. https://doi.org/10.1177/0263276411424420

Chun, R. (2017, September). Big in Venezuela: Bitcoin Mining. *The Atlantic*. Retrieved from https://www.theatlantic.com/magazine/archive/2017/09/big-in-venezuela/534177/

Citron, D. K., & Pasquale, F. A. (2014). The Scored Society: Due Process for Automated Predictions. *Washington Law Review*, *89*, 1–33.

Clark, L. (2015, July 23). How one coder used 23andMe to create a race wall around the web. Retrieved May 28, 2018, from http://www.wired.co.uk/article/23andme-api-blocks-based-on-race-gender

CoinDesk. (2015, June 10). New CoinDesk Report Reveals Who Really Uses Bitcoin. Retrieved May 9, 2018, from https://www.coindesk.com/new-coindesk-report-reveals-who-really-uses-bitcoin/

Coleman, J. A. (1997). Authority, Power, Leadership: Sociological Understandings. *New Theology Review*, *10*(3). https://doi.org/10.17688/ntr.v10i3.563

Datta, A., Tschantz, M. C., & Datta, A. (2015). Automated Experiments on Ad Privacy Settings. *Proceedings on Privacy Enhancing Technologies*, *2015*(1), 92–112. https://doi.org/10.1515/popets-2015-0007

De Filippi, P., & Loveluck, B. (2016). The Invisible Politics of Bitcoin: Governance Crisis of a Decentralized Infrastructure. *Internet Policy Review*, *5*(3). Retrieved from https://policyreview.info/articles/analysis/invisible-politics-bitcoin-governance-crisis-decentralised-infrastructure

Digiconomist. (2018). Bitcoin Energy Consumption Index. Retrieved June 4, 2018, from https://digiconomist.net/bitcoin-energy-consumption

Dougherty, C., & Huang, G. (2014). Mt. Gox Seeks Bankruptcy after $480 Million Bitcoin Loss. *Bloomberg*.

DuPont, Q. (2014). The politics of cryptography: Bitcoin and the ordering machines. *Journal of Peer Production*, *1*(4). Retrieved from http://hplusmagazine.com/2014/05/07/the-politics-of-cryptography-bitcoin-and-the-ordering-machines/

DuPont, Q., & Campbell-Verduyn, M. (2017). Experiments in Algorithmic Governance: A history and ethnography of "The DAO," a failed Decentralized Autonomous Organization. In *Bitcoin and Beyond*. Routledge.

Ekbia, H., & Nardi, B. (2014). Heteromation and its (dis)contents: The invisible division of labor between humans and machines. *First Monday*, *19*(6). http://dx.doi.org/10.5210/fm.v19i6.5331

Ekbia, H., & Nardi, B. (2017). *Heteromation, and Other Stories of Computing and Capitalism*. MIT Press.

Elsden, C., Manohar, A., Briggs, J., Harding, M., Speed, C., & Vines, J. (2018). Making Sense of Blockchain Applications: A Typology for HCI. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (pp. 458:1–458:14). New York, NY, USA: ACM. https://doi.org/10.1145/3173574.3174032

Elsden, C., Nissen, B., Jabbar, K., Talhouk, R., Lustig, C., Dunphy, P., … Vines, J. (2018). HCI for Blockchain: Studying, Designing, Critiquing and Envisioning Distributed Ledger Technologies. In *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems* (p. W28:1–W28:8). New York, NY, USA: ACM. https://doi.org/10.1145/3170427.3170602

Eyal, I., & Sirer, E. G. (2014). Majority Is Not Enough: Bitcoin Mining Is Vulnerable. In *Financial Cryptography and Data Security* (pp. 436–454). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-45472-5_28

Fabian, B., Ermakova, T., & Sander, U. (2016). Anonymity in Bitcoin? – The Users' Perspective. *ICIS 2016 Proceedings*. Retrieved from http://aisel.aisnet.org/icis2016/Crowdsourcing/Presentations/10

Farivar, C. (2016, February 18). Bitcoin startup Butterfly Labs settles with FTC for $38.6M, but it can't pay. Retrieved May 28, 2018, from https://arstechnica.com/tech-policy/2016/02/bitcoin-startup-butterfly-labs-settles-with-ftc-for-38-6m-but-it-cant-pay/

Folkinshteyn, D., Lennon, M., & Reilly, T. (2015). A Tale of Twin Tech: Bitcoin and the WWW. *Journal of Strategic and International Studies*, *X*(2), 82–90.

Galloway, A. R. (2004). *Protocol: How Control Exists After Decentralization*. MIT Press.

Gambetta, D. (1988). Can We Trust Trust? In D. Gambetta (Ed.), *Trust: Making and Breaking Cooperative Relations*. Basil Blackwell. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.24.5695

Gao, X., Clark, G. D., & Lindqvist, J. (2016). Of Two Minds, Multiple Addresses, and One Ledger: Characterizing Opinions, Knowledge, and Perceptions of Bitcoin Across Users and Non-Users. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (pp. 1656–1668). New York, NY, USA: ACM. https://doi.org/10.1145/2858036.2858049

Gibbs, S. (2017, July 11). Head of Mt Gox bitcoin exchange on trial for embezzlement and loss of millions. *The Guardian*. Retrieved from http://www.theguardian.com/technology/2017/jul/11/gox-bitcoin-exchange-mark-karpeles-on-trial-japan-embezzlement-loss-of-millions

Gillespie, T. (2010). The politics of 'platforms.' *New Media & Society*, *12*(3), 347–364. https://doi.org/10.1177/1461444809342738

Gillespie, T. (2014). The Relevance of Algorithms. In P. Boczkowski, K. Foot, & T. Gillespie (Eds.), *Media Technologies: Essays on Communication, Materiality, and Society* (p. 344). MIT Press. Retrieved from http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6733906

Gillespie, T., & Seaver, N. (2016, December 16). Critical Algorithm Studies: a Reading List. Retrieved May 16, 2018, from http://socialmediacollective.org/reading-lists/critical-algorithm-studies/

Glaser, B. G., & Strauss, A. L. (2009). *The Discovery of Grounded Theory: Strategies for Qualitative Research*. Transaction Publishers.

Goffey, A. (2008). Algorithm. In M. Fuller (Ed.), *Software Studies: A Lexicon*. MIT Press.

Greenspan, G. (2015, November 2). Smart contracts: The good, the bad and the lazy. Retrieved August 4, 2017, from https://www.multichain.com/blog/2015/11/smart-contracts-good-bad-lazy/

Gregory, J. (2000). *Sorcerer's apprentice: Creating the electronic health record, re-inventing medical records and patient care*. University of California, San Diego.

Grinberg, R. (2011). Bitcoin: An Innovative Alternative Digital Currency. *Hastings Science & Technology Law Journal*, 160–206.

Guha, S., Cheng, B., & Francis, P. (2010). Challenges in Measuring Online Advertising Systems. In *Proceedings of the 10th ACM SIGCOMM Conference on Internet*

Measurement (pp. 81–87). New York, NY, USA: ACM. https://doi.org/10.1145/1879141.1879152

Gunawan, F. E., & Novendra, R. (2017). An Analysis of Bitcoin Acceptance in Indonesia. *ComTech: Computer, Mathematics and Engineering Applications*, *8*(4), 241–247. https://doi.org/10.21512/comtech.v8i4.3885

Hallinan, B., & Striphas, T. (2014). Recommended for you: The Netflix Prize and the production of algorithmic culture. *New Media & Society*, 1461444814538646. https://doi.org/10.1177/1461444814538646

Hart, K. (2014, February). *Money and Markets in a Human Economy: Harnessing Bureaucracy to Grassroots Democracy*. University of California, Irvine.

Hern, A. (2018, February 13). How Iceland became the bitcoin miners' paradise. *The Guardian*. Retrieved from http://www.theguardian.com/world/2018/feb/13/how-iceland-became-the-bitcoin-miners-paradise

Hileman, G., & Rauchs, M. (2017). Global cryptocurrency benchmarking study. *Cambridge Centre for Alternative Finance*.

Hill, K. (2014, May 15). 21 Things I Learned About Bitcoin Living On It A Second Time. *Forbes*. Retrieved from https://www.forbes.com/sites/kashmirhill/2014/05/15/21-things-i-learned-about-bitcoin-living-on-it-a-second-time/

Hoepman, J.-H. (2007). Distributed Double Spending Prevention. In B. Christianson, B. Crispo, J. A. Malcolm, & M. Roe (Eds.), *Security Protocols* (pp. 152–165). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-17773-6_19

Hurd, M. D., & Rohwedder, S. (2010). *Effects of the Financial Crisis and Great Recession on American Households* (Working Paper No. 16407). National Bureau of Economic Research. https://doi.org/10.3386/w16407

IceTurtle4. (2014, March 25). SURVEY RESULTS: Bitcoiners of Reddit • r/Bitcoin [Reddit post]. Retrieved May 9, 2018, from https://www.reddit.com/r/Bitcoin/comments/21a0n4/survey_results_bitcoiners_of_reddit/

Introna, L., & Nissembaum, H. (2000). Shaping the Web: Why the Politics of Search Engines Matters. *The Information Society*, *16*(3), 169–185. https://doi.org/10.1080/01972240050133634

Irani, L. (2015). The cultural work of microwork. *New Media & Society*, *17*(5), 720–739.

Irani, L., & Silberman, M. S. (2013). Turkopticon: Interrupting Worker Invisibility in Amazon Mechanical Turk. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 611–620). New York, NY, USA: ACM. https://doi.org/10.1145/2470654.2470742

Jabbar, K., & Bjørn, P. (2017). Growing the Blockchain Information Infrastructure. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (pp. 6487–6498). New York, NY, USA: ACM. https://doi.org/10.1145/3025453.3025959

Jaroszewski, S., Lottridge, D., Haimson, O. L., & Quehl, K. (2018). “Genderfluid” or “Attack Helicopter”: Responsible HCI Research Practice with Non-binary Gender Variation in Online Communities. In *Proceedings of the 2018 CHI Conference on*

Human Factors in Computing Systems (pp. 307:1–307:15). New York, NY, USA: ACM. https://doi.org/10.1145/3173574.3173881

Kaplanov, N. M. (2012). Nerdy Money: Bitcoin, the Private Digital Currency, and the Case Against Its Regulation. *Temple University Legal Studies Research Paper*. Retrieved from http://papers.ssrn.com/abstract=2115203

Kelty, C. M. (2008). *Two Bits: The Cultural Significance of Free Software*. Duke University Press.

Knuth, D. E. (1973). *The Art of Computer Programming: Fundamental algorithms*. Addison-Wesley Publishing Company.

Kolata, G., & Murphy, H. (2018, April 27). The Golden State Killer Is Tracked Through a Thicket of DNA, and Experts Shudder. *The New York Times*. Retrieved from https://www.nytimes.com/2018/04/27/health/dna-privacy-golden-state-killer-genealogy.html

Kow, Y. M., & Ding, X. (2016). "Hey, I Know What This is!": Cultural Affinities and Early Stage Appropriation of the Emerging Bitcoin Technology. In *Proceedings of the 19th International Conference on Supporting Group Work* (pp. 213–221). New York, NY, USA: ACM. https://doi.org/10.1145/2957276.2957279

Kow, Y. M., & Lustig, C. (2017). Imaginaries and Crystallization Processes in Bitcoin Infrastructuring. *Computer Supported Cooperative Work (CSCW)*, *27*. https://doi.org/10.1007/s10606-017-9300-2

Kowalski, R. (1979). Algorithm = Logic + Control. *Communications of the ACM*, *22*(7), 424–436. https://doi.org/10.1145/359131.359136

Latour, B. (2005). *Reassembling the Social: An Introduction to Actor-Network-Theory*. Oxford University Press.

Lee, M. K., Kusbit, D., Metsky, E., & Dabbish, L. (2015). Working with Machines: The Impact of Algorithmic and Data-Driven Management on Human Workers. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (pp. 1603–1612). New York, NY, USA: ACM.

Lustig, C., & Nardi, B. (2015a). Algorithmic Authority: The Case of Bitcoin. In *2015 48th Hawaii International Conference on System Sciences (HICSS)* (pp. 743–752). https://doi.org/10.1109/HICSS.2015.95

Lustig, C., & Nardi, B. (2015b). *Bitcoin Users' Perceptions of Anonymity*. Unpublished manuscript.

Lustig, C., Pine, K., Nardi, B., Irani, L., Lee, M. K., Nafus, D., & Sandvig, C. (2016). Algorithmic Authority: The Ethics, Politics, and Economics of Algorithms That Interpret, Decide, and Manage. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems* (pp. 1057–1062). New York, NY, USA: ACM. https://doi.org/10.1145/2851581.2886426

Mainelli, M., & von Gunten, C. (2014). *Chain Of A Lifetime: How Blockchain Technology Might Transform Personal Insurance*. Z/Yen Group Limited. Retrieved from http://www.the-blockchain.com/docs/Chain%20Of%20A%20Lifetime%20-%20How%20Blockchain%20Technology%20Might%20Transform%20Personal%20Insurance.pdf

Mallard, A., Méadel, C., & Musiani, F. (2014). The Paradoxes of Distributed Trust: Peer-to-Peer Architecture and User Confidence in Bitcoin image. *Journal of Peer Production*, (4). Retrieved from http://peerproduction.net/issues/issue-4-value-and-currency/peer-reviewed-articles/the-paradoxes-of-distributed-trust/

Maurer, B. (2016). Re-risking in Realtime. On Possible Futures for Finance after the Blockchain. *BEHEMOTH - A Journal on Civilisation*, *9*(2), 82–96. https://doi.org/10.6094/behemoth.2016.9.2.917

Maurer, B., Nelms, T. C., & Swartz, L. (2013). "When perhaps the real problem is money itself!": the practical materiality of Bitcoin. *Social Semiotics*, *23*(3), 261–277.

Metcalf, J., & Fiesler, C. (2018, March 18). The Cambridge Analytica Scandal Shows Facebook Needs to Give Researchers More Access, Not Less. Retrieved May 31, 2018, from https://slate.com/technology/2018/03/cambridge-analytica-demonstrates-that-facebook-needs-to-give-researchers-more-access.html

Meyer, E. A. (2014, December 24). Eric's Archived Thoughts: Inadvertent Algorithmic Cruelty. Retrieved May 17, 2018, from https://meyerweb.com/eric/thoughts/2014/12/24/inadvertent-algorithmic-cruelty/

Miconi, A. (2012). Under the skin of the networks: How concentration affects social practices in Web 2.0 environments. *Unlike Us Reader: Social Media Monopolies and Their Alternatives*. *INC Reader*, (8), 89–102.

Mochizuki, T. (2014, February 14). Bitcoin Protester Confronts Mt.Gox Executive. Retrieved June 2, 2018, from https://blogs.wsj.com/japanrealtime/2014/02/14/bitcoin-protester-confronts-mt-gox-executive/

Morning, A. (2008). Ethnic Classification in Global Perspective: A Cross-National Survey of the 2000 Census Round. *Population Research and Policy Review*, *27*(2), 239–272. https://doi.org/10.1007/s11113-007-9062-5

Müller, M. (2015). Assemblages and Actor-networks: Rethinking Socio-material Power, Politics and Space. *Geography Compass*, *9*(1), 27–41. https://doi.org/10.1111/gec3.12192

Musiani, F. (2012). Caring About the Plumbing: On the Importance of Architectures in Social Studies of (Peer-to-Peer) Technology. *Journal of Peer Production*, *1*. Retrieved from https://hal-mines-paristech.archives-ouvertes.fr/hal-00771863

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. Retrieved from https://bitcoin.org/bitcoin.pdf

Nardi, B. (2016). When Fieldnotes Seem to Write Themselves: Ethnography Online. In R. Sanjek & S. W. Tratner (Eds.), *EFieldnotes: The Makings of Anthropology in the Digital World*. University of Pennsylvania Press.

Orlikowski, W. J., & Scott, S. V. (2015). The Algorithm and the Crowd: Considering the Materiality of Service Innovation. *MIS Quarterly*, *39*(1), 201–216.

Pew Research Center. (2009). *Obama's Approval Rating Slips Amid Division Over Economic Proposals*. Retrieved from http://www.pewresearch.org/2009/03/16/obamas-approval-rating-slips-amid-division-over-economic-proposals/

Pitcher, T., & Lebaron, J. (2015). *Life on Bitcoin*. Retrieved from http://www.imdb.com/title/tt3910512/

Podolny, S. (2015, March 7). If an Algorithm Wrote This, How Would You Even Know? *The New York Times*. Retrieved from http://www.nytimes.com/2015/03/08/opinion/sunday/if-an-algorithm-wrote-this-how-would-you-even-know.html

Proferes, N., Centivany, A., Lustig, C., & Brubaker, J. (2017, May 15). ICWSM 2017 Workshop: Studying User Perceptions and Experiences with Algorithms. Retrieved May 19, 2018, from http://www.studyingusers.org/

Randewich, N. (2013, November 3). Chip designers see dollar signs in Bitcoin miners. *Reuters*. Retrieved from https://in.reuters.com/article/technology-bitcoins/chip-designers-see-dollar-signs-in-bitcoin-miners-idINDEE9A205W20131103

Razsa, M., & Kurnik, A. (2012). The Occupy Movement in Žižek's hometown: Direct democracy and a politics of becoming. *American Ethnologist*, *39*(2), 238–258. https://doi.org/10.1111/j.1548-1425.2012.01361.x

Reddit Originals. (2011, September 12). Who in the World is reddit? Results are in…. Retrieved May 17, 2018, from https://redditblog.com/2011/09/12/who-in-the-world-is-reddit-results-are-in/

Reid, F., & Harrigan, M. (2013). An Analysis of Anonymity in the Bitcoin System. In Y. Altshuler, Y. Elovici, A. B. Cremers, N. Aharony, & A. Pentland (Eds.), *Security and Privacy in Social Networks* (pp. 197–223). Springer-Verlag New York.

Roberts, P. (2018). This Is What Happens When Bitcoin Miners Take Over Your Town. *POLITICO Magazine*. Retrieved from http://politi.co/2p3fFRF

Sandvig, C. (2014). Seeing the Sort: The Aesthetic and Industrial Defense of "The Algorithm." *Journal of the New Media Caucus*, *10*(3).

Sas, C., & Khairuddin, I. E. (2017). Design for Trust: An Exploration of the Challenges and Opportunities of Bitcoin Users. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (pp. 6499–6510). New York, NY, USA: ACM. https://doi.org/10.1145/3025453.3025886

Schumpeter, J. A. (2013). *Capitalism, Socialism and Democracy*. Routledge.

Seaver, N. (2013). Knowing algorithms. Presented at the Media in Transition 8, Cambridge, MA, USA.

Shirky, C. (2001). Listening to Napster. In A. Oram (Ed.), *Peer-to-Peer: Harnessing the Power of Disruptive Technologies* (pp. 19–28). O'Reilly.

Shirky, C. (2009, November 15). » A Speculative Post on the Idea of Algorithmic Authority Clay Shirky. Retrieved May 6, 2018, from http://www.shirky.com/weblog/2009/11/a-speculative-post-on-the-idea-of-algorithmic-authority/

Smyth, L. (2013). Overview of Bitcoin Community Survey Feb-Mar 2013 | Simulacrum. Retrieved September 25, 2015, from https://web.archive.org/web/20150103171621/http://simulacrum.cc:80/2013/04/13/overview-of-bitcoin-community-survey-feb-mar-2013

Smyth, L. (2014, December 16). Bitcoin Community Survey 2014 | Simulacrum. Retrieved May 9, 2018, from https://web.archive.org/web/20141216120030/http://simulacrum.cc:80/2014/02/01/bitcoin-community-survey-2014/

spamgirl. (2015, March 9). Response: If an Algorithm Wrote This, How Would You Even Know? Retrieved May 17, 2018, from http://turkernation.com/archive/index.php/t-23895.html

Star, S. L. (1999). The Ethnography of Infrastructure. *American Behavioral Scientist*, *43*(3), 377–391. https://doi.org/10.1177/00027649921955326

Star, S. L., & Ruhleder, K. (1996). Steps Toward an Ecology of Infrastructure: Design and Access for Large Information Spaces. *Information Systems Research*, *7*(1), 111–134. https://doi.org/10.1287/isre.7.1.111

Stone, H. S. (1971). *Introduction to Computer Organization and Data Structures*. New York, NY, USA: McGraw-Hill, Inc.

Striphas, T. (2010). How to have Culture in an Algorithmic Age. Retrieved from http://www.thelateageofprint.org/2010/06/14/how-to-have-culture-in-an-algorithmic-age/

Swan, M. (2015). *Blockchain: Blueprint for a New Economy* (1 edition). O'Reilly Media, Inc.

Sweeney, L. (2013). Discrimination in Online Ad Delivery. *Communications of the ACM*, *56*(5), 44–54.

Szabo, N. (1997). Formalizing and Securing Relationships on Public Networks. *First Monday*, *2*(9). https://doi.org/10.5210/fm.v2i9.548

Taylor, M. B. (2013). Bitcoin and the Age of Bespoke Silicon. In *Proceedings of the 2013 International Conference on Compilers, Architectures and Synthesis for Embedded Systems* (pp. 16:1–16:10). Piscataway, NJ, USA: IEEE Press. Retrieved from http://dl.acm.org/citation.cfm?id=2555729.2555745

Thrift, N. (2005). *Knowing Capitalism*. London, UK: SAGE.

ToTheMoonGuy. (2018, May 21). ToTheMoonGuy - About. Retrieved May 22, 2018, from https://tothemoonguy.com/pages/about

Trudell, M. (2012). The Occupy movement and class politics in the US – International Socialism. *International Socialism*, (133). Retrieved from http://isj.org.uk/the-occupy-movement-and-class-politics-in-the-us/

Tufekci, Z. (2014). Big Questions for social media big data. Presented at the 8th International Conference on Weblogs and Social Media, ICWSM 2014.

Tufekci, Z. (2015). Algorithmic Harms beyond Facebook and Google: Emergent Challenges of Computational Agency. *Journal on Telecommunications and High Technology Law*, *13*, 203–217.

United Nations (UN). (2017). *Principles and Recommendations for Population and Housing Censuses, Revision 3*. United Nations, New York. Retrieved from https://unstats.un.org/unsd/publication/seriesM/Series_M67Rev3en.pdf

van Otterlo, M. (2013). A machine learning view on profiling. In M. Hildebrandt & K. de Vries (Eds.), *Privacy, Due Process and the Computational Turn: The Philosophy of Law Meets the Philosophy of Technology* (pp. 41–64).

Velasco González, P. R. (2016). Superabundant design: from waste to control in Bitcoin mining. *A Peer-Reviewed Journal About Excessive Research*, *5*(1). Retrieved from http://www.aprja.net/superabundant-design-from-waste-to-control-in-bitcoin-mining/

Vigna, P. (2014, February 25). 5 Things About Mt. Gox's Crisis. *Wall Street Journal*. Retrieved from https://blogs.wsj.com/briefly/2014/02/25/5-things-about-mt-goxs-crisis/

Vries, A. de. (2018). Bitcoin's Growing Energy Problem. *Joule*, *2*(5), 801–805. https://doi.org/10.1016/j.joule.2018.04.016

Wagenknecht, S., Lee, M. K., Lustig, C., O'Neill, J., & Zade, H. (2016). Algorithms at Work: Empirical Diversity, Analytic Vocabularies, Design Implications. In *Proceedings of the 19th ACM Conference on Computer Supported Cooperative Work and Social Computing Companion* (pp. 536–543). New York, NY, USA: ACM. https://doi.org/10.1145/2818052.2855519

Weaknesses - Bitcoin Wiki. (n.d.). Retrieved May 27, 2018, from https://en.bitcoin.it/wiki/Weaknesses

Weber, M. (1978). *Economy and Society: An Outline of Interpretive Sociology*. (G. Roth & C. Wittich, Eds.). University of California Press.