The social construction of blockchain privacy platforms

by

Jennifer Mentanko

B.A., MacEwan University, 2015

Thesis Submitted in Partial Fulfillment of the
Requirements for the Degree of
Master of Arts

in the
School of Communication
Faculty of Communication, Art and Technology

SIMON FRASER UNIVERSITY
Summer 2020

Declaration of Committee

Name:	**Jennifer Mentanko**
Degree:	**Master of Arts (Communication)**
Title:	**The social construction of blockchain privacy platforms**
Examining Committee:	**Chair:** Ahmed Al-Rawi Assistant Professor, Communication
	Peter Chow-White Supervisor Professor, Communication
	Andrew Feenberg Committee Member Professor, Communication
	Frederik Lesage Examiner Associate Professor, Communication

Ethics Statement

The author, whose name appears on the title page of this work, has obtained, for the research described in this work, either:

a. human research ethics approval from the Simon Fraser University Office of Research Ethics

or

b. advance approval of the animal care protocol from the University Animal Care Committee of Simon Fraser University

or has conducted the research

c. as a co-investigator, collaborator, or research assistant in a research project approved in advance.

A copy of the approval letter has been filed with the Theses Office of the University Library at the time of submission of this thesis or project.

The original application for approval and letter of approval are filed with the relevant offices. Inquiries may be directed to those authorities.

Simon Fraser University Library
Burnaby, British Columbia, Canada

Update Spring 2016

Abstract

Our current Internet environment is characterized by online conglomerates, predictive computing and data mining. With this, there is a growing concern among users on how to protect their privacy and manage their identities online. Advocates for blockchain, the newest large-scale wave of Internet based platforms, argue it is highly useful for privacy protection. Blockchain is an encrypted and decentralized public ledger that verifies and stores information through a peer-to-peer network. Using the social construction of technology (SCOT) as a theoretical framework, I deploy a comparative discourse analysis of three blockchain platforms - Brave, Civic and Oasis Labs - along with user discourse on Reddit and Medium. This thesis explores how users socially construct this emerging technology by comparing privacy discourse between blockchain platforms and motivated social agents. I found blockchain privacy platforms and its users both value data ownership, ad-blocking and safety and security. However, there is also friction and disagreement about themes of trust and ethics as well as usability.

Keywords: social construction; online privacy; blockchain; identity management

Dedication

For Mum.

You always believed in my dreams too.

Acknowledgements

This thesis would not have been possible without the guidance of Dr. Peter Chow-White. Thank you for introducing me to blockchain and the GeNA lab. My academic experience was incredibly fulfilling because of the opportunities you gave me to collaborate, learn and better myself both academically and as a person. I have grown so much these past three years, and it is thanks to your mentorship.

I'd also like to thank my committee. Dr. Andrew Feenberg inspired my theoretical framework and Dr. Frederik Lesage helped to form my methodology. Thank you Ahmed Al-Rawi for your participation and thoughtful feedback.

I would like to thank the GeNA lab for their guidance, encouragement and friendship. Working in the lab was my favourite part of this academic journey. Pippa Adams and Julie Frizzo-Barker, thanks for being such positive role models. Camille Jasinski, I am so glad to have met you in our methodology class.

Outside of the university, I'd like to thank my husband, Sparky. You are my number one fan. Your encouragement and support mean everything. My brother Blake, you didn't really help let's be honest, but thanks for being you. AGF – I never felt alone in this city because of you. Thank you to my mum, the best mum in the whole wide world. And lastly, to my best friend, my dog, Waffles.

Table of Contents

List of Tables

List of Figures

List of Acronyms

CCTV	Closed-Circuit Television
GDPR	General Data Protection Regulation
PIPEDA	Personal Information Protection and Electronic Documents Act
SCOT	Social Construction of Technology
SCR	Social Construction of Reality
SNS	Social Networking Service
UGC	User Generated Content

Chapter 1.

Introduction

Our current Internet paradigm is characterized by centralization, online conglomerates and data silos, far removed from the Internet's original static, read-only architecture. We now face an Internet driven by data, algorithms and automation, making it difficult for individual users to maintain authority when they are only valued for their data. Data mining by online conglomerates has raised concerns about user privacy, security, data ownership and the overall ethics of gathering and scrutinizing our online information. Users have become more aware of the nefarious consequences of data mining as the media consistently publishes stories on the latest data breaches and instances of data manipulation. This includes the 2018 Cambridge Analytica scandal where a data firm working with the Trump election team harvested millions of Facebook profiles in an attempt to sway users' vote toward the Republicans. The data breach was only revealed after a whistleblower provided The Guardian with documents outlining Cambridge Analytica's unauthorized possession of over 50 million Facebook accounts for the purpose of targeted campaign advertising (Cadwalladr & Graham-Harrison, 2018). This scandal was a catalyst for the growing public interest in datamining and its consequences not only for privacy and security, but overall democracy. Fortunately, despite increasing centralization, the Internet's architecture remains fluid and groups of social agents are motivated to reimagine the Internet and reclaim power that is rightfully theirs. According to Feenberg (2013), the Internet as a technical system is comprised of layers conducive to participation and its ultimate reimagination. Through participatory discourse, users can negotiate the Internet's technical code, in hopes that it can be restructured to better represent user values such as decentralization, community and equality.

Online privacy is difficult to define because it represents a movement that expounds its formal definition. For users, online privacy discourse is used to reassert individual power, and reign in the centralized conglomerates that threaten democratic values. It is no longer a static term used to describe the safety of our data. Privacy discourse has become a symbol of the power struggle between online conglomerates

and individual users. This is made evident by the numerous organizations that use privacy as a way to bring awareness to the exploitative powers of corporations and governments that use datamining, tracking and more. For instance, Privacy International is an organization that uses online privacy to symbolize the fight to “protect democracy, defend people’s dignity and demand accountability from the powerful institutions who breach public trust” (Privacy International, 2020). Or, the Electronic Privacy Information Centre that aims to focus public attention on “emerging privacy and civil liberties issues and to protect privacy, freedom of expression, and democratic values in the information age” (EPIC, 2020). By deducing what is wrong with the Internet today into a single point of discussion, it provides users with a tangible movement and gives lawmakers the substance to create regulations to reign in powerful online corporations. This has come to fruition in regulations such as the European Union’s General Data Protection (GDPR), which aims to provide citizens with more control of their online data. The power of privacy discourse cannot be understated, and this thesis works to discover how this cultural discourse effects change in emerging technology. This paper aims to define, compare and contrast definitions of online privacy according to blockchain privacy platforms and social agents on Reddit and Medium to discover how social agents negotiate power through emerging technology.

1.2. What is Online Privacy?

Pre-Internet, the desire for privacy was demonstrated by shutting a door or closing the curtains. As the Internet’s ubiquity grows, conceptions of privacy shift, but the desire to be let alone remains. Users must balance self-censorship with social sharing as social media platforms encourage users to publish the minutia of their day-to-day life. The term privacy maintains a legal definition, but conceptions of privacy change depending on who you talk to. Privacy is as much of a feeling as it is a concrete definition but above all, privacy is a basic human need.

Privacy has a long history within society and has been valued since the beginning of civilization. Notable philosophers such as Aristotle and John Locke reference privacy in their philosophies on the nature of society. Aristotle makes a distinction between the public sphere and the private sphere, where the private sphere

functions as the household and satisfies human needs such as food, water, shelter and family. In turn, these needs are a prerequisite for participating in the public sphere for the common good. To Aristotle, man must be satisfied in both spheres to maintain a quality of life (Tholen, 2016, p. 244-245). Similarly, social theorist Robert F. Murphy (1964) asserts that privacy is an essential precondition of participation in a public role and is essential to both social relationships and a sense of self. Privacy then, should not be considered the opposite of the public realm, rather, public and private spheres must function in harmony for individuals to be satisfied. John Locke is another well-known philosopher who made a distinction between public and private life, stating that the natural liberty of man is free from legislative authority and his zone of privacy ought to be protected by those in power (Rengel, 2013). A libertarian would insist that privacy is an innate human right and the government should do everything in its power to protect this right.

While most governments recognize privacy as a lawful right, privacy laws vary globally. Samuel D. Warren and Louis D. Brandeis (1890) are credited with laying the foundation for modern privacy law in their famous article in *Harvard Law Review* which broadened the scope of the "right to life" to mean "the right to enjoy life." To enjoy life, one must maintain the right to be "let alone" (p. 193). By advocating this right, Warren and Brandeis hoped to remedy "the evil of the invasion of privacy by the newspapers," as town gossip had become a full-fledged trade (p. 195). They believed this law was an inevitable by-product of advancing civilization where individuals, more than ever, needed to experience privacy and solitude in the face of increasing cultural influence. Now, privacy rights are recognized globally and were written into the Universal Declaration of Human Rights in 1948: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor attacks upon his honour and reputation" (United Nations, 1948). In Canada, the right to privacy was not included in legislation until the late 1980s. While some provinces drafted their own privacy legislation in the late 1960s, it was not until 1983 that The Access to Information Act and the Privacy Act were enacted. While this Privacy Act has seen little to no revision since the 1980s, the Personal Information Protection and Electronic Documents Act (PIPEDA), was put forth in April 2000. This legislation brings us into the Internet age, where privacy becomes more contested, and more ambiguous than ever before. It is a time where lawmakers

struggle to keep up with the ubiquity of the Internet and datamining, and users are not waiting up. Instead, they are attempting to solve the privacy problem on their own.

This thesis focuses on privacy in the digital age. Just as the notion of privacy was contested throughout history, there is no clear definition of what online privacy is or should be. Much of the literature on communication privacy acknowledges the ambiguity and uncertainty of the term (Powers, 1996; Lane, 2009; Craig and Ludloff, 2011; Dixon and Gellman, 2011). Online privacy is shifting terrain in both the management of it by people and organizations and in communication literature. Further, social media platforms and big data creates a major challenge in theorizing what privacy means and how to manage it. Much of the literature that attempts to define online privacy lags behind emerging surveillance technologies, algorithms and predictive technology. This thesis examines privacy as a movement and a symbol of reclamation, rather than as a static, definitive term. By classifying the egregious actions of centralized organizations online into the “privacy” umbrella, users and lawmakers have a platform to resist increasing centralization and data siloes. This thesis examines privacy discourse in an effort to understand how motivated social agents negotiate power through new technology.

1.3. Online Surveillance Practices

Online privacy concerns have grown in conjunction with the Internet. Researchers began linking computers to privacy loss as early as the 1970s when government bodies used computer matching - a technique that compares different sets of personal data - to detect patterns and cases of interest. The influx of data recorded by administrations allowed governments, particularly in the United States, to detect large scale fraud, but at the risk of revealing personal information (Clarke, 1994). Azrael (1984) outlined how computer matching results in privacy loss, and recommended revisions to the 1974 Privacy Act to include protection from surveillance via computer matching. In 1988, the Computer Matching and Privacy Act was enacted in the United States. Nevertheless, Azrael predicted privacy in the digital age would only become greater and more challenging, and that current data mining practices deserved “immediate attention” (p.19).

Our current Internet environment has greatly transformed since the static, hyperlink-based web from the 1980s and 1990s. We have just entered Web 3.0, characterized by online conglomerates, algorithms, big data and social sharing. Now, users are not only worried about government surveillance, but corporate surveillance, too. There is an abundance of literature documenting how corporations mine user data to target audiences, predict consumer behaviour and foresee upcoming trends. Moreover, digital conglomerates are becoming increasingly centralized, making them powerhouses in the business of data collection. We can see this increasing centralization by observing the way big data is siloed between a small number of corporations, making them the gatekeepers of information. For instance, Facebook's "Like" button transcends the platform and is distributed throughout the web. Through this Facebook Connect system, users can "like" products and ideas outside of the platform, providing Facebook with a clearer picture of users' browsing habits. This data is then gathered into a centralized and enclosed server farm controlled by Facebook (Gehl, 2018). As of 2019, Facebook is the largest social media platform with approximately 2.27 million monthly active users; however, social media platforms are not the only organizations hoarding user data. Of all search engine queries, 75% are typed into Google, followed by the second largest search engine, Baidu which holds only 11% of the market share (Net Market Share, 2019). Furthermore, as of 2019, Amazon holds 45% of the retail e-commerce market share, making it four times larger than Walmart.com (ecommerceDB, 2019). These online superpowers are as much of a threat to user privacy and data ownership as social media platforms as they continuously mine data and track user browsing activity to understand and capture potential customers.

This mode of corporate surveillance, as proposed by Andrejevic (2002), is exploitative not only because it invades user privacy, but because it forces users to enter the online workforce by producing value in the form of data. Users are given the convenience and connectivity of platforms, and in turn, grant these platforms power to mine their data. Andrejevic (2002) argues this is a unique consumer labour model which forces users to create and consume as another cog in the capitalist machine. For instance, in the last quarter of 2018, Facebook made $6.18 in revenue per user by allowing advertisers access to user data. There are roughly 98 data points that Facebook uses to target users, from basic information like age and gender, to more

intrusive details such as political leaning, the style and brand of a user's car, or credit card type (Glum, 2018 & Dewey, 2016). Further, the data collected by major conglomerates or third-party marketing organizations is not always secure, whether it is due to weak security or human error. Users have no way of ensuring their data is protected once it is collected. For instance, in 2015 hackers leaked the identities of 30 million users of Ashley Madison, a dating website for extra-marital affairs, which caused instances of public humiliation and even reported suicides (Kuchler, 2016). Additionally, Equifax made headlines in 2017 when 150 million users had their data compromised due to a preventable, unpatched security framework (Swinhoe, 2019).

Outside of data mining for capitalist production, there are pressing ethical questions when it comes to online content manipulation. In 2014, Facebook along with American researchers manipulated users' news feeds for a psychological experiment to determine how exposure to different emotions changed posting behaviour (Kramer, Guillory & Hancock, 2014). While this experiment was deemed intrusive and disturbing by users and privacy advocates, nothing devastated user trust quite like the Cambridge Analytica scandal of March 2018. To sway voting behaviour in support of the Republican Party, Cambridge Analytica harvested personal data of millions of Facebook users and manipulated their feeds preceding the 2016 United States presidential election (Cadwalladr & Graham-Harrison, 2018). These actions revealed a more sinister side to data collection as a powerful tool used to undermine the sanctity of democracy.

Whether it is due to increased media exposure on major data breaches, or eerily personalized advertisements, users and governments alike are becoming wary of the power of big data, and the corporations that are involved in its collection. The United Kingdom enacted the GDPR in May 2018, which forces organizations to make explicit what personal data will be collected from users and how that data will be used. Moreover, it gives users the "right to be forgotten," meaning websites must delete all data associated with an individual upon request (European Parliament and Council, 2016). The UK's actions have not gone unnoticed in Canada, as the GDPR was a major source of interest at the annual Canadian Privacy and Access Conference held in July 2018. Privacy experts urged Canadian businesses to meet the GDPR standard, acknowledging that Canada's privacy legislation is woefully outdated. While the GDPR is considered the gold standard for privacy legislation, globalization and transnational flows of big data add complexity to application and enforcement. For instance, Cambridge

Analytica largely targeted American users, but new documents show that a much larger, global operation of data manipulation intended to sway voters on an “industrial scale” (Cadwalladr, 2020). Big data collection and its ramifications for individual online privacy and data ownership is a pressing global issue that requires a united solution. Attempting to regulate cross-border data flows through a national regulation is challenging as data collection, data and storage can occur in multiple jurisdictions. Blockchain is a potential solution to the complexities of creating and enforcing transnational privacy legislation by providing users with a ground-up, globalized solution to protect individual privacy.

1.4. Blockchain’s Role in Privacy Protection

Fortunately, the Internet’s interactive and fluid framework leaves room for motivated social agents to redefine their online environment. According to social construction, society and the social groups within it hold weight in shaping emerging technologies. Technology is a result of the social, economic and political environment in which it flourishes, as well as the influence of social agents that work to see their values reflected in the technology they use (Feenberg, 1992). By examining the origins as well as current iterations of blockchain, we can see how this technology is informed by social agents and has the potential to revolutionize the way we think about privacy.

Blockchain is an encrypted, decentralized ledger that verifies and stores information on a peer-to-peer network without the need for third party intermediaries. Information on the blockchain is encrypted and invariable, prompting *The Economist* to dub it the “Trust Machine” in 2015. Blockchain is imperative in the facilitation of cryptocurrency but has been adapted for a variety of use-cases including smart contracts, supply chain management, data ownership and privacy protection. Because blockchain is in a nascent stage, it is well-suited to be interpreted and perhaps adapted and reimagined by social agents, making it a valuable technology to study.

Blockchain features key characteristics that maintain security and data confidentiality such as decentralization, cryptography and immutability. Blockchain runs on a dispersed network of computers, rather than on a central database. No one entity is in control and there are multiple copies of records spread between computers.

Decentralization makes hacking more difficult as more than 50% of the systems in a blockchain network must be compromised in order to gain control (Kshetri, 2017). Encryption is built within the architecture, making users' identity, transactions and communication secure. Cryptology is used to hide proof of identity and personal data can only be seen when given permission, making data storage and transmission highly secure (Kshetri, 2017). Further, records on blockchain are permanent and immutable, forcing transparency and trust.

Along with data confidentiality, data sovereignty is a driving force behind blockchain. With blockchain, users can control who has access to their records. Applications built on blockchain aim to build this value within the architecture. For instance, blockchain applications for medical records would facilitate the secure transmission of sensitive records. A patient would have control over who can access and share this information (Kshetri, 2017). Tapscott and Tapscott (2018) call this feature of blockchain a "black box of identity" or a "personal avatar" which acts as a "software servant" that can "release only required detail or amount for each situation and at the same time whisk up your data crumbs as you navigate the digital world" (p. 15). There have been variations of this "black box" from different technology companies, academics and computer scientists building blockchain applications, but each have the same mission: to create data autonomy in a digital world increasingly characterized by centralized data silos.

1.5. Thesis Overview

This thesis uses a social constructivist lens to understand how motivated social agents negotiate power through an artefact's technical code by participating in cultural discourse. More specifically, this thesis applies a social construction of technology (SCOT) framework to understand how users on two user-generated content (UGC) platforms negotiate blockchain's technical code through privacy discourse. This thesis begins by outlining the critical frameworks that inform this study. I begin with a brief overview of the social construction of reality (SCR) because it informs how we understand privacy and cultural discourse altogether. In order for social agents to negotiate power structures through privacy discourse, they must have common

constructions of reality. SCR explains how social and cultural values shape our understanding of reality, and how we express these constructions via a linguistic schema that others recognize. For instance, this thesis reveals that in general, users have a similar conception of what privacy is based on their own realities. Following, I outline the major theorists that have contributed to science and technology studies (STS) which include Pinch and Bijker (1984), Latour (1992) and Feenberg (1992, 2013). SCOT is the grounding theory for this thesis, as it explains how social agents can reshape an artefact to better represent their values. This theory explains how motivated users on UGC platforms can alter the technical code of an emerging technology, like blockchain, through privacy discourse. Next, I provide an overview of surveillance theory to elucidate how surveillance threatens individual freedoms, communication rights and overall privacy. Big data and privacy theory further invigorate these concerns, and this section explores the adverse effects of data mining on individual users and attempts to understand what privacy means in the age of big data.

Following my theoretical exploration, in chapter three I outline the methodology used for this study. This study uses a comparative discourse analysis to understand the relationship between privacy discourse on blockchain platforms and on the UGC platforms Reddit and Medium. In this section, I provide the rationale for my methodology, along with my criteria for selecting the blockchain and UGC platforms to study. Next, chapter four outlines the ways in which the Internet and blockchain are socially constructed technologies. This chapter explores the fluidity of the Internet and emerging technology through a SCOT lens. To understand how social agents on Reddit and Medium can shape blockchain privacy platforms, we must first understand the Internet's inherent malleability. Finally, chapters five and six delve into the findings from my comparative discourse analysis. In these chapters, I compare and contrast themes of privacy from blockchain platforms and its users. Through this comparative analysis, I explore how privacy discourse informs the construction of blockchain platforms, and the affordances and constraints of these platforms for privacy according to users.

Chapter 2. Literature Review

2.1. Introduction

Regardless of the time in history, privacy has always been an innate, human feeling. Rengel (2013), understands privacy to exist prior to and independent of political order and the rule of law. Rather, privacy is a natural law, an intrinsic need grounded in reason (p. 9). While all human beings under natural law should have the right to privacy, the definition of privacy has seen many iterations throughout history depending on the political, social and economic environments and new technologies. For instance, originators of privacy law, Warren and Brandeis (1890) reportedly wrote "The Right to Privacy," in reaction to the social environment at the time, particularly the actions of the yellow press. While the accuracy of this anecdote has been questioned (Rossen & Santesso, 2010), Warren was frustrated with the intrusiveness of journalists after the *Saturday Evening Gazette* in Boston published his daughter's wedding guest list in the spring of 1890. In particular, Warren recognized the impact new technology, in this case cameras, were having on society.

> Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the housetops' (Warren & Brandeis, 1890, p 195).

To escape increasing culture and technological influence, people required a sacred space to themselves that was free from outside intrusion.

> The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary retreat from the world, and man, under refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected hum to mental pain and distress far greater than could be inflicted by mere bodily injury (Warren and Brandeis, 1980, p.196).

Since 1890, culture and technology have evolved, as has the definition of privacy. The idea of privacy changes depending on societal circumstance, which is a key feature in the theory of social construction. I argue that privacy has outgrown its formal definition and now epitomizes the struggle between increasing centralization and the

power of users. Social construction argues that knowledge or technology is a result of the social, political and economic environment in which it is created. Furthermore, the theory sees that humans create their own understanding of their environment in coordination with others. These groups can be classified as social agents. This paper aims to define, compare and contrast definitions of online privacy according to blockchain privacy platforms and social agents on Reddit and Medium to discover how these social agents negotiate power through emerging technology. Just as Warren and Brandeis witnessed the significance of privacy in light of new technologies that threaten the "sacred precincts of private life" (p. 195), these social agents recognize the consequences of the information society and the pervasiveness of surveillance technologies.

In this chapter, I discuss three areas of literature that underpin my analysis of blockchain platforms and users' constructions of online privacy. The first section begins with an introduction to the SCR, which segues into an exploration of SCOT. SCOT explains how technology is inextricably tied to the social, political, and economic environment in which it is constructed. In addition, relevant social groups aid in the construction of technology by instilling their values within it (Pinch & Bijker, 1984). This process can be applied to the development of the Internet and in blockchain. SCOT provides a foundation for not only understanding new technology but understanding how cultural discourse influences the technical code of these emerging artefacts. Next, I delve into communication and surveillance theory. A review of surveillance literature is needed to understand the context for the emergence of privacy discourse and the technologies that work to mitigate online surveillance. This thesis contributes to surveillance literature by outlining affordances and constraints of blockchain platforms for privacy mitigation. This fits into a practical implications schema, which is identified by scholars as a significant gap in surveillance and privacy literature (Barth & Jong, 2017). Lastly, I discuss critical works in big data scholarship to delineate the Internet's shifting terrain. This section informs why privacy rights and data ownership are necessary in our current digital age and why social agents are motivated to change their online environment.

2.2. Constructing Technology

I begin this section by briefly outlining SCR as an introduction to SCOT. SCR explains how social agents participate in cultural discourse through mutual understandings of linguistic schema. SCR demonstrates how users reach a common understanding of the complex and ambiguous notion of privacy. Privacy discourse is developed through shared realities and becomes a powerful force when vying for online rights. While online privacy may be difficult to define, it is an important concept to consider as it is ultimately a human right.

Berger and Luckmann (1966) are credited as the founders of SCR with their ground-breaking text, *The Social Construction of Reality* (Leeds-Hurtitz 2016; Knoblauch & Wilke, 2016). Scholars have adapted this theory in a number of disciplines. According to Knoblauch and Wilke (2016), sociology cites SCR most often with 701 published articles between 1966 and 2015. In communication, 56 articles were published in the same timeframe. Berger and Luckmann see the world as intersubjective, shared with others through interaction and communication as "common objectivations of everyday life are maintained primarily through linguistic signification" (p. 35). Language allows us to organize experiences and Berger and Luckmann use the example of "mother-in-law" trouble to explain this practice. Those who have experienced this type of tension immediately recognize this linguistic schema (p. 37). Through communication, individuals compare and contrast common experiences through their "available stock of knowledge" (p. 39). While Berger and Luckmann insist face-to-face communication is the strongest way to create shared realities, more modern scholars prove common realities can be shaped through technology. For instance, media effects studies of the 1970s and 1980s explored how television and media shape common realities (Adoni & Cohen, 1978; Peterson & Peters, 1983; Shapiro & Lang, 1991; Gamson, Croteau, Hoynes & Sasson, 1992). Now, it is more common for scholars to examine the Internet as a space where users can construct social realities via communication, identity construction and online role play. For instance, SCR is used to understand how virtual role-playing games create collective worldviews (Simona, 2007; Coussieu, 2010; Edgar, 2016; Mills, 2018). In the age of big data, scholars use SCR to understand how algorithms can create limited social realities through echo chambers and feedback loops that represent only a small portion of reality (Just & Latzer, 2016; Hilbert et al, 2017; Cohen, 2018).

SCR can help us understand how social agents use online discourse to negotiate privacy online. To orient Berger and Luckmann in terms of privacy, it must be understood that individuals conceive shared ideas of privacy through their own knowledge base. This knowledge base is built through interacting with technology, communicating with others, and sharing social worlds, be it online or offline. Scholars have acknowledged the dialectical nature of privacy, as it is negotiated through patterns of self-disclosure and the exploration of openness and selective control of access to oneself (Altman, 1975; Newell, 1998; Powers, 1996; Craig and Ludloff, 2011). Craig and Ludloff (2011) attribute privacy's arbitrary definition on influences, such as history, culture and social norms that shape an individual's reality and in turn, expectation of privacy. For instance, China's digital authoritarianism yields a different expectation of privacy than comparatively freer nations, like Canada. Craig and Ludloff argue that redefining online privacy must depend on a collective network of individuals to construct an online, shared reality. Offline, this universal schema is much more recognized, as demonstrated by Newell's (1998) cross-cultural comparison of privacy definition and functions. Newell found that pre-Internet definitions of privacy had striking commonalities between three distinct countries studied: Ireland, Senegal and the United States. All three cultures agreed that privacy was a condition of a person, and the most important facet was to be let undisturbed. Berger and Luckmann refer to this as symbolic language, a maximum detachment from the "here and now" (p. 38).

As the concern for online privacy increases in conjunction with new technologies, it is important to consider what privacy means to users. What features of privacy are important to users? What are our privacy rights as users? Our worldview is shaped by a variety of factors including language, communication, family, friends, media and increasingly, algorithms, online collectives, SNS and interfaces. The focus of this paper is to compare meanings of privacy between two online collectives: Reddit and Medium users, as well the parties behind blockchain privacy platforms. The conception of privacy is socially constructed, and these definitions will not come without context from social, political and economic realms.

To introduce SCOT, I begin with Marshall McLuhan's famous interpretation of technology as a codependent tool that is shaped by society, and in turn, shapes society. Throughout his communication studies, McLuhan employed a media ecology perspective, which interprets media not as a separate technology, but as an environment

in itself. To study media is to study the ways in which people and technology interact and influence one another. Like media ecology, SCOT understands technological innovation as a social system. Pinch and Bijker (1984), originators of the SCOT approach, bridge the gap between SCR and SCOT, stating that both technological artefacts and scientific facts should be understood as social constructs: "...science and technology are both socially constructed cultures and bring to bear whatever cultural resources for the purposes at hand" (p. 404). This subjective nature of scientific facts was famously observed by Latour and Woolgar (1979) in their breakthrough ethnographic study of laboratory processes. What appears to outsiders as a logical systematic process to reveal objective truth is realistically a "disordered array of observations with which scientists struggle to produce order" and scientists are "routinely confronted by a seething mass of alternative interpretations" (p. 36). The construction of facts and technological artefacts are therefore a non-linear, socially negotiated process.

Commonalities can be drawn between Pinch and Bijker's oft-cited analysis of the development of the recumbent bicycle and the development of blockchain technology. Namely, both follow a multi-directional model of innovation as different social agents interpret and influence how these technologies take shape. Social agents are collectives that share a set of meanings and values when interpreting a technology. In the case of blockchain privacy platforms, these relevant social agents include privacy advocates, platform developers, interested businesses and organizations, investors, and more. While there are many relevant social groups vying to be the most influential, this paper will focus on the collective reality observed on Reddit and Medium. According to SCOT, social groups define problems with a technology, which results in the technology's reimagination. For instance, Pinch and Bijker found that female bike riders saw the lack of safety assurance as a problem, which influenced developers of the bicycle to create a safer model to satisfy the needs of this social group. Once the most influential social agents are satisfied, a technology reaches closure and stabilization. In the case of the bicycle, this occurred when the bicycle was not only safe, but fast so male, female and elderly riders reached an agreement that their unique problems were solved.

The influence of social agents is a significant factor in the social construction of technology; however, social, economic and political contexts must be taken into account as well. Latour (1992) sees technological development occur through interactions between people, much like the process of knowledge construction. STS theorists, like

Latour and Pinch and Bijker understand technology to be inextricably tied to people and the environment in which it is developed. Latour further invigorates the theory of social construction by outlining how social values and political goals can be realized through the development of technology. A vehicle, for example, forces the driver to buckle up by alarming the driver when there is a body in the car without a seatbelt. In doing so, the value of safety is ingrained within the vehicle's architecture, compelling society to comply. Feenberg (1992) applies social construction to the Internet age in his theory of technical code - the incorporation of societal demands in technology. Technology is not simply engineered by an isolated team of experts, rather, society aids in shaping technological design by encoding meaning within artifacts. Increasing societal representation in technological design represents a democratic rationalization, an improved reflection of human needs in technology. Blockchain's development is wrought with economic, political and social ties, making the technology intrinsically value laden. The decentralized, peer-to-peer and trust-free architecture was created in retaliation to the increasingly centralized space we see today. Feenberg (2013) outlines five layers of the Internet that are contingent to its fluidity and allowed for the creation of blockchain: a non-hierarchical structure, anonymity, broadcasting, data storage and many-to-many communication. Despite the powerful Internet entities such as Amazon, Facebook and Google, that make up our online experience, the Internet's architecture remains a participatory and malleable space. In his work, Feenberg refutes ideas of communicative capitalism put forth by Dean (2005) and Fuchs (2010) by identifying the Internet's democratic potential.

> Design is pulled in many directions by actors with different interests and worldviews, for example, some pursuing profits and others involved in public life. No one social group has complete control so all must be treated symmetrically. In sum, the Internet cannot be reduced to a single one of its many dimensions (Feenberg, 2013, p. 2).

This democratic potential can be seen in open data initiatives, particularly when the movement is shaped by both citizens and government. Lassinantti et al. (2014) demonstrate the social construction of open data initiatives in two Swedish municipalities. In their qualitative analysis, the authors observed that two open data initiatives followed separate paths in accordance with the aims of social agents and the contextual challenges of each region. Two interpretations of the open data initiative evolved: one focused on techno-economic growth, while the other was more socially

focused, incorporating more citizen council in the long run. Drawing from Pinch and Bijker, the two open data initiatives followed a multidirectional innovation process influenced by social agents and local environments.

Similar to Pinch and Bijker, Feenberg (1992, 2013) allows for ambiguity in the development of technologies, as actors understand these new technologies based on their own social realities. Flexibility is a key component to SCOT as it allows for social agents to define problems and solutions and ascribe meaning to an artifact. For Feenberg, social agents' interpretation is an act of democracy and increasing societal representation in technological design represents a democratic rationalization. A. Flanagin, C. Flanagin and J. Flanagin (2010) in their exploration of Feenberg's technical code, address a number of design features of the Internet that are conducive to social construction. For instance, during the Internet's history as a military platform, the values of survivability and performance were valued over the commercial concerns we see today (p. 182). Despite this, the most significant characteristic of the Internet remains its ability to be altered, reimagined and adapted by individual users. Users have become powerful social agents, creating meaningful group participation and shifting the Internet authority from one, to many.

While these ideas fall in line with what Feenberg hoped would be the democratic potential of the Internet, A. Flanagin, C. Flanagin and J. Flanagin published during the Web 2.0 boom. This period was characterized by social networking, sharing, interactivity and collaboration. Comparatively, the pendulum has swung towards the direction of corporatization. In Hrynyshyn's (2008) exploration of the globalization and corporatization of the Internet, the author recognizes the affordances of SCOT in identifying social agents and contexts that impact the development of technology. However, he believes this theory fails to address the hierarchies that exist within social agents. The social construction of the Internet is not an act of democratic rationalization as only a few, powerful social agents are able to participate in its social shaping. Hrynyshyn explores this notion in an analysis of domain names and country codes, which is controlled by a U.S. institution called ICANN. The United States' control of domain name registry is problematic, as social agents from this institution have more influence over the Internet's architecture than other global institutions. Nevertheless, the development of blockchain proves that aspects of community and decentralization still exist on the Internet. Blockchain is an amalgamation of motivated social agents hoping

to rearrange the Internet to become better representative of the values of individual users.

Through privacy discourse, the Internet's technical code is currently being arranged to better suit the needs of users in an environment that has become a representation of capitalist ideals. Within the blockchain space, social agents play a significant role in identifying problems and solutions with the technology. This paper identifies some of those social agents and their ideas of online privacy compared to those of blockchain privacy platforms. A SCOT framework is crucial in this investigation, as it follows the logic that if the problems identified by social agents are not solved by the blockchain privacy platforms, the technology will alter according to the needs of users. Dismissing the social construction of technology would consider blockchain privacy platforms as an isolated technology, which departs from the technology's historical roots as a libertarian, trust-free and decentralized innovation. Moreover, to understand the social construction of blockchain, it is important to understand the social, political and economic environment in which the technology was conceived. The following section provides context for our growing surveillance society that justifies the need for blockchain to protect user privacy rights and online freedom.

2.3. Surveillance Society

While the ubiquity of the Internet leads us to associate surveillance with the digital space, surveillance theory has been present since the early 20th century. Pre-Internet, digital surveillance took shape via cameras, especially in popular public places (Albrechtslund & Lauritsen, 2015). Scholars studying public surveillance via closed circuit television (CCTV) cameras seek to balance the public good associated with mass surveillance, such as crime deterrence and safety, with the potential privacy infringement of innocent citizens (Norris & Armstrong, 1999; Raab & Mason, 2004; Hu & Cen, 2009; Walby, 2009; Larsen, 2011). Panopticonism as a surveillance theory maintained its relevance in the age of CCTV surveillance as the metaphor of an invisible, authoritative observer resonated well with the elusive, yet powerful CCTV surveillance system (Galic, Timan & Koops, 2016). Jeremy Bentham's panopticon as interpreted by Foucault (1977) is a prison configuration featuring a centre windowed guard tower that is backlit, so the

guards, or lack thereof, cannot be seen by the surrounding prisoners in their cells. The goal of this prison design is to:

> ...induce in the inmate a state of conscious and permanent visibility that assures the automatic functioning of power…he is seen, but does not see; he is the object of information, never the subject of communication (Foucault, 1997, p. 200-201).

Galic, Timan and Koops (2016) see panopticonism as an apt metaphor for CCTV surveillance as there is a constant mediated gaze that moulds citizens in public spaces to behave according to norms. Scholars that use panoptic theory in studying CCTV surveillance focus on the disciplinary parallels of the panopticon and CCTV systems (Fyfe & Bannister, 1996; Norris & Armstrong, 1999; Koskela, 2002).

In the eras of Web 2.0 and Web 3.0, surveillance literature has moved away from panopticonism into the realm of post-panopticonism, cryptopicon, synopticon and the panoptic sort, among others (Boyne, 2010; Vaidhyanathan, 2012; Mathiesen, 1997; Gandy, 1993). Scholars studying surveillance in the digital age recognize the limitations of panopticonism as a theoretical idea. Some criticisms of Foucault's interpretation of Bentham's panopticon include: the assumption that those surveyed are rational and perceive the consequences of being seen as a serious cost (Leman-Langlois, 2002), the panoptic gaze is asymmetrical and contributes to selective social monitoring or social exclusion (Hier, 2004), the theory does not capture the nuances and complexities of multi-directional information flow in the digital age (Bossewitch & Sinnreich, 2013), Foucault applied the panopticon to a societal phenomenon while Bentham considered it to be for a small, closed community and the theory simply cannot take into account the power of modern databases (Ansorge, 2011).

> ...for some who have studied surveillance for some time, mere mention of the panopticon elicits exasperated groans. For them, too much has been expected by too many of the panopticon with the result that the diagram is wheeled out at every conceivable opportunity to well, explain surveillance (Lyon, 2013, p. 52).

To overcome these limitations, scholars have either reimagined Bentham's panopticon to fit the new big data environment or have disregarded the theory altogether for a more modern framework. Bauman (2013), contests the panoptic model is alive and well, but only in institutions such as prisons, camps and psychiatric clinics or marginalized spaces, particularly in the global south. Although, when discussing

workplace bureaucracy, Bauman refers to mobile devices as a personal panopticon: "...just as snails carry their homes, so the employees of the brave new liquid modern world must grow and carry their personal panopticons on their own bodies" (p. 59). Mobile devices force employees to be at their superiors' call, enacting a 24-hour, 7-day a week surveillance on employee performance. Moreover, Bauman posits society has moved to a seduction model of self-surveillance rather than a disciplinary one, especially in the workplace. This managerial revolution departs from top-down surveillance, to the "experience economy" characterized by seduction and performativity, forcing employees to self-regulate and outperform themselves and one another (p. 73). Boyne (2000) in his analysis of the current state of panopticonism, argues Bauman's "fun ethic" is over-generalized. It may be easy to express the panoptic model in terms of dualism between global north and south, but by examining societies like the United States or the United Kingdom, it is difficult to argue the seduction model is the only form of societal control. Boyne calls for an integration of both the traditional panoptic model and the seduction-exclusion model that Bauman offers.

In regard to big data, Bauman (2013) expands on Gandy's (1993) panoptic sort - a theory which denotes surveillance as a categorizing method used to discriminate - in relation to modern surveillance techniques. Users contribute to the databases that categorize them in the panoptic sort. Rather than discriminating against these users, databases target users as prospective buyers. Similarly, Lyon (2002), proposes a theory that explains surveillance as social sorting. Not only do surveillance practices limit individual freedoms, they create and reinforce social differences. Lyon expands on Gandy's (1993) notion of the panoptic sort and applies it to other realms of human life. According to Lyon, surveillance serves to classify and manage populations, particularly online. Like Gandy, Lyon sees marketing as an obvious example of this social sorting as users are categorized according to how valuable they are as a consumer. In other realms, such as policing, surveillance is used to predict crime according to demographics, which can exacerbate stereotypes and apply different values to individuals depending on their socio-economic status. Alternatively, online, social sorting is no longer a regional matter and is seen in terms of flows and networks, rather than geographically. Chow-White and Green (2013) observe this social sorting phenomena in the context of big data and genome science. While technologies used to collect big data are presented as value-neutral, the practice of collecting and interpreting this data stems

from an institutional or organizational base of knowledge that contributes to decision-making. Chow-White and Green argue the process of decoding big data to discernable patterns of human behaviour and social relations is a political and communicative act, which can lead to biased interpretations and social sorting. Recently, Lyon (2018) revisited his position on surveillance as social sorting and characterized the modern era of surveillance as “user-generated surveillance.” Users contribute content to be surveyed and in turn, survey others in the form of liking their posts, or following their newsfeed. Today’s surveillance society then, is a product of digital modernity where there is a new imperative to perform, especially online. In doing so, users willingly share their personal information, contributing to the modern surveillance culture.

Like Lyon (2013), Vaidhyanathan (2012), expresses his exasperation at the overused panopticon model stating: “...this trope has exhausted its utility” and “Those who write about privacy and surveillance usually can’t help invoking the Panopticon to argue that the great harm of mass surveillance is social control” (p. 84). However, Vaidhyanathan argues that the panopticon does not in fact deter delinquent behaviour as proven by CCTV cameras that regularly capture these behaviours. Instead, he offers the cryptopicon, which involves the ubiquitous surveillance of an individual by many, or all. The cryptopticon theory adequately addresses why online conglomerates have an interest in exploiting users’ personal information, the cost of this surveillance to the user, and what users can do to resist it. Instead of regulating our behaviour, major corporations like Facebook and Google hope that users express their individuality which can then be exploited via precise marketing tactics. Unlike the panoptic sort, cryptopticon encourages individuality rather than categorization, so marketers can capitalize on eccentricities rather than through blanket, all-encompassing marketing ploys. Vaidhyanathan argues this online self-expression is so woven within the fabric of Web 2.0, that users are unsure how to avoid the negative consequences associated with surveillance. Only those technically savvy users can avoid the pitfalls through techniques such as changing default settings or employing virtual private networks (VPNs). This technically confident, wary group of users is the focus of this paper. In this study, I examine users actively engaged in online privacy protection, who are aware of the consequences of data mining and online surveillance. Vaidhyanathan’s theory falls in line with surveillance as exploitation theories such as Andrejevic’s (2002) “work of being watched.” Andrejevic outlines the asymmetrical power structure that exists in our current

Internet architecture, where corporations own and control much of the data that is generated by consumers. Andrejevic addresses panopticonism in his theory, but its productive deployment rather than its repressive force. Unlike the centralized power the panopticon wields, current surveillance is self-stimulating, and creates a cycle of rationalized consumption. Similar to the way workplace surveillance encourages production, online surveillance instigates participation within a consumer society.

Surveillance theory is wide ranging and has been developed by a variety of disciplines including communications, sociology, criminology and political science. The topic of surveillance has grown with the information society and era of big data. Surveillance literature from the social sciences is often theoretical and descriptive as scholars grapple with big picture understandings of surveillance, its ties to political economy and neoliberal ideologies. There are notable empirical studies of surveillance and communication including Marwick and Boyd's (2014) ethnographic project on teen social media practices; Moore, Piwek and Roper's (2018) study in self-tracking in the workplace; and Spiller et al's (2017) analysis of how users view and value data collected via self-tracking devices. Moreover, while scholars outline the negative implications of big data surveillance, there is little research and assessment conducted on how users can practically protect their online privacy. According to Smith, Dinev and Xu's (2011) assessment of information privacy research, they found an abundance of theoretical developments and purely descriptive studies of privacy that have not been addressed empirically. The authors found that much of the empirical knowledge of privacy from the social sciences evaluates levels of individual privacy concern and privacy risk assessment. Further, limited studies focus on the outcomes of attempts to mitigate privacy or the process of implementation of normative conclusions. Oftentimes, normative conclusions do not lend themselves to empirical study. This thesis adds to both theoretical and empirical notions of privacy as blockchain privacy platforms will be evaluated for their affordances and constraints. This study addresses the gaps in literature mentioned, as it provides a practical evaluation of blockchain privacy platforms, within a theoretical context.

Throughout this review, I focused on progressions of the panoptic model. For years, the panoptic model has been the key metaphor for understanding the role of privacy in society. For instance, in the age of Taylorism, managers became guards in the watchtower, and employees became prisoners, controlled through constant surveillance.

As surveillance technology progressed, the panoptic model became limiting, and surveillance theorists have imagined countless iterations of the metaphor to better represent the ubiquity of online surveillance techniques we see in Web 2.0 and beyond. Rather than focus on the disciplinary aspect of the panopticon, post-panoptic models, such as the cryptopticon, look at the exploitative aspects of online surveillance. Surveillance theory provides theoretical context for this paper by demonstrating the exploitative nature of online surveillance practices, insinuating a need for mitigation put forth by blockchain privacy platforms.

2.4. Big Data and Privacy

Web 2.0 and 3.0 are marked by big data, algorithms and predictive technology, shifting our surveillance into new and alarming territory. Surveillance theory in the digital world focuses on the consequences of big data and the ways in which users contribute to our modern surveillance culture. By participating online, particularly on SNS, users provide digital intermediaries with mass amounts of personal data that is used to personalize SNS feeds, advertise and provide platforms with user feedback. Moreover, surveillance theory posits a more nefarious goal of data collection, that of social sorting and societal control. This section explores what privacy means in the age of big data. From SCR, we know that understanding privacy is a complex process involving history, culture, social norms and technology (Craig and Ludloff, 2011). This section begins with an explanation of big data and the ideologies that support our big data society. Next, I situate privacy within this big data era and explore how blockchain could help mitigate the negative consequences of data collection.

Chow-White and Green (2013) characterize the first ten years of the 21st century as the “decade of data” (p. 556). As the Internet transitioned from the static, hyper-linked Web 1.0 to the sharing economy of Web 2.0, and now, the intelligent Web 3.0, the amount of data produced and collected is staggering. According to the World Economic Forum, the amount of data in the digital universe is expected to reach 44 zettabytes by 2020 - 40 times more bytes than there are stars in the observable universe (2019). These bytes come in the form of tweets (500 million per day), emails (249 billion per day), searches (5 billion per day), and much more (Desjardins 2019). Technologies used

to collect and interpret this data have grown in sophistication along with the Internet, particularly in areas of cloud and molecular computing, artificial intelligence, machine learning and natural language processing, among others (Schintler and McNeely, 2019). Data management systems have transitioned from structured, relational databases to schema-less catchalls to capture the increasing volume, variety and velocity of big data. For instance, BigTable, developed by Google Inc, is a highly adaptable data storage technology that can manage petabyte scale data on thousands of machines (Siddiqa, Karim and Gani, 2017). Chow-White and Green (2013) define this schema-less, data mining process as:

> ...the nontrivial process of using algorithmic techniques to discover (faster than is humanly possible) hidden patterns and unknown relationships among many variables in masses of observed data to produce understandable, meaningful, and potentially useful information for knowledge building and decision-making (Chow-White & Green, 2013, p. 559).

While this paper focuses on the negative implications of big data collection for users, this data is an invaluable resource for innovators, scientists and researchers. Big data reaches nearly all sectors of society and allows experts to better understand our world. With big data, we are better prepared to predict disease outbreak, address climate change and foster economic development (Mayer-Schonberger and Cukier, 2013). In studying privacy, we cannot disparage big data collection altogether, as its positive implications for society are tremendous. Mayer-Schonberger and Cukier (2013) use Farecast, a website that tracks airline ticket prices using big data, to illustrate how big data drives innovation. Farecast transformed the airline ticket industry altogether by providing intelligent airfare predictions to consumers. Frizzo-Barker and Chow-White (2014) outline big data's contribution to healthcare in medical discovery, treatment decisions and precision medicine. In addition, Craig and Ludloff (2011) explain how governments use big data to combat crime and terrorism and increase national security. While these big data practices impose a trade-off between personal privacy and societal innovation, big data as currency or as a source of economic value poses a significant threat to fundamental values, such as autonomy, fairness and most importantly, the right to privacy. Van Dijck (2014) defines this information paradigm as datafication, and the widespread optimism and belief in the datafication process as dataism. This ideological grounding is a widespread secular belief supported by institutional rhetoric, such as big data as imperative for research discovery. To Van Dijck, dataism explains why users

entrust their personal information to corporate platforms and public institutions. This brings us to scholarly contributions that consider privacy within a dataism context. Scholars have become increasingly interested in the tension between big data and privacy and have taken a critical look at this new information paradigm.

Scholars have grappled with the idea of separating the public from private realms and the rights beholden to those who wish to maintain the sanctity of their personal communications. Habermas (1962) is at the forefront of this discussion, and his public sphere philosophy is still widely cited by communication scholars, particularly in reference to social media as a new public sphere. For Habermas, the public sphere was a social life outside of private communication where citizens could freely assemble and discuss societal life in an act of democracy. In Greek philosophy, the polis was a space for public opinion, and the “wants of life and the procurement of its necessities” were only discussed within the oikos (home, or private life) (p. 4). While Habermas emphasized the importance of the public sphere, for social scientists today, the pendulum has swung towards advocacy for the private realm (Bailey, 2000). According to Bailey (2000), the vitality of the public sphere has dwindled due to postmodern thought and globalization, as a world exists beyond what can be influenced by local public spheres. Like Habermas, Bailey understands the private realm to be “areas of social life which are protected from anything other than personal or domestic gaze” (p. 384). Like most scholars discussing privacy, Bailey acknowledges its vagueness and complexity. This dualism between public and private life is increasingly challenged, as outside forces such as culture and socialization aid in the construction of private realities. Butt and Langdridge (2003) too, disagree with the complete separation of private and public life as outlined by Habermas and Cartesian privacy. Like Bailey, Butt and Langdridge seek a theoretical framework that “recognizes the social construction of the private sphere, and also sees the individual, once constructed, as being a centre of personal and moral agency” (p. 479). While public life does indeed influence an individual’s private realm and the understanding of oneself, private life should still be privileged as such, particularly in the dimensions of intimate relationships, the conscious self and the unconscious self. Butt and Langdridge add the conscious self is a significant target of control and surveillance by the public state to manage social problems. Concluding remarks acknowledge the private sphere to be “vestigial, fluid and uncertain” (p. 396).

Big data adds complexity to discussions of privacy, compelling us to consider data privacy as a new right that should be protected. Craig and Ludloff (2011) consider data privacy as a "debate about the collection and use of our personal information from a commercial and political standpoint" (p. 2). Particularly from the commercial standpoint, SNS platforms encourage users to share their personal information as a part of their business model. Some scholars suggest privacy and the current business model of these platforms is simply incompatible. Elmer (2013) argues it is this impulse to constantly share information that complicates the argument that users should be able to control their personal information. Elmer insists privacy is not dead, rather, it is fruitless to reject the political economy of social media, which is fundamentally designed as a "space of publicity" (p. 3). Rather than focus on individual privacy, Elmer suggests theoretical frameworks should tackle the accountability of corporations, particularly those who go public. Elmer likens this accountability to Bentham's original conception of the guard in the watchtower as a moral enterprise, "one that like his panopticon required an 'inspective' gaze" (p. 10). Similarly, Strandburg (2014) argues that current privacy law is currently incompatible with datafication. Like Elmer, Strandburg urges us to reconsider privacy not as an individual implication, like current policies suggest, but as a collective issue. Strandburg defines a taxonomy that could be used to redress current privacy laws for datafication, which includes a collective assessment of privacy impact, rather than on an individual basis. Barocas and Nissenbaum (2014) identify this conflict between privacy and big data as characteristic of new technological innovations over the past half-century. Drawing from contextual integrity theory, which regards informational norms as a product of social context, big data conflicts with what we expect to be entrenched in our information-flow norms. In their work, Barocas and Nissenbaum analyze anonymity and consent as a way to avoid these conflicts in the context of data collectors and human subjects. While seemingly attractive tools for maintaining privacy, the scholars reveal "virtually intractable challenges to both" (p. 45). Like Elmer and Strandburg, Barocas and Nissenbaum suggest a top-down approach that focuses on the actions of data gatherers, rather than the individuals:

> A burden is upon the collector and user of data to explain why a subject has good reason to consent, even if consenting to data practices that lie outside the norm. That, or there should be excellent reasons why social and contextual ends are served by these practices (Barocas & Nissenbaum, 2014, p. 67).

Much of the literature surrounding big data and privacy follows a similar contention. There is a clear disparity between big data and privacy regulation which requires further research and government intervention (Ohm, 2014; Trepte, 2015; Allen, 2016; Steinfeld, 2016) For instance, Ohm (2014) suggests current privacy laws are failing to protect individual users and privacy law gaps must be filled to address the risks of big data. In addition, Allen (2016) argues the moral obligation users have to protect their information is rendered implausible because of big data. Instead, businesses and governments should make a collective effort to offer more effective privacy protections. While it seems that communication scholars have denounced individual efforts to mitigate datafication, there is a movement to restore data ownership for the individual. This notion is not adequately covered in communication scholarship, and I hope to address this gap within this thesis.

Particularly in the field of computer science, researchers are empowering individuals to protect their own privacy and data through software development. By harnessing blockchain technology for privacy protection and data ownership, developers are providing individual users with the tools to re-establish data as their own, rather than as a product available for data gatherers. Within the field of emerging technologies, literature on blockchain and privacy is burgeoning. According to a systematic review on blockchain literature, 7% of literature collected from 2014-2018 focused on privacy (Frizzo-Barker et al, 2019). Frizzo-Barker et al. (2019) found that privacy was often discussed in conjunction with other topics such as healthcare, governance and cyber-security, such as a proposed blockchain application for healthcare patients to control their health data. Scholarship on blockchain and privacy often follows this practical application, as developers offer their platforms as a way to mitigate the consequences of big data and strengthen security (Dorri, Kanhere, Jurdak and Gauravarm, 2017; Yu, Li, Tian and Liu, 2018; Zhang and Lin 2018; Li, Zhu and Lin, 2019, among many others). Elisa, Yang, Chao and Cao (2018) offer a prototype of a blockchain application that can be used in e-governance to ensure information privacy and security while increasing trust in the public sector. For individual privacy and data ownership, Dunphy and Petitcolas (2018) evaluate the constraints and affordances of three blockchain-based identity management systems. These works are technical and are often published in computer science journals. A small number of blockchain and privacy literature includes introductory or descriptive works, such as Kshetri's (2017) evaluation of blockchain-

based systems in comparison to IoT for privacy protection and Schwerin's (2018) assessment of blockchain technology for privacy against Europe's General Data Protection Regulation.

This section of the literature explored privacy within the context of our current big data era. This deluge of data has provided researchers with more information about people, relationships and society that was ever thought possible. While big data works to bring about positive change within society, such as personalized medicine and urban planning, scholars recognize its consequences, particularly for individual SNS users whose information has become an easy commodity. The want for privacy is innate, which is why the topic of online privacy is so pressing in both academic and non-academic circles. Much of the scholarship outlined in this section seems to dismiss individual efforts to establish privacy and data ownership. However, by adjusting our focus to the computer science community, we see a new wave of technology based on blockchain that empowers individuals in the fight for the right to online privacy. This paper evaluates some of these blockchain privacy platforms to understand how privacy has shifted in the age of big data.

2.5. Conclusion

This literature review has brought together three areas of thought: the social construction of technology, surveillance theory and big data and privacy. I began with a brief outline of SCR as it provides the basis for understanding how concepts, such as privacy, depend on an individual's values, beliefs, location, cultural background, among others. Following SCR, SCOT provides a theoretical background for understanding how social agents influence new technologies. By comparing user discussion of privacy to conceptions of privacy put forth by blockchain platforms, we can better understand how social agents inform the development of new innovations. What aspect of privacy protection is important to users? Do blockchain privacy platforms address these concerns? How are blockchain privacy platforms socially constructed technologies? Following this grounding theory, surveillance theory provides background on the pervasiveness of modern surveillance techniques. Theories of the modern panopticon outline the nefarious consequences of big data, not only as a tool for advertisers but as a

mechanism for social control. A conversation on big data and privacy follows naturally as big data has shifted the idea of surveillance society. The political economy of SNS encourages users to share their habits, location, interests and more, which adds to the deluge of data. While individual privacy efforts may seem hopeless in the face of monopolized data troves like Facebook and Google, blockchain technology offers a solution in the form of secure, decentralized and trustless platforms that could potentially mitigate the consequences of big data to personal privacy. Each of these communication theories works to inform my research questions which are as follows:

Research Questions

1. What is the relationship between privacy discourse and technical code in reshaping power structures online?
2. Are developers/programmers of blockchain platforms responding to privacy problems brought forth by users?
3. What are the affordances and constraints of using blockchain for online protection according to user discourse?

The following chapters will explore these questions in relation to the theoretical frameworks presented. Chapter three outlines my methodological approach as informed by similar communication studies that use a SCOT theoretical framework. This chapter explains the data collection process and coding process, and my rationale for choosing each blockchain privacy platform and UGC platform. Chapters four, five and six outline my findings, and include an in-depth discussion of privacy-related themes found throughout the coding process.

Chapter 3. Methodology

3.1. Introduction

This section outlines the methodological approach I used to answer my research questions. This thesis employs a comparative discourse analysis to compare and contrast privacy discourse in social agents and blockchain privacy platforms. In doing so, this thesis explores how users negotiate power structures online by participating in cultural discourse. More specifically, this study investigates how motivated social agents on Reddit and Medium negotiate blockchain platforms' technical code through privacy discourse. In this section, I explain my rationale in choosing these particular groups to study, my methodology, and my data collection process.

3.2. Choosing Discourse Analysis

Social media analysis is a popular area of study for social scientists due to the wide availability of data and the relative ease in data collection. Early social media analyses often applied social network theory to understand the relationship between users. Now, the ubiquity of social media lends to a more robust sociological investigation (Burgess, Marwick & Poell, 2017). Social scientists look to social media platforms such as Facebook, Twitter and Reddit to understand broader societal and cultural trends that provide insight into "social phenomena that extend beyond online settings" (Pearce et al, 2020). In addition, by studying user communication, researchers can understand the role social media plays in democracy, mobilization and expressive participation (Gil de Zuniga & Coddington, 2013). User discourse on social media can also point to attitudes about a particular topic. For instance, Chow-White et al. (2017) uses Twitter discourse to understand user sentiments about the direct-to-consumer genetic testing company, 23andMe. Or, Betteridge (2016) unpacked Reddit discourse to trace patterns of misogyny within particular subreddits. When choosing a methodological approach, I explored such social media studies that had similar aims as my own. I also sought empirical studies that attempted to measure instances of social construction or used a SCOT lens to unpack user discourse. A compelling illustration of this method came from

Mills' (2018) study on the social construction of beauty in the online role-play game, Second Life. Mills employs a content analysis of user avatars to understand ideal constructions of beauty in an online space. Similarly, Bilic (2015) employs ethnographic content analysis to analyze discussion of anonymous editors on Wikipedia to understand how knowledge is constructed on the online encyclopedia. Both Bilic and Mills employ a content analysis methodology to analyze data in "their natural interaction setting" to measure instances of online social construction. Berger (2000), an authority on qualitative media analysis, endorses content analysis for researchers attempting to express qualitative data in a quantitative format such as units and percentages that can be compared and contrasted. While content analysis is a useful strategy to measure and interpret qualitative data, I opted for a discourse methodology to compare and contrast privacy narratives on blockchain platforms and UGC platforms.

In this study, I employ a discourse analysis because it allows for an interpretive method when analyzing texts. There are a number of advantages of discourse analysis as a research method, namely it is unobtrusive, inexpensive, and yields data that can be quantified (Berger, 2000). Compared to pre-Internet discourse analysis, which was time-consuming and labour intensive, online discourse analysis can be a fast and efficient alternative to interviews, surveys or focus groups. When employed in the social sciences, discourse analysis should be objective, replicable and present valid inferences from the text while providing new insights to a particular phenomenon (Krippendorf, 2004). Because the researcher is unseen and uninvolved in communication production, data collection can be relatively unbiased. This thesis aims to not only extrapolate themes of privacy from two different collectives, it also explores how privacy discourse influences emerging technologies, and more broadly, how power is negotiated online through this discourse. According to SCR, language is the tool that allows individuals to relate to one another and to organize experiences. Through online communication, individuals share common experiences through a linguistic schema (Berger & Luckmann 1966). Privacy discourse represents a greater ideology that underscores the reclamation of data sovereignty and a rejection of our current centralized Internet architecture. Berger (2000) would call for a critical discourse analysis in the investigation of privacy discourse. Critical discourse analysis examines the ideology and politics within communication and is generally critical of capitalist bourgeois leanings. However, I am interested in employing a more general approach to capture social contexts rather than

purely power relations. According to Berger (2000), discourse analysts are interested in the ways in which language shapes peoples' relationships with others and the institutions in society. Discourse analysis calls for an interpretive method, rather than a systematic method often used in content analysis. Unlike content analysis, it focuses on style and expression, rather than solely the content produced.

To inform my research methodology, I referred to Phillip and Hardy's (2002) book, *Discourse Analysis: Investigating Processes of Social Construction* as a primary resource. According to the authors, discourse analysis goes one step further than other qualitative methods because it embraces a strong social constructivist epistemology. Discourse analysis takes into account the social and political contexts in which communication is written or spoken to extract meaning.

> Discursive activity does not occur in a vacuum, however, and discourses do not 'possess' meaning. Instead, discourses are shared and social, emanating out of interactions between social groups and the complex societal structures in which the discourse is embedded. Accordingly, if we are to understand discourses and their effects, we must also understand the context in which they arise" (Phillips & Hardy, 2000, p. 4).

To use discourse analysis, researchers must understand the role language plays in the creation of social reality. Moreover, it is not texts in isolation that carry meaning, it is their connection to other discourses, the context in which they are created and their dissemination and consumption that make them significant. This thesis employs a comparative discourse analysis to discover this meaning within two different bodies of text on UGC platforms and blockchain platforms.

3.3. Data Collection and Analysis

I began my inquisition by researching burgeoning blockchain platforms. The blockchain platforms I included had to fit a four-point criteria:

1. They had to be focused on privacy protection and data ownership;
2. The website for each platform had to include clear descriptions of what privacy protection and data ownership entailed;
3. The platforms had to be fairly new developments, allowing interpretative flexibility and lastly,

4. The platforms must be discussed on UGC platforms.

The platforms that fit this criteria that I chose are Brave, Civic and Oasis Labs.

Brendan Eich, former Mozilla CEO and creator of JavaScript, founded Brave in 2015 (California Secretary of State, 2019). The beta version of the web browser was released in January 2016 and was introduced as a novel approach to ad-blocking. The Chromium-based browser uses blockchain technology to reward users that choose to view ads with Brave's cryptocurrency, BAT (Basic Attention Tokens). As of October 2019, Brave has 8 million monthly active users (Brave, 2019).

Civic was developed in California and the beta version of the Civic application was released in July 2016. The website's first blog post introduced the application as a way to "help Americans manage their identity and stop identity fraud before it happens" (Lingham, 2016). In May 2017, Civic released their Secure Identity Platform based on blockchain technology. Advertised as "redefining digital identity," the Secure Identity Platform allows users to store and secure their digital identities on their smartphones (Lingham, 2017). As of 2019, Civic offers Secure Identity Platform, Civic Reusable KYC (Know Your Customer) and Secure Relationship Verification.

Lastly, Oasis Labs is the newest blockchain privacy platform of the three and is led by CEO Dawn Song, professor of computer science at the University of California Berkeley. The private testnet was released July 2018 with an overall goal of providing a cloud computing platform on blockchain featuring decentralized trust and privacy protection. The latest release from Oasis Labs is their Devnet 2.0 and a new Oasis software development kit (SDK) to better streamline contract and app creation (Song, 2019).

The operational definition that I used for privacy was broad in order to capture as many privacy-based themes as possible. As we know, privacy is an ambiguous term that changes depending on the context, time in history, location and more. In this discourse analysis, privacy refers to informational privacy, or "the ability to determine for ourselves when, how, and to what extent information about us is communicated to others" (Westin, 1968, sec. 1). In the digital era, privacy not only means we choose how our information is communicated, but also our behaviours and actions, which are often shared in the form of data. In this discourse analysis, any textual matter that referenced this

comprehensive notion of privacy was included as a theme of privacy. The coding units were thematic, which according to Krippendorf (2004), involves analyzing text for overall features or categories that emerge from the narrative.

Researchers employing discourse analysis act as collectors and interpreters of data. For qualitative data to be deemed trustworthy and useful, the data collection and coding process must be conducted in a consistent, exhaustive and methodical manner. To ensure accuracy and rigour, I followed a thematic analysis criteria put forth by Nowell, Norris, White and Moules (2017). A thematic analysis is useful for summarizing key features of a data set and producing a clear and organized interpretation of data. This criteria outlines six phases in a thematic analysis: familiarizing yourself with the data, generating initial codes, searching for themes, reviewing themes, defining and naming themes and producing the report.

Step one, I used Nvivo12 to capture the homepage and the features page of each website. After familiarizing myself with the discourse on each platform, I chose to include both the homepage and the features page for a more comprehensive description of the privacy protections offered by the respective platforms. Next, I generated my initial code using the operational definition of privacy I mentioned previously. The overall goal of this discourse analysis was to discover, interpret and compare privacy themes on blockchain platforms and UGC platforms. Step three, I used Nvivo12 to code for themes. These themes were generated inductively, meaning, I began with privacy generally, then moved to more specific themes of privacy such as safety and security and ad-blocking. According to Nowell, Norris, White and Moules (2017), “themes are identified by bringing together components or fragments of ideas or experiences, which often are meaningless when viewed alone” (p. 8). Themes capture an important idea that relates to the research questions and link the data together (Nowell, Norris, White & Moules, 2017). The initial coding process in step three was broad and I also coded for general themes unrelated to privacy such as usability, cost. Next, I organized privacy themes into particular subcategories depending on their characteristics. By doing so, five privacy subcategories were identified: ad-blocking, data ownership, decentralization, safety and security and general privacy. For instance, on Brave’s features page, under the headings “Shields” it lists features such as cookie control, block scripts and more. This content was coded as ad-blocking. Content on the Civic homepage read, “We are giving businesses and individuals the tools to control and protect identities” (Civic, 2019).

Particularly the words “control” and “identity” indicate data ownership. If discourse on the website or features page discussed privacy in general, it was coded as “privacy general.” Further, content could be coded into more than one subcategory. Finally, I completed second and third rounds of coding to ensure accuracy. To note, I collected data on the homepage and features page as it appeared in 2019. Websites are apt to change and the discourse and content in 2019 may not be the same as they are today.

Table 1. Total Number of Items Coded on Blockchain Platforms

	Coded Items Homepage	Coded Items Features Page
Brave	6	15
Civic	9	12
Oasis Labs	7	15

Table 2. Broad Themes on Blockchain Platforms

	Cost	Open Source	Privacy	Rewards	Usability
Brave	1	1	10	2	7
Civic	1	0	20	0	4
Oasis Labs	0	0	10	0	13

After coding content on each blockchain privacy platform, I sought the most popular forums to discuss these technologies. These forums had to fit three criteria:

1. The platforms must feature strictly user-generated content
2. They must host an active community of technology enthusiasts
3. The platforms must be active enough to provide ample content for a comparative analysis

Reddit and Medium fit this rationale, and the conversations surrounding privacy and blockchain were fascinating and valuable to my research.

The Reddit community is oft-studied due to the participatory and relatively democratic nature of the platform. Anderson (2015) describes the platform as a “social scientist’s dream” because of the unique communities and subcultures that flourish on the platform (p. 9). Scholarship on these communities range from health communication, cyberpsychology, sociology and gender studies, many of which use a content analysis methodology. Reddit describes itself as “the frontpage of the internet” and the home of

“thousands of communities, endless conversation and authentic human connection” (Reddit, 2019). More often than not, Reddit users appear anonymous as only their usernames are shown. The platform is organized into communities where users can post and leave comments. Posts and comments are ranked via the “upvote” or “downvote” button and indicate users’ support or disapproval. A Reddit user’s “karma” fluctuates depending on the upvotes or downvotes they receive. A user with a large amount of karma points indicates they are relatively active or well-supported.

Next, Medium is a publishing platform that features articles written by users, professionals and organizations. To publish an article, users must join as a member at no cost. While comments are encouraged, engagement on this platform is not as high as Reddit as it operates as a publishing platform rather than a forum. However, the user-written narratives add an interesting long-form perspective to discussions on privacy and blockchain. At the time of my data collection in 2019, much of the data I collected was published in a subsection of Medium called Hackernoon. Hackernoon has since parted with Medium to become an independent technology media site. For the sake of brevity and because Hackernoon was still a part of Medium at the time of data collection, this content will still be considered from Medium. I used a private browser to search a combination of keywords on Google that included the term “privacy,” the name of the blockchain platform and either “Reddit” or “Medium.” For instance, “Brave” and “privacy” and “Reddit” or “Civic Labs” and “privacy” and “Medium.” All combinations of these search terms were used to capture privacy discussion on all three blockchain privacy platforms on both Reddit and Medium. To keep the results manageable, I only examined content on the first page of Google results. Posts on Reddit and Medium spanned 2017 to 2019, which coincides with the newness of each blockchain platform.

Again, I followed the qualitative coding steps outlined by Nowell, Norris, White and Moules (2017) which identifies broad themes and then moves towards more specific themes of privacy. Four themes of privacy were identified in the coding process done with Nvivo12: ad-blocking, data ownership, general privacy, safety and security and trust and ethics. Throughout this process, I chose to leave usernames as is, rather than anonymize them. I consulted both the Tri-Council Policy Statement and the Association of Internet Researchers to inform my rationale. Both guidelines state that users do not have to be anonymized if there is no expectation of privacy. Reddit and Medium are both public platforms and the discourse I analyzed was not password protected. Furthermore,

the privacy policies of Reddit and Medium explicitly state that their usernames and content are in the public domain.

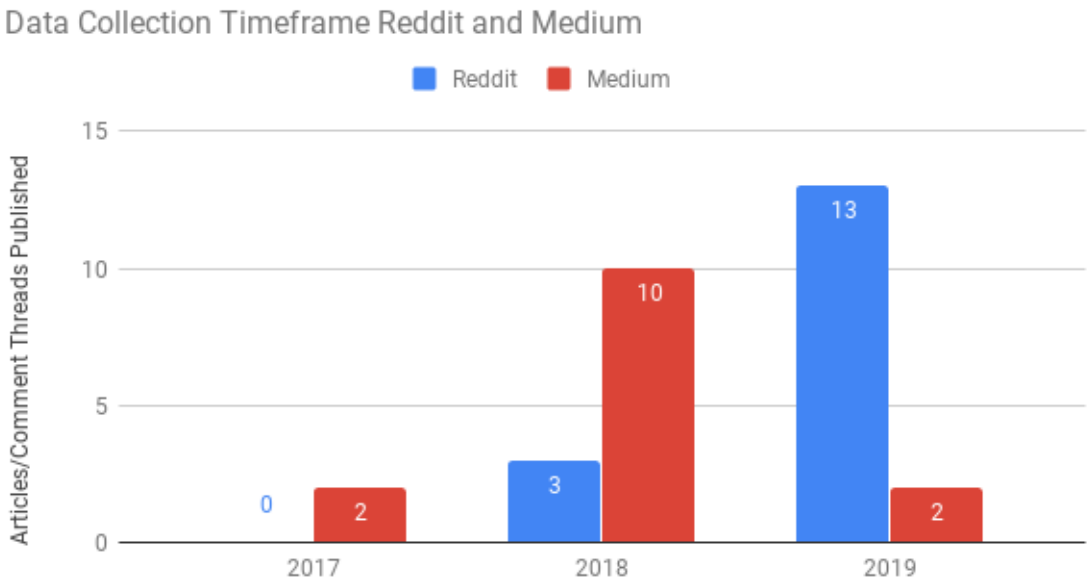

Figure 1. Timeframe of Medium Articles and Reddit Comment Threads Published

While discourse analysis is less obtrusive and poses minimal risk to humans compared to other data collection techniques such as interview or focus group, there are challenges. Two of the most significant challenges are finding an appropriate sample size, and ensuring reliability in coding (Berger, 2000). Collecting an appropriate sample size was not an issue as my search parameters were ample, yet restrictive enough to produce a suitable number of texts to assess. Conversely, because I was the only researcher inductively coding for privacy, among other themes, it is difficult to ensure coding reliability. To mitigate the risk of inaccurate coding, I coded the same content three times, starting with major themes and then narrowing down with each pass through. An operational definition of privacy was used to further ensure coding accuracy. Moreover, when searching for content on the Internet, it is important to note that depending on browsing habits, location and preferences, users' interfaces may appear different than others. Search terms could yield different results depending on a user's

particular Internet environment. To mitigate personalized algorithmic influence, I cleared my search history and cookies and used an anonymous browser when conducting my research. Furthermore, I was not logged into a Reddit or Medium account when gathering data. To note, due to my location, I have a specific view of the Internet that other individuals the world over may not experience. The western Internet experience is not an accurate representation of the online space in its entirety. This thesis is a Eurocentric analysis of privacy themes.

This section provided a rationale behind choosing a methodology, selecting platforms to analyze and the coding process. Discourse analysis proved a successful methodology to interpret online discourse, the context in which it was communicated and its relationship to other texts. Themes of privacy were sought inductively and became evident throughout the coding process. By employing a comparative discourse analysis, I translated qualitative themes into quantitative data that can be easily compared and contrasted. While discourse analysis does present limitations, such as coder bias, I remained objective as possible in my examination and used techniques such as clearing my Internet cookies to ensure objective search results.

The following chapter explores the results of my comparative discourse analysis as I examine themes of privacy through a SCOT lens. Chapter four first outlines the Internet as a socially constructed technology, then moves on to explain blockchain in a similar way. Following this exploration, I discuss the privacy themes I discovered throughout my coding process. Through identifying privacy themes, I can understand how blockchain privacy platforms conceptualize privacy and compare this to groups of users on Reddit and Medium. Overall, the findings will inform the social construction of blockchain platforms.

Chapter 4. Blockchain Platforms

4.1. Introduction

Blockchain platforms must be oriented within a SCOT framework to understand the significance of the data collection. By comparing user conceptions of privacy to blockchain platforms' idea of privacy, we can discover if user values are represented in emerging technology. This informs whether or not privacy discourse is used to negotiate blockchain's technical code and overall power structures online. For users to have an impact on the development of blockchain privacy platforms, the technology must be in a state of interpretive flexibility, which cites human participation as critical in determining the final definition of a new technology (Bakardjieva and Feenberg, 2004). The process of interpretative flexibility takes place in emergent technologies before they are embedded within society. Social agents negotiate the meaning of a new technology before what Pinch and Bijker (1984) characterize as closure. Closure is reached when the dominant group of social agents reaches a consensus of the meaning and purpose of a burgeoning technology. According to Doherty, Coombs and Loan-Clarke (2006), information technologies are particularly flexible when technology developers involve users in trial stages of the technology, which we see in blockchain privacy platforms. This section will trace the development of blockchain technology and explore the characteristics of blockchain that make it intrinsically flexible. In this chapter, I argue that like the Internet, blockchain is conducive to heterogeneity. Blockchain was shaped by motivated social agents to better represent values of decentralization and equality. By presenting blockchain as a socially constructed technology, I argue social agents on Reddit and Medium are currently reshaping blockchain privacy platforms to better represent characteristics of privacy protection valuable to them.

4.2. Social Construction of the Internet

It is unproductive to consider the Internet as an autonomous entity as its ubiquity demands an inseparability from the social world. In our modern, digital era we are rarely offline and with increasing technical sophistication we may never have to be. By

examining our current Internet architecture, it is easy for users to consider themselves separate from the development process of the Internet. Today, the Internet landscape is characterized by major conglomerates, fueled by big data as a commodity, creating a centralized space motivated by commercial interests. In academia, this alienation of the user is invigorated by arguments of communicative capitalism, the audience commodity and exploitation (Dean, 2005; Smythe, 1981 and Andrejevic, 2002). While these theories are relevant and important particularly in discussions of big data and privacy, the power of users in reconstructing the Internet is understated. Similar to the way big data and privacy theorists underscore the capabilities users have to protect and own their data, communication theorists neglect the democratic potential the Internet maintains, despite its current centralized framework. Feenberg discussed this very notion at the 2013 Dialectics of the Digital World conference at Athabasca University. Here, Feenberg argues contemporary critical theory has framed the Internet as a "problem rather than the solution to the crisis of democracy" (p. 1). Feenberg acknowledges that while such critiques of the Internet are crucial, they "deflate the myth of the Internet as a revolutionary technology" (p. 1). For instance, Dean (2005) argues the network society has effectively transformed online communication into capitalist production as messages simply become contributions to this capitalist ethos. Communicative action, be it commenting, liking, or sharing is a form of passivity, a consequence of technological fetishism, rather than democratic action. While I agree with notions of user exploitation pushed forward by scholars such as Andrejevic (2000), I also contend that there remains room for motivated social agents to redefine their online environment. Feenberg's (2013) five layers of the Internet makes the technology conducive to constructivism: a non-hierarchical structure, anonymity, broadcasting, data storage and many-to-many communication. With this technical structure in mind, Feenberg disputes the undemocratic nature of the Internet and asserts these layers can accommodate special interests which can alter the very nature of the Internet. To illustrate the Internet's inherent flexibility, I will discuss key instances throughout the Internet's history that exemplify its social construction.

The introduction of a network linking computers via Arpanet in 1969 set the tone for our modern digital landscape. The United States Department of Defense funded the development of Arpanet as a tool for data transfer between research institutions. Those involved in the design process of Arpanet, which Braman (2011) characterizes as "the

framing years," had to consider the nature of society, communication, politics and the law in their technical design. With Arpanet, institutions like the University of California at Los Angeles and the Stanford Research Institute could use computers in other locations and transport files back and forth (ARPAnet, 2019). Braman (2011) in her analysis of Arpanet's technical documents noted that this early iteration of the Internet facilitated change: "the fact that technical solutions continued to change once put in place was particularly vexing" (p. 298). Developers agreed that protocol change could slow down network development, but also stimulated further innovation. Because developers embedded change as a value within the technical design of Arpanet, key technologies emerged that otherwise would not have. It is these cases that demonstrate the transformative power of social agents; first, in the developers that built Arpanet with flexibility in mind, and second, in the users that adapted Arpanet to suit their particular needs. Once email capabilities were introduced in 1971, users began creating online discussion groups with other users that held common interests. This peripheral TALK function of Arpanet became the main interest for users, and within four years of its implementation, it made up three quarters of all traffic (Bartlett, 2016). Arpanet's successors, Usenet and Bulletin Board Systems, became communication centred networks, hosting chat rooms and forums for those with access to the technology.

A similar instance of social construction can be seen in France's version of networked computing, the Minitel. According to Feenberg (1992), the Minitel was designed to bring France into the digital age and gave users access to a variety of databases. What was a rational project to improve the flow of information became a budding personal communication network at the hands of social agents. While the Minitel provided users with a wealth of bibliographic information, hackers adapted the seemingly insignificant communication application, Gretel, into a widespread messaging system. The primary use of the technology became for anonymous chatting with other users for "amusement, companionship and sex" (Feenberg, 1992, p. 308).

Firms recognized the potential profitability of this communication through advertisements and firms reworked the Minitel to accommodate increasing communication on the network, which in turn altered its technical code. This exemplifies the different ways social agents interpret new technologies, which can result in a redefinition of the technology altogether. For Feenberg (1992), this demonstrates why scholars must examine the sociopolitical environment and the actors involved when

tracing the technological developments. While Arpanet became defunct in the 1990s “its effects on online communications in the late twentieth and early twenty-first centuries was immeasurable” (ARPAnet, 2019, sec. 4).

Finally, in 1990, Tim Berners-Lee developed a prototype for what would become the World Wide Web. With this prototype, Berners-Lee set out to create a decentralized infrastructure that would allow separate academic departments to maintain projects and documents. By 1994, what was once a niche tool used largely by government officials, computer scientists and academics was now in the hands of the public (Aiello, 2018). Like many new technologies, the Internet was heralded as revolutionary. The optimism surrounding this new technology sparked movements such as cyberfeminism. This branch of feminism saw the Internet as an empowering tool for women, a space where women could experiment with identity and gain new forms of power and authority (Plant, 1997). In the same vein, cryptoanarchists of the early 2000s predicted the Internet would eventually dissolve the nation state to create a libertarian way of life, free from government control (Bartlett, 2016).

However, while early iterations of the Internet, such as Arpanet and the Minitel, possess obvious signs of social construction by users, the cyberspace we know today is unlike the decentralized community Tim Berners-Lee envisioned in the 1990s. The Internet today has become increasingly centralized as players, like Facebook and Google, own a major share of user data, information and power. Hughes (2019), cofounder of Facebook, penned an opinion piece in the *New York Times* outlining Facebook’s control over the current market. Hughes argues this monopoly, which was made possible by the Federal Trade Commission, should be broken up into multiple companies to reign in its utter dominance over the market. Not only that, Hughes (2019) argues for a new agency, empowered by Congress to regulate technology companies and protect user privacy. While academics and thought leaders see regulation and privacy protection as a top-down approach, the Internet maintains the dynamism and fluidity put forth by Feenberg (2013) that allows users to negotiate power from the bottom up. Social agency, innovation and social construction can be seen when users attempt to protect their privacy on their own. The technical layers of the Internet, despite being exploited by conglomerates, still support its social construction, which is best represented through the development of blockchain technology.

4.3. Blockchain Technology and Social Agency

Like the Internet, blockchain is comprised of layers: it is a decentralized, encrypted, public or private ledger that operates on a peer-to-peer network. In its early stages, blockchain was intrinsically tied to bitcoin as a platform for monetary transactions to take place anonymously and free from third party regulation. Through blockchain, encrypted transactions are stored on a public ledger and verified through a voluntary peer network. As transactions are verified, the information is stored to a preceding block, creating a chain. As of November 2019, Bitcoin remains the top cryptocurrency, followed by Ethereum and XRP (CoinMarketCap, 2019). The origins of blockchain come from Satoshi Nakamoto's 2008 white paper, a document outlining a new, paperless currency that operates solely through a peer-to-peer network. According to the white paper, Nakamoto's motivation behind Bitcoin was to create a digital currency that avoids the pitfalls of financial institutions which includes cost, fraud, and most importantly, trust (2008). Flanagin, et al. (2009) would classify Nakamoto's white paper as a technical code document - a document that outlines the need to re-evaluate an artifact's technical code. For instance, in his landmark book, *Unsafe at Any Speed,* Ralph Nader (1965) investigates the design flaws of U.S. automobiles and its impact on consumer safety. Nader spurred a re-evaluation of American's automobile industry and eventually the instatement of the National Traffic and Motor Vehicle Safety Act just a year later in 1966 (Brumagen, 2018). Nakamoto's white paper holds a similar evaluative mission, particularly towards the financial industry and governmental institutions. Baldwin (2018) posits this technical code document helped shift American ethos from "In God We Trust" to "In Digital We Trust" (p. 2). The transition from material wealth to symbolic wealth has long been theorized. The transition from paper currency to digital is said to be a natural step in the dematerialization of currency. Hayek (1976) famously called for the denationalization of money in the form of private and competitive currencies. To Hayek, the government failed to provide a stable currency, and the supply of money should be in the hands of the marketplace for the good of self-interest. Similar libertarian ideas are expressed by Rothsbard (1963) in his critique of government-controlled currency. Rothsbard proposes money as a factor in the free market to ward off government invasion of person and property. Too, Goux (1994), outlines the transition of money from

gold; or material money; to paper, a representation of money and finally, to immaterial digital money.

Bitcoin emerged in 2008 in a time of economic tumult. In the United States especially, the Great Recession was in full force, creating an atmosphere of distrust in centralized banks and the government for the subsequent bailouts. According to Baldwin (2018), the first bitcoin block held a concealed message that read: “The Times 03/Jan/2009 Chancellor on brink of second bailout for banks” (p.3). This message made clear the current problems with the traditional banking system. While each cryptocurrency embodies its own narrative and values, the philosophy of bitcoin - economic freedom and decentralization - piqued the interest of right-wing libertarians. Swartz (2018) in her analysis of the emails surrounding bitcoin’s launch surmised that early bitcoin conversations represented anti-government and cryptopunk values made popular in the 2000s. While the creation of bitcoin is credited to Nakamoto, Swartz argues it was a collective effort of social agency, an amalgamation of years of crypto discourse and crypto-anarchy, which was revealed in an email connected to Bitcoin’s creator Satoshi Nakamoto that read “We are all Satoshi” (p. 6). Reimagining currency and the narrative surrounding physical capital itself was a significant step in socially constructing the currency to better represent social values such as individual agency and trust.

Shortly after Bitcoin disrupted the financial sector, blockchain began drawing attention of its own. Frizzo-Barker et al. (2019) saw a rapid increase in blockchain publications beginning in 2016. While the majority of interest remains within the financial sector (31%), they identified significant publications in fields such as business (25%), law and governance (22%) and privacy (7%). Like Bitcoin, there is considerable hype surrounding blockchain. Swartz (2017) described it as an “equality technology, one that can be used to expand freedom, liberty, possibility, actualization, expression, ideation and realization for all entities in the world, both human and machine” (p. 42). Like Bitcoin, early use-cases of blockchain were consistently described as disruptive or reactionary to the current economic, social and political climate, particularly online. Early descriptions of blockchain exemplify the hype and optimism surrounding its revolutionary potential. For Koonce (2016), the most poignant part of early blockchain discussion is the revaluation of existing digital infrastructure and the long-established business practices that currently underpin our Internet architecture. Offline, too, Koonce describes

a range of industries that could be disrupted by blockchain including supply chain, manufacturing, and the music industry. Similarly, Aztori (2017) highlights blockchain's ability to transform not only finance and business, but the digital world as we know it. Aztori argues the danger of central powers in a tone reminiscent of early crypto anarchists and suggests that centralized control leads to disempowered citizens. Blockchain then, represents a desire for increased digital democracy, a transition from central authority to decentralization and a stronger trust in computations over people.

Redshaw (2017), directly applies blockchain to Feenberg's critical theory, outlining the significance of social agency in technical action. Bitcoin and blockchain prove that online subgroups can appropriate technology to create an alternative future, demonstrating the importance of agency in technical action and resistance. While Redshaw acknowledges the significance of social construction in new technology, he argues this social shaping is not always a case of democratic rationalization as Feenberg suggests. As in the case of blockchain, this construction is an example of popular rationalization, rather than democratic decision making. Similar to the cryptoanarchists surrounding Bitcoin's launch, the subgroup subverting Nakamoto's "time-stamp server" represents a distinct subgroup that hold largely libertarian values such as decentralization, and individual agency.

From Nakamoto's distrust in third party intermediaries, to the increased academic interest in the decentralized values of blockchain, the technology is rife with social agency and presents an alternative view of digital infrastructure. Just as the feudal system was overturned by revolutionaries, central authorities in the digital space are being reimagined through blockchain to better reflect the values of individual users.

4.4. Blockchain Solutions

This thesis investigates a particular subgroup of social agents interested in testing blockchain privacy platforms. Online privacy advocates say the Internet has strayed from its original design as a community model, which Feenberg (2013) argues is imperative for online participation. Instead, the Internet has veered towards a consumption model, serving business interests rather than user interests. Features of a consumption model support commercial transactions and advertising through data

mining, cookies, and location tracking, while the community model upholds egalitarianism and participation in public discourse. Both online models exist in conflict, as users and businesses vie for the Internet's preferred technical code. Although, as transnational corporations continue to dominate larger portions of Internet traffic, it seems the consumption model defines our current online environment.

This was not always the case, and Tapscott and Tapscott (2016) describe the early Internet as possessing the aura of a young Luke Skywalker - ""with the belief that any kid from a harsh desert planet could bring down an evil empire and start a new civilization by launching a dot-com" (p. 12). According to O'Reilly (2006), it was not until the dot-com bubble that the community model of Tim Berners-Lee's original web began to shift.

> Ironically, Tim-Berners Lee's original Web 1.0 is one of the most "Web 2.0" systems out there - it completely harnesses the power of user contribution, collective intelligence, and network effects. It was Web 1.5, the dotcom bubble, in which people tried to make the web into something else, that fought the internet, and lost (O'Reilly, 2006, para. 4)

While there are successful examples of mass collaboration in websites like Wikipedia, centralized powers have redefined the Internet as their own. The Internet is a space where user data is the new asset and power is easily acquired by a few conglomerates. Not only commercial interests, but governments too exploit big data to survey citizens, silo information and censor content. In their annual report on the state of the Internet, Freedom House identified decreasing Internet freedom due to authoritarian regimes subverting social media for political distortion and social control (Shabaz and Funk, 2019). The report cites countries such as China, Iran and Saudi Arabia as prime examples of expanded efforts to manipulate the online realm. For Internet optimists, such as Tapscott and Tapscott (2016), the answer lies in new technologies such as blockchain, and the social agents motivated to apply these technologies toward individual liberty. Primarily, blockchain could reverse authoritarian trends by allowing users to own and manage their online identity and personal data. Innovators have already applied blockchain for such purposes. There are currently applications being developed to digitally store users' personal records such as a drivers' license, birth certificate, or a land title (Jacobovitz, 2016; Dunphy & Petitcolas, 2018; Li, et al., 2018). This way, records can be released and revoked at will. Some applications will even allow users to monetize their data to corporations or third parties if they so choose. Kshetri

(2017), compares blockchain data storage to traditional cloud-based storage systems, particularly in areas of manipulation and security. Overall, Kshetri posits blockchain solves the key challenges associated with IoT security through cryptography and decentralization, while citing its newness and low adoption as potential issues. Particularly for industries that require the transmission of sensitive documents, such as healthcare, Kshetri sees blockchain as an important breakthrough in record storage and exchange.

While blockchain is in its nascent stage, the technology has come a long way since its introduction in Nakamoto's white paper. The enthusiasm surrounding the opportunity to alter the future of the Internet remains palpable, and in some cases, social construction has materialized into new technologies. For instance, Zyskind, Nathan and Pentland (2015) created Enigma out of the Massachusetts Institute of Technology (MIT). The blockchain-based, open-source protocol is a decentralized privacy solution, with a goal to "unlock the original potential of the Internet and empower individuals all over the world" (Enigma, 2018). Enigma gives developers the opportunity to perform computations on encrypted data, making decentralized solutions more accessible. As of June 11, 2019, developers have access to the Enigma testnet and can begin building secure blockchain-based applications. Also, out of MIT comes Invisible Ink, a similar technology that uses blockchain to distribute sensitive data, creating autonomy through heightened transparency, control and security of personal data. The aim is to take back "what once was rightfully ours and under our control" (Lazarovich, 2015, p. 3). Invisible Ink also boasts a certified mail service that allows users to send encrypted messages that can only be decoded by recipients. Social networks too have been reimagined to showcase the values associated with blockchain's community model. Ushare is one such network by Chakravorty and Rong (2017) that works to solve the privacy implications of centralized social networks. Ushare is a blockchain-based social media platform that allows users to control, trace and own their content. Users can share their data with a chosen circle of friends, while maintaining an unbreakable link with their data, even if it is shared outside the circle. Similarly, Mihai Alisie, co-founder of Ethereum, created Akasha which is a platform that promotes freedom of expression, communication and privacy rights through a decentralized social network. According to the Akasha team, the project began as "an idea embedded in a handful of minds...that crystallized into a community of thousands of people united by the dream of a better

home of mind" (Akasha, 2018). After three years, the next phase of the social network, Akasha Reloaded, is available for early access. There are numerous examples of blockchain-based applications, but they all share a similar origin story: an attempt to reassert values that were ingrained within the Internet's original model such as decentralization, anonymity, community and democracy. Next, chapter five outlines the findings from the discourse analysis on blockchain privacy platforms and interprets themes of privacy as they relate to these values. These themes will then be compared to themes of privacy presented by social agents on UGC platforms, which will be detailed in chapter six.

Chapter 5. Privacy and Blockchain

5.1. Introduction

This chapter examines how blockchain privacy platforms frame privacy discourse. By comparing conceptions of privacy between blockchain platforms and its users, we can better understand how one shapes the other. Because these blockchain platforms are relatively new and in a state of flux in response to user feedback or technical updates, this is an ideal stage for examination. Interpretive flexibility is typically applied to the development phase of artefacts. The relationship between constructions of online privacy from blockchain platforms and its users can help us understand the impact of social agents in the construction of nascent technology. More importantly, this comparison provides insight on how users can negotiate power structures online through cultural discourse.

5.2. Unpacking Themes on Blockchain Platforms

Blockchain privacy platforms represent a change from the status quo, a reaction to current online social, economic and political conditions. An initial pass over Brave, Civic and Oasis Labs presents discourse centered around user-control. Much of the content on the homepage is user-focused, repositioning the power towards the individual. For instance, the first and largest title on the Brave homepage reads: “You are not a product” (Brave, 2019) (Fig. 2). Civic’s homepage title presents a similar empowering message: “We are giving businesses & individuals the tools to control and protect identities” (Civic, 2019) (Fig. 3). Additionally, the Oasis Labs homepage tells users to “Unlock the potential of your data without compromising security or privacy” (Oasis Labs, 2019) (Fig. 4). By engaging in user-focused discourse, these platforms are creating an alternative narrative that disputes centralized conglomerates as a central authority online.

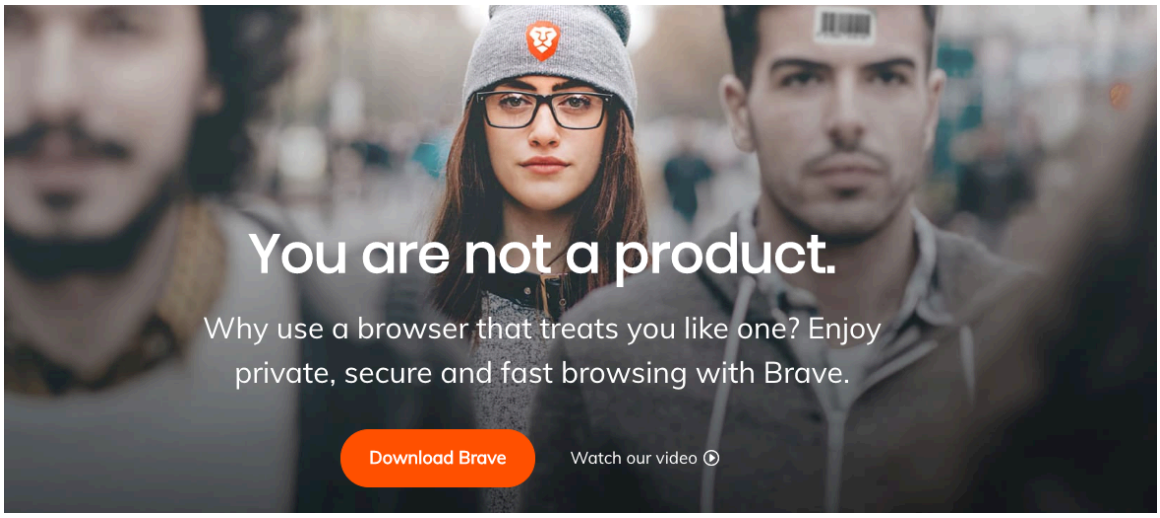

Figure 2. Brave Homepage

Figure 3. Civic Homepage

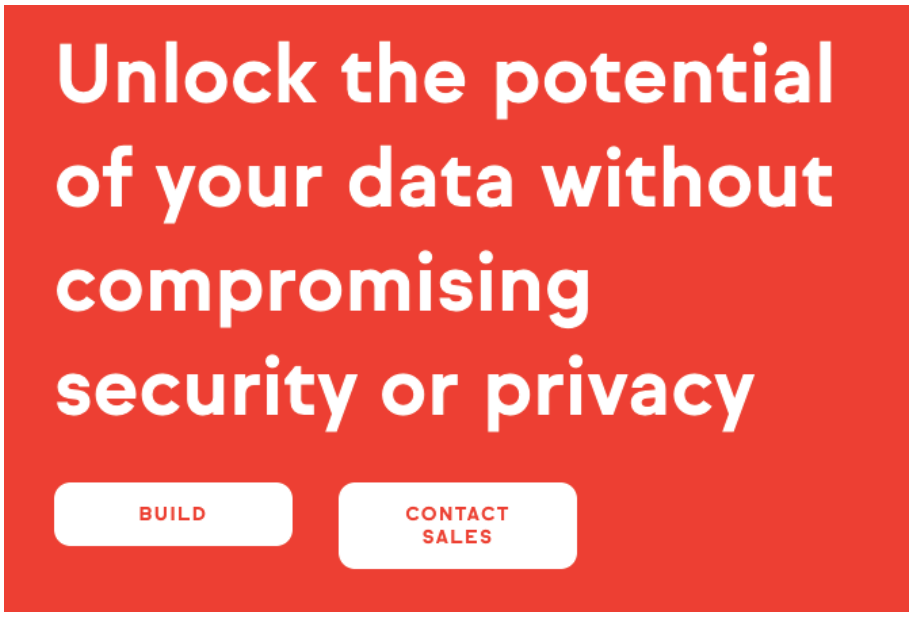

Figure 4. Oasis Labs Homepage

Besides the user-focused discourse, an initial observation of homepage content reveals a purposeful framing of blockchain as a breakthrough technology. The developers clearly use the hype surrounding blockchain as a revolutionary technology to their advantage and frame their platforms as such. For instance, Brave is "On a mission to fix the web" as the browser is touted as a "new way of thinking about how the web works" (Brave, 2019). Blockchain is central on the Oasis Labs' homepage and their performance is credited to "an entirely new blockchain architecture that separates computing from consensus, allowing computationally complex applications to run at scale" (Oasis Labs, 2019). Similarly, Civic boasts a "decentralized architecture with the blockchain" as the basis for their ground-breaking Secure Identity Platform (Civic, 2019). Each homepage presents an enticing solution to the problems users face when interacting with an increasingly commercialized digital space.

In addition, each platform places the responsibility of change in the hands of the user, as if by downloading or purchasing the application, the user is participating in democratic activism. For instance, Brave offers their platform as a solution to being treated like a "product" and asks users to "Help us fix browsing together" (Brave, 2019). By emphasizing user power, these blockchain platforms are perhaps creating an environment of pseudo data activism. According to Fuchs (2010), data activism is the use of digital technology to communicate or foster social change. For instance, open data movements foster social change by allowing citizens to access data held by the

government or other institutions, creating a more transparent and accessible digital space. While blockchain privacy platforms aim to reposition online power structures, for Fuchs (2010), the key to digital activism is self-organization, citizen-control and non-commercial activity.

While blockchain privacy platforms may have activist roots, their profitability negates a grassroots ethos. For instance, Dawn Song, professor at the University of California Berkeley and creator and CEO of Oasis Labs has been reimagining the digital space since her time as an undergraduate student and is oft-considered a privacy advocate. Nevertheless, Oasis Labs is a lucrative business venture, rather than a platform for activism. The company has received approximately $45 million in funding as of 2018 (Takahashi, 2018). Data activism as a marketing technique is a relatively new phenomena, reminiscent of green marketing which promotes sustainable and environmentally friendly strategies such as a minimal environmental impact in the creation, production or consumption of a product (Roy, 2018). Green marketing both projects ethical business practices while appealing to environmentally conscious shoppers. Data activism falls into the general realm of social activism marketing or corporate social responsibility (CSR). These tactics aim to foster trust and transparency between the organization, its shareholders, employees and customers. While CSR can result in a more socially responsible organization, critics say this approach profits off of social justice. For instance, closely tied to green marketing is the notion of greenwashing, when organizations exaggerate or make false claims regarding the environmental benefits of their product (Whellams, 2018). Similarly, openwashing is the digital version of this practice wherein organizations spin a product or company as open-source or open-license for marketing purposes when this is a false or exaggerated claim (Openwashing.org). It is not to say that these blockchain privacy platforms are indeed practicing openwashing, or presenting data activism as a marketing tool, but a simple overview of the homepage of each platform demonstrates a purposeful orientation of the user as a source of power in the reimagination of the Internet.

The discourse analysis revealed five broad themes: usability, cost, rewards, open-source and privacy. I will begin this exploration by briefly outlining the first four themes unrelated to privacy, and then provide an in-depth analysis of privacy and its five sub themes which include ad-blocking, general privacy, data ownership, decentralization and safety and security.

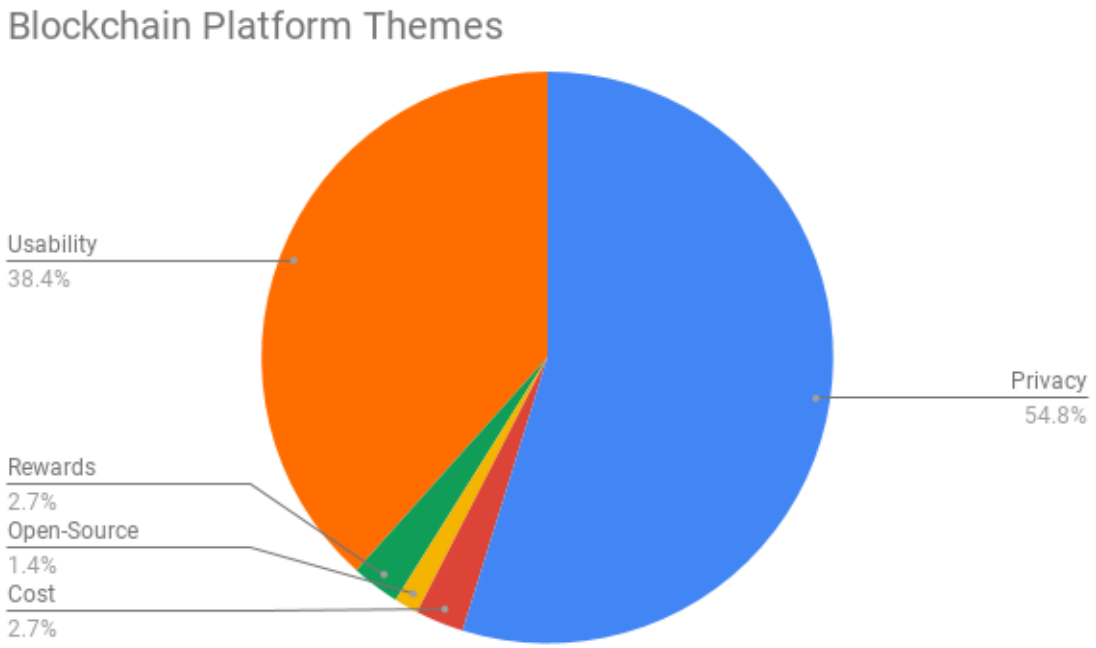

Figure 5. Blockchain Platform Broad Themes

Usability

Usability was a significant theme on each platform and accounted for 38% of coded content. Usability was coded 13 times on Oasis Labs, 11 times on Brave and 4 times on Civic. This theme included content on user experience such as ease of use, speed, practicality, compatibility and customization. Each platform emphasized usability, perhaps to ease anxieties of navigating a new technology and make it more accessible for the everyday Internet user. New technology adoption is a significant area of study and scholars have outlined the importance of usability in persuading users to work with nascent technology. A well-known model for assessing the uptake of a new technology is Everett Rogers' (2003) diffusion of innovations model. This theory outlines a multi-step diffusion process that takes into account conditions that increase or decrease the adoption of innovative products, services or ideas. Rogers acknowledges that all innovations carry a degree of uncertainty, but if the innovation has a degree of relative advantage during a trial period, then it is more likely to be adopted. Similarly, Davis (1986) in his empirical study on the acceptance of computers, saw that potential adopters must recognize a perceived usefulness and perceived ease of use for adoption

to be successful. These two factors are key determinants to the adoption of new technologies and provide practical guidance for developers hoping to share technological innovations to the general population. In the case of the blockchain privacy platforms, usability was touted through phrases such as “Simple, right?” and “Security meets simplicity” in the case of Brave, “Flexible and easy-to-use” on Oasis Labs and “accessible and on-demand solution” on Civic. (Brave, 2019; Oasis Labs, 2019; Civic, 2019). Civic frames their platform as a simpler, more streamlined alternative to traditional secure identity platforms: “Authenticate without the need for traditional physical IDs, knowledge-based authentication, username/password, and two-factor hardware tokens” (Civic, 2019). The motivation behind promoting the usability of each platform is likely to broaden interest from privacy and technology enthusiasts, to a wider range of users.

Cost, Rewards and Open-Source

I coded cost twice, making it only 3% of coded content. Both Brave and Civic offered their platform as a cost-saving solution. For Brave, users save money by switching to the ad-free platform as it negates the unwanted data charges that come with downloadable advertisements. On the homepage, Brave claims the platform can save users approximately $276 a year in unwanted data charges. On the other hand, Civic frames its platform as cost-saving because users work with a public blockchain rather than proprietary software.

Blockchain platforms as an open-source solution was explicitly mentioned once on Brave. While this is not openwashing, as the public blockchain is indeed open-source, the concept of open-source remains a buzzword in the realm of software development and data activism. Similar to cryptocurrency and blockchain, the values ingrained in open-source software have evolved into its own digital ideology. For developers, the motivation behind developing open-source software can be altruistic, ethical or political, or purely for fun (Giuri, Rochetti and Torristi, 2002). Additionally, according to Raymond (2002), there exists a “very zealous and very anti-commercial” facet to the open-source community which, like blockchain, promotes user rights over commercial gain (As cited in Giuri, Rochetti and Torristi, 2002). While the ideology behind-open source is user-oriented, it should be known that not all open-source

software is free. In the same vein as “free” social media, wherein the payment is user data, using open-source software can bear a cost. In the case of Brave, there is no upfront monetary cost to use these platforms, but open-source business models can still make a profit. For instance, Brave offers its users the opportunity to earn rewards, in the form of exclusive cryptocurrency - Basic Attention Tokens (BAT) - to view advertisements. By partnering with advertising networks Brave splits advertising revenue between users and publishers, while maintaining a portion itself (Finley, 2019). Because the majority of online platforms are free, Brave has oriented their cost saving in terms of data charges.

To Brave, the “new Internet” is one in which personal data is kept private, but also, where users are rewarded for watching advertisements. Brave is the only platform that features a reward system based on cryptocurrency called the Basic Attention Token or, BAT. By downloading Brave, users are choosing to participate in a space of digital democracy and can be rewarded for this. Additionally, users can tip content creators with BAT. This system is framed as a reimagination of the current Internet architecture, a solution that values the user rather than the advertiser. The rewards system falls in line with Brave’s ethos of user-control and their attempt at “fixing” the current state of the Internet.

5.3. Blockchain Platforms and Privacy Themes

There are five privacy subthemes in this content analysis of blockchain privacy platforms: safety and security (68%), decentralization (10%), data ownership (10%), general privacy (8%) and ad-blocking (5%). This section provides a description of each privacy theme and analyzes the content that constitutes each. These themes provide a deeper understanding of how privacy is framed on the homepage and features pages of each blockchain privacy platform. This is a crucial step in discovering the relationship between users’ construction of privacy and blockchain platforms’ constructions of privacy. There were 73 items of content coded on either the homepage or the features page of Brave, Civic and Oasis Labs. Of these 73 items, 40 related to privacy, or 55% of the coded content.

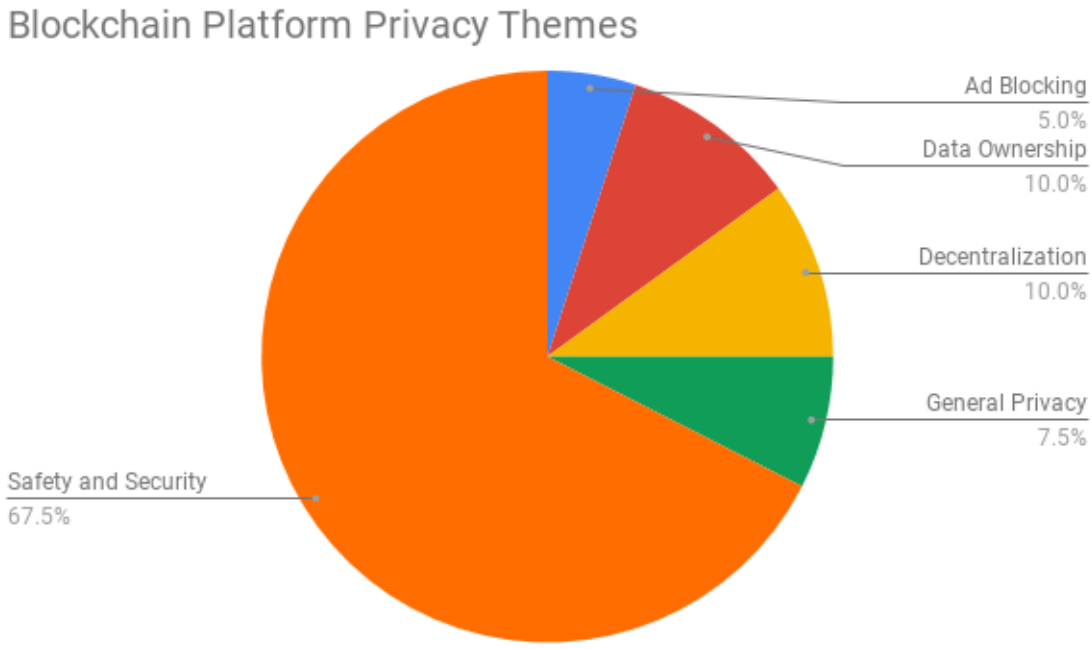

Figure 6. Blockchain Platform Privacy Themes

Safety and Security

This was the most significant privacy theme and was coded 27 times (68%): four times on Brave, 16 on Civic and six on Oasis Labs. While the terms privacy and security may seem synonymous, there is a distinction. The term cybersecurity was made popular after President Barack Obama used the term in a 2009 press release to recognize the importance of data security in overall national security (Schatz, Bashroush & Wall, 2017). Generally, cybersecurity is protection from malicious data breaches by state actors, non-state actors and hackers (Buchan, 2018). Like privacy, the definition of cybersecurity is inconsistent, particularly in industry and policy settings. To the general public, browsing securely means having little to no risk of personal data breaches such as a hijacked social security number, bank account data, credit card information or social media accounts. According to Pew Research Centre, 21% of adults have had their email or social media account hacked while 11% have had vital information, like social security numbers, stolen (Rainie, Kiesler, Kang & Madden, 2013). In an attempt to amalgamate an improved definition of cybersecurity based on a literature review of authoritative sources, Schatz, Bashroush and Wall (2017) concluded that cybersecurity is:

> The approach and actions associated with security risk management processes followed by organizations and states to protect confidentiality, integrity and availability of data and assets used in cyber space. The concept includes guidelines, policies and collections of safeguards, technologies, tools and training to provide the best protection for the state of the cyber environment and its users (Schatz, Bashroush & Wall, 2017, p. 66).

Through my discourse analysis I found the concept of cybersecurity framed by blockchain privacy platforms fell in line with this general definition, particularly the protection and confidentiality of personal data. For instance, for Brave, safety and security is a "top priority" and by choosing Brave, users are browsing "safer" and experiencing "unparalleled privacy and security." To maintain user security, Brave "fights malware and prevents tracking, keeping your information safe and secure" (Brave, 2019). Security measures listed on the features page include: built-in password management, form autofill control, clear browsing data, among others. Moving to Civic, the platform uses the increasing instance of identity theft and data breaches as rationale for using their secure identity platform, which is their primary feature. Security is a lead selling point for Civic and was coded for 16 times on either the homepage or the features page. Along with features such as decentralization, encryption and multi-factor authentication, Civic reassures users that "Civic never stores member data" and "Civic cannot be compelled by a foreign government or criminal organization to invalidate identity data" (Civic, 2019).

Oasis Labs on the other hand, takes a more technical approach when championing their security features, owing their safety and security to "secure enclaves and zero-knowledge proofs," "multi-party computation" and "confidentiality frameworks" (Oasis Labs, 2019). Oasis Labs differs from Brave and Civic in that what it deems "flexible and easy-to-use" is directed towards a technically savvy audience, such as developers, rather than everyday users. For instance, the language used to describe their security measures is much more technical: "secure enclaves, secure multi-party computation and zero-knowledge proofs" (Oasis Labs, 2019).

Data Ownership

Data ownership is a significant part of overall privacy, as noted by Cavoukian & Tapscott 1995; Petrie, 2016; Scassa, 2018, among others. Defined by *The Economist* as

the “new oil,” data is a lucrative resource for major corporations, marketing companies, government institutions and more (The Economist, 2017). According to Scassa (2018), data is frequently characterized as the answer to society’s problems. In this context, debates over who controls and owns data have become critical and more frequent in both legal and public arenas. Data and privacy intersect when we consider who owns data, who has the right to user data, and how users can control their own data. For the most part, it is major corporations, such as Facebook, Amazon and Google that reap the benefits of this new resource, as they can now expertly market to consumers based on their online activities. Scassa (2018) seeks a balance between public and private data rights so users can maintain control over their private information while organizations can use big data to spur innovation and further societal knowledge. One way in which users can regain control over their personal data is through these blockchain platforms, as all three acknowledge the importance of user control over data. The theme data ownership was coded four times: two times on Civic, and once on both Brave and Oasis Labs. Both Civic and Oasis Labs stress the importance of control when framing data ownership. Civic is “giving businesses and individuals the tools to control and protect identities” while Oasis Labs strives for the balance proposed by Scassa (2018):

> We’re creating a system that gives the best of both worlds. It can address the problem of data siloes by enabling data sets to be easily used while still protecting user data and ensuring it remains in control of the user (Oasis Labs, 2019).

This too reaffirms the previous verdict that Oasis Labs is directed towards a technically savvy user group or organization, one that would benefit from accessing user data sets. Brave also extends the concept of user control as it states, “Our servers neither see nor store your browsing data - it stays private, on your devices, until you delete it” (Brave, 2019). User control is part of the overall ethos of blockchain and platforms are maintaining this to differentiate themselves from mainstream platforms.

Decentralization

I coded decentralization four times: twice on Civic and twice on Oasis Labs. Decentralization is an interesting theme, as it is especially applicable to blockchain technology. While other themes directly relate to online privacy, decentralization does not have a clear connection to privacy unless you are familiar with the affordances of a

decentralized Internet architecture or blockchain technology. Particularly for platforms operating on blockchain, decentralization not only strengthens privacy, but maintains security and prevents hacking and other clandestine activity. Whereas centralized structures are controlled by a single party, blockchain platforms operate without intermediaries, storing data in blocks that are distributed and verified by a peer-to-peer network. Civic mentions decentralization in conjunction with blockchain by introducing their verified identity system as a "distributed solution" through a "decentralized architecture with the blockchain" (Civic, 2019). On the other hand, Oasis Labs does not mention decentralization specifically, rather, uses the phrases "trustless privacy" when promoting their decentralized architecture. In this context, trustless privacy can be equated to decentralization as it infers the absence of intermediaries in favour of the "trust machine," or the distributed nature of blockchain technology (The Economist, 2015).

Ad-Blocking, General Privacy

Ad-blocking was a small theme exclusive to Brave and was coded for two times. Brave differentiates itself from traditional ad blockers by "block[ing] unwanted content by default" rather than through a secondary application such as Ad-Blocker on Chrome. Along with ad-blocking, Brave lists additional shields on its features page such as block scripts, cookie control and per-site shield settings. Again, Brave separates itself from "popular sites" and positions the browser as an empowering alternative to the status quo.

The theme general privacy encompasses the content that related to privacy but did not fit into the established subthemes. For instance, the introduction of Brave platform as "built by a team of privacy focused, performance-oriented pioneers of the web" includes privacy yet doesn't point to a direct theme. Similarly, the general introduction to Oasis Labs was coded as general privacy: "Unlock the potential of your data without compromising security or privacy" (Oasis Labs, 2019). These general statements serve as an introductory header to the rest of the content on the homepages of Brave and Oasis Labs.

5.4. Conclusion

This section unpacks how blockchain privacy platforms understand and promote privacy on their homepage and features page. The discourse analysis methodology proved effective in grouping similar conceptions of privacy into five pertinent themes: Safety and Security, Data Ownership, Decentralization, Ad Blocking and General Privacy. These themes provide insight into what privacy means to blockchain privacy platforms and how these ideas are then communicated to users. For instance, according to this coding process, safety and security is a primary facet of privacy in that it protects users from data breaches and other malicious activity. It is significant too, that each blockchain platform is relatively similar in their conceptions of privacy as there was no disparate content between the three platforms. Not only was safety and security the most popular theme for each platform, but all three platforms mentioned data ownership as an important feature of overall privacy. Other than ad-blocking and open-source as exclusive to Brave, there was a general cohesiveness between the three platforms. This is significant considering how notoriously difficult privacy is to define. In the introduction of this project, I mention the abstract nature of privacy; it maintains a legal definition, but the individual concepts of privacy can fluctuate depending on the person, the context and environment. While scholars acknowledge the difficulty in defining privacy, the consensus between blockchain platforms perhaps points to a more universal understanding than was previously considered (Powers, 1996; Lane, 2009; Craig & Ludloff, 2011; Gellman and Dixon, 2011). This means that developers assume potential users conceptualize privacy in a similar way as well. These findings fall in line with Newell's cross-cultural comparison of definitions of privacy. While Newell studied pre-Internet privacy, she found significant commonalities in conceptions of privacy between three distinct cultures and understood privacy to be a universal desire (Newell, 1996). By examining user conceptions of online privacy, we will discover whether blockchain privacy platforms are correct in their assumptions about how users consider online privacy, or if these two rationales are disconnected.

Chapter 6. Reddit and Medium

6.1. Introduction

In this section, I compare how blockchain privacy platforms frame online privacy, to conceptions of privacy discussed by social agents on Reddit and Medium. I begin by providing background on the social agents in question. Next, I explain the significance of using Reddit and Medium as a source of study. Following, I delve into the findings of my discourse analysis and explore themes of privacy shared by Reddit and Medium users. By comparing themes of privacy between platforms and social agents, we have further insight into a comprehensive definition and understanding of online privacy in the face of emerging technology. Additionally, this comparison outlines affordances and constraints of these blockchain platforms according to this sample of users. Users on Reddit and Medium are critical in their examination of these platforms and identify technical gaps and practical concerns. Further, according to SCOT, this user feedback aids in the construction and reimagination of the technology, particularly during the innovation phase as developers attempt to solve the quandaries brought up by social agents.

6.2. Reddit and Medium Platforms

The motivation behind coding content on Reddit and Medium was twofold. First, both Reddit and Medium host active technology communities. Particularly, on Reddit, privacy-related subreddits welcomed participation and featured discussion with many voices and different points of view. Medium too welcomed product reviews and opinion pieces on the topic of new technology. Second, Reddit and Medium users can be characterized as innovators - those typically ahead of the curve in the area of new technology and innovative projects. They are open-minded and take pride in finding the next breakthrough technology product or service. In addition, the participatory and democratic nature of Reddit makes it a valuable site for qualitative research. Massanari (2015) characterizes Reddit as a “unique, boundary-spanning platform that elicits new questions about the nature of participatory culture and community in the age of social networking” (p. 7). Users participate on Reddit to socialize, for entertainment or to seek

out information. Especially when information seeking, the Reddit community works to "break down barriers between expert and novice" due to a lack of intermediaries, making conversation "more democratic, more authentic and more deliberate" (p. 9).

Much of the content I analyzed was information-seeking. Users posed questions on the affordances of particular blockchain platforms or sought recommendations on which platform is the best for private browsing. For instance, in the subreddit r/privacy, user Veritasmaximuss asks: "Is Tor on the Brave browser legit?" (2019). The following discussion thread exemplifies the blurred lines between expert and novice. Due to the anonymous nature of the platform, it is difficult to decipher whether or not a user is in fact an "expert." However, users that are deemed experts, either by themselves or members of the subreddit communicate with an air of confidence and authority. For instance, in response to Veritasmaximuss, user MercuryWhiskey (2019) answers with a definitive "Yup" followed by a short explanation of Tor's configuration on Brave. Moriarty and Mehlenbacher (2019) assessed how Reddit users evaluate experts on the subreddit r/science, a primarily information-seeking community, and found Reddit users adopt a simple ethos-assessment heuristics to judge the trustworthiness and credibility of users. This assessment is based on an aggregate of information about the "expert" such as the use of hyperlinks, adherence to discursive norms, post points and karma scores. This information offers a picture of "ethotic qualities" including "credibility, reputation and trustworthiness that allows Redditors to use shortcuts to validate both epistemic and social trust" (p. 515). Similarly, Record, Silberman, Santiago and Ham (2018) found Reddit users are open to different perspectives when actively seeking information, demonstrating a level of trust in the information provided. Additionally, users will often try to enact the information found, despite engaging in minimal source credibility checking. This level of trust is seen in Veritasmaximuss's sincere response: "Ok thank you for the insight. Much appreciated" (2019).

While Medium does not herald such a high interest by scholars, it is an important community of technologically savvy individuals motivated to share their thoughts on emerging and disruptive technology. Like Reddit, posts on Medium are organized according to themes such as OneZero (technology and science), Gen (politics and culture), and Hackernoon (AI and crypto). As mentioned in Chapter three, at the time of this study Hackernoon was affiliated with Medium, but it is now its own independent platform. While there is no scholarship on the nature and behaviour of Medium users,

the website provides its selection criteria for the articles that get published on the platform. According to Medium, articles are written by “writers, journalists and experts” that “educate, inspire and move understanding forward” (2019). While users must create a profile that includes a full name, a clear photo and a short biography outlining a user’s credentials, users do not have to have any particular qualifications to publish. Users can self-identify as a writer and have their content posted on Medium. However, unlike Reddit, Medium requires citations when discussing facts, including quotations and excerpts. The views expressed on blockchain privacy platforms on Medium are pertinent as they elucidate privacy ideals held by potential early adopters. Hackernoon describes their demographic as “technophiles,” 48% of which are between 25-34 years old, with 62% residing in the United States. David Smooke, Hackernoon COO categorizes their contributions into three lanes of interest, the primary one being blockchain, bitcoin and cryptocurrency (Hackernoon, 2020).

In addition, while content on blockchain privacy platforms was relatively neutral informational or promotional material, there were a variety of conversational tones noted on Reddit including argumentative, skeptical, hopeful and optimistic. Often discourse was casual, yet Reddit “experts” tended to use a higher degree of formatting and correct grammar, punctuation and sentence structure than non-experts. For instance, a Reddit user reached out to members of the subreddit r/privacy with the following question:

> Can someone plz help me understand this? Everyone just keeps saying ‘Brave isn't FireFox’ and ‘At least FireFox isn't Chromium’ but BRAVE isn't just any other Chromium fork. Is Brave the future of Private Web Browsing? (u/OverallGain, 2019).

Note, the use of shorthand “plz” and the overall casual tone. Compare this question to the response by a Reddit “expert.”

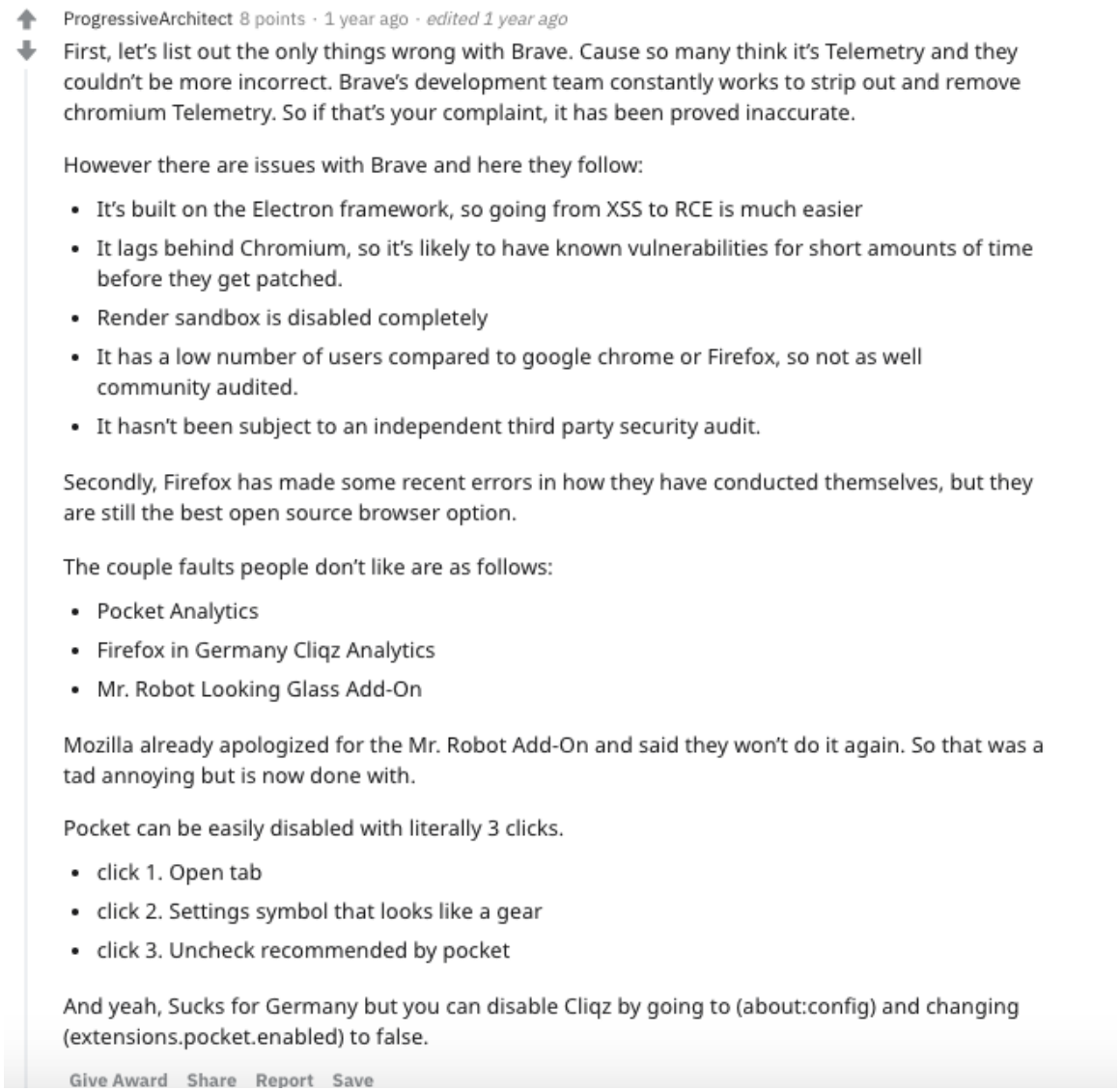

Figure 7. u/ProgressiveArchitect, 2019

Note the format, length of the response, and authoritative tone. Definitive phrases such as “they couldn’t be more incorrect,” “it has been proved inaccurate” and “they are still the best open source browser” denote the user’s authority. Additionally, this was the top-rated comment in the thread, which, according to Moriarty and Mehlenbacher (2019), reinforces trust through ethos-assessment heuristics. On the other hand, contributors to Medium must follow editorial guidelines, making the discourse more formal and similar to content on traditional platforms that feature UGC such as *The Huffington Post* and *Mashable.*

6.3. Privacy Themes

Now that I have provided the context surrounding privacy discourse on Reddit and Medium, this section will work to unpack these themes and compare them to notions of privacy presented on blockchain privacy platforms. Conversations regarding blockchain platforms and privacy fell into five themes: ethics and trust (38%), safety and security (34%), general privacy (12%), ad-blocking (9%) and data ownership (7%). First, I will compare similarities between blockchain platforms and UGC platforms, followed by an analysis of disparate themes. The theme of general privacy will not be discussed at length as it encompasses the miscellaneous content that mentioned privacy in a general way, without pointing to a specific theme.

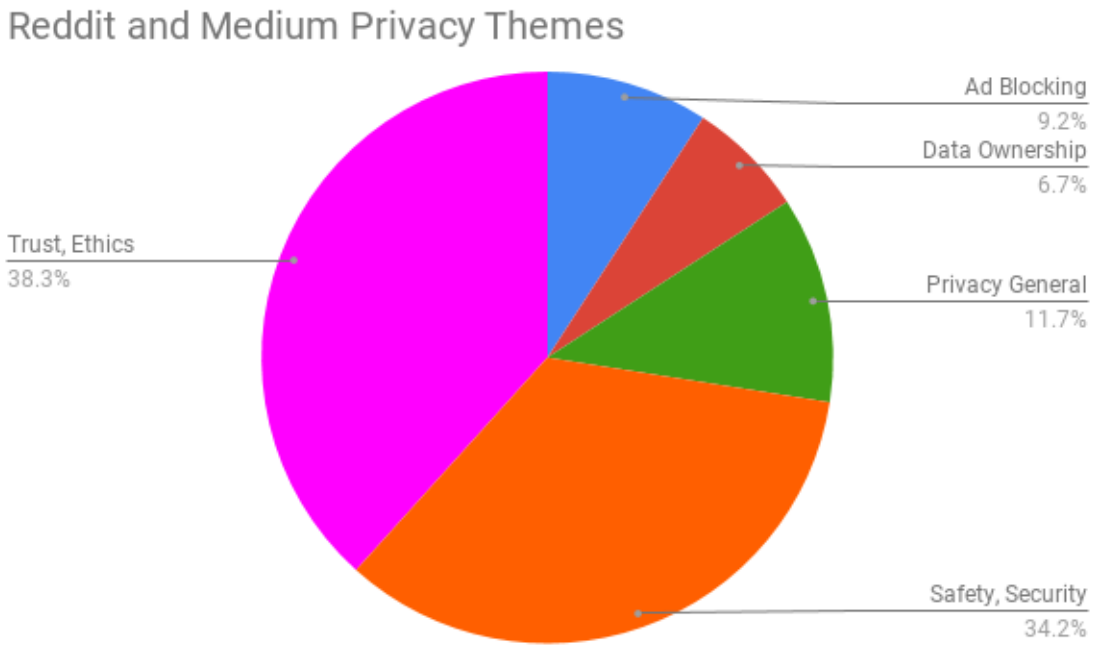

Figure 8. Reddit and Medium Privacy Themes

Safety and Security

This theme was significant for both blockchain platforms and its users and made up 38% of coded content on Reddit and Medium. Safety and security was mentioned 41 times by social agents in conjunction with all three blockchain privacy platforms. Similar to the way blockchain privacy platforms characterized safety and security, social agents

associate security with protection from malicious hackers, secure identity storage, prevention of data leaks and overall confidentiality. Overall, the content in this section was almost all positive, save for one comment that compared Civic's identity model with pre-existing centralized models. In a Medium article outlining key trends in the blockchain space, user Torque (2018) suggests:

> Civic still relies on traditional identification methods that are not particularly customizable or flexible. This still means that individuals may have to give up more personal information than necessary, and will still need to manage multiple identities" (p. 5).

Other than Torque's (2018) comment, all other mentions of safety and security in regard to blockchain platforms are positive and generally praise the platforms' efforts to protect user privacy. For instance, in a post titled "Why I believe Civic will not succeed" that characterizes Civic as unimaginative and akin to Facebook's established identity management feature, user chongkwongsheng defends Civic:

> I don't think you understand how Civic works or (at least tries to) solves the problem of identity theft. Facebook is centralised and can't scale validation of all sorts of information like your government licenses nor do can your [sic] trust them to store that information (chongkwongsheng, 2019).

Likewise, Medium user Devin Soni (2018), introduces Civic as a solution to centralized data storage: "Luckily, new decentralized services like Civic aim to fix the current issues facing identity security using biometric verification and blockchain technology" (para. 2).

Users also understand the significance of blockchain technology when it comes to maintaining data security. Reddit user AI-girl (2019) explains: "This is why companies like civic are using Blockchain; because you can secure personal identity data." Likewise, Medium user Anonymous Ledger (2018) explains how Oasis Lab uses blockchain to effectively maintain data security in smart contracts: "Blockchains and trusted enclaves have complementary security properties that can be combined effectively to provide a powerful, generic platform for confidentiality-preserving smart contracts" (p. 1). When discussing the security features of these blockchain privacy platforms, users are generally enthusiastic and hopeful that the technology will help users reinstate data privacy and overall security.

Ad-Blocking

Brave is the only platform that promotes an ad-blocking feature explicitly and this theme was mentioned in conjunction with Brave. Brave places ad-blocking as a high priority while Civic and Oasis Labs focus on identity management and data ownership. Ad-blocking was coded for 11 times and made up 9% of privacy content on UGC platforms. The majority of comments regarding Brave and ad-blocking were made on Reddit and were defensive, with users refuting misinformation and untrue claims made by other users. For instance, a post titled “Brave Privacy Browser is Whitelisting Trackers of Facebook and Twitter,” which was subsequently flagged by moderators for containing a misleading title, created a stir among the Reddit privacy community. So much so that amongst the discussion, a Brave representative made himself/herself known in the comment thread in an attempt to clear up any misconceptions. User brave_w0ts0n (2019) addresses the subject of the post and offers an explanation of how Brave uses Chromium software without Google’s tracking technology.

> It's understandable, the title was quite misleading, I don't blame you. As I mentioned before, I run the Ops team at Brave, lots of server and infrastructure related stuff so I can only speak from my perspective. As you mentioned Chromium is open source. So first thing we at Brave did was remove any and all calls back to Google and Google servers (brave_w0ts0n, 2019).

Users unaffiliated with Brave came to the platform’s defense as well. In response to user Lalade’s (2019) comment “hard pass”, user bbondy (2019) states: “But it needs to be understood that Brave has no need to dance with advertisers since its business model and funding does not come from advertising companies.” ThriceHawk (2019) argues that Reddit users, particularly those who support Firefox “unjustly talk down on Brave” and fellow privacy enthusiasts “don’t need to tear down one in support of the other.

> Brave is simply trying to provide a browser that natively blocks trackers/malicious ads while simultaneously revamping our current broken advertising model that sees Google profiting off our data (ThriceHawk, 2019).

Opinions shared on Medium regarding Brave’s ad-blocking potential were positive or neutral. Medium writer Charles Bordet (2019) is complimentary towards

Brave's ad-blocking: "The default reply on Brave browser is No. I prefer this behavior. And I still have the choice to turn it on." Medium writer Gokul N K (2018) shares the same appreciation for default ad-blocking: "Now that brave has an alternative revenue model I think we can safely start using 'Disable ads and trackers.'

By analyzing the robust discourse surrounding ad-blocking, it shows that overall, users are in favour of ad-blocking as a feature of overall online privacy. Most users are enthusiastic about ad-blocking by default, but some users remain skeptical of the ad-blocking model and are hesitant to trust Brave altogether. For instance, user imillonario (2019) says: "Not sure if trustworthy or not but I use it haha.... I like what they are doing with the ad blocker, tracker blocker, and https auto upgrades and that's why I use it...." While platform developers and social agents may agree on the value of ad-blocking for overall privacy, themes of trust become readily apparent throughout this content analysis and will be further explored in upcoming sections.

Data Ownership

Social agents discussed data ownership in conjunction with all three blockchain platforms with 8 comments coded (7%). While ad-blocking saw conflicting ideas regarding the legitimacy of Brave's ad-blocking claims, the discourse on data ownership was rather homogenous. Social agents acknowledged the importance of data ownership to overall privacy protection and responded well to this ethos held by blockchain platforms. For instance, Medium user Brandon Goldman (2018), applauds Brave's initiative to remove middlemen that can access user data and associates this with overall privacy: "Your browsing history can be kept private, as all data required for ad-matching never leaves your device" (Goldman, 2018, para 3). Similarly, Medium user Henk van Cann (2017) equates Civic's secure identity platform with self-sovereignty: "Civic has the ambition to become the world's ecosystem for self sovereignty in identity provisioning" (para. 2). In content related to Oasis Labs, we see a shift in audience focus from individual users, to business. In a Medium article by user Primei.co (2018), Oasis Labs is discussed as a solution for performing data analytics without disclosing sensitive data. This is important "since users are more and more aware of the exploitation of their data by large centralized companies" (para. 1). In doing so, Oasis Labs "has the objective to preserve privacy while executing smart contracts" (para. 1).

On Reddit too, users commended this ethos of user control. Again, in an effort to defend Brave user 0gicbea writes:

> Brave does NOT collect, monitor, or store user data. Period. Additionally, if you bothered to scroll down the page a little further, you would've read the portion where they explicitly state that user data does NOT leave their device even if they are opted in to the program (0gicbea, 2019).

Another defensive comment comes from the thread titled “Why I believe Civic will not succeed.” User RobertBartus (2019) attempts to iterate the benefits of Civic for secure identity protection and data ownership:

> Civic is your (secure) identity. Imagine having your ID, passport, health record, credit score etc. in one place, and you do not hustle when you need to prove something. CIVIC is instead of usernames and passwords and filling registration fields, CIVIC is instead of sending picture of your passport and electricity bill no older than 3 months to prove who are you. Civic is going to take down the unethical companies that buy and sell all of our personal information (RobertBartus, 2019).

Reddit users who support a particular platform are often vocal. It is common to see defensive explanations that attempt to convince other users of the benefits of using a blockchain platform for security, data ownership and overall privacy. This theme exemplifies that users are passionate about data sovereignty and their ethos are in line with what blockchain privacy platforms are presenting to users. When discussing data ownership, users typically trust these platforms to provide users with more control of their data, and by doing so, are helping to reimagine the Internet’s current centralized framework.

Ethics and Trust

This data set was coded inductively without the use of a predetermined coding scheme. For this reason, this theme was unexpected, yet critical. While the themes expressed by social agents are relatively comparable to those presented by blockchain privacy platforms, ethics and trust is exclusive to social agents. This theme encompasses discourse on the trustworthiness of blockchain privacy platforms and the developers behind the platform. Additionally, the ethics of developers and creators are

called into question. This theme yielded 47 coded items, or 38% of all content, which is the largest theme.

In the famous “Trust Machine” article by the *Economist* (2015) *blockchain* is described as “a machine for creating trust,” a technology that “lets people who have no particular confidence in each other collaborate without having to go through a neutral central authority” (p. 1). Since its early inception, the narrative of blockchain as a trust machine has remained. For instance, in a 2019 systematic review of blockchain business literature, “trust, security and transparency” was the second most salient definition of blockchain after “distributed or decentralized ledger” (Frizzo-Barker et al., 2019, p. 7). This clear association may lead us to believe that blockchain platforms yield a similar image of transparency and trustworthiness. However, for Reddit users in particular this is not the case. While users are overall enthusiastic about blockchain for privacy, they are extremely critical in their evaluation, too. Throughout this content analysis, blockchain remains a trustworthy technology, but users are not so quick to trust the developers behind the platforms. There were a number of subcategories within this theme, which included distrust in individual developers, the ethos of the platforms, or the technology behind the platforms. Not all discourse regarding trust was negative and some users discussed blockchain privacy platforms in a positive light in relation to trust and ethics.

Brendan Eich, co-founder of Brave, bore the brunt of user criticism, particularly on Reddit. As the co-founder of Mozilla and creator of JavaScript, Brendan Eich is well known in the software community. Despite his experience in the industry, social agents are skeptical. For instance, in a discussion comparing Brave’s data privacy to Firefox, Reddit user Tyler1492 shares the opinion that Brave Eich only created Brave because he lost his job at Mozilla. In response, user meltingspark (2019) comments: “He was CEO of Mozilla for a whopping 11 days before he stepped down. The whole story on why he actually stepped down is a little controversial but there is no doubt he had no choice essentially.” Reddit user atoponce (2019) blames Brave’s “shady” business practices on Eich, stating:

> Brandon Eich claims that most of its collected revenue goes to the online publishers, but this is the same deceptive practice that Adblock Plus executes, and one of the many reasons why uBlock Origin is the preferred ad blocker these days (2019).

Further harsh words were said by sapphirefragment in regard to Brave and its co-founder: “brave browser is cryptocoin-crank snake oil and this should be surprising to nobody also brendan eich is a loser” (sapphirefragment, 2019).

Not all sentiments on Eich were unfavourable. One social agent, while deliberating the effectiveness of Brave in protecting privacy, stated that Eich’s hand in the creation of Brave brought a sense of comfort because Eich’s previous mission with Mozilla was to create an open and private browser. However, in response to this, user RoseTheFlower condemns Eich for his opposition to same-sex marriage:

> Maybe so, but I have no desire to support a company that is run by a man that opposes equal rights. One could argue it has nothing to do with privacy, but it always takes the same kind of person to want more control over others and their lives (RoseTheFlower, 2019).

Eich’s opposition to same-sex marriage is well-known and was reported by numerous news outlets including the Guardian and BBC. On Eich’s Wikipedia page the “known for” heading reads: “JavaScript, opposition to same-sex marriage” (Wikipedia, 2019). When it comes to evaluating the browser, user RosetheFlower cannot separate the creator from his personal values. This is not an issue exclusive to the software community, and consumers often grapple with how to separate an individual from their work and personal ethos, if they should at all. Becker, Einwiller and Medjedovic (2014) outline the importance of a CEOs personality and reputation to the overall assessment of an organization. They found a company’s figurehead to be closely tied to the corporate brand and its reputation, using Steve Jobs and Apple as an example of this symbiosis. Fetscherin (2015) found that a CEO’s overall persona, education and physical appearance impact a company, and particular traits, such as Machiavellianism, can negatively affect a company’s bottom line. This is evident as controversial CEOs that participate in alienating behaviour often step down from the position or are let go. Interestingly enough, Eich did in fact step down as CEO of Mozilla because of the controversy surrounding his views on same-sex marriage. According to Mozilla Executive Chairwoman, Mitchell Baker, Eich’s personal beliefs were incongruent with the diverse and inclusive culture of Mozilla (2014).

On the other hand, leaders with a positive reputation bode well in the face of critical evaluations of their organization. The leadership team behind Oasis Labs is the antithesis of Eich. Throughout the discourse analysis, all comments on the Oasis Labs' leadership team were positive, and even solidified trust between social agents and the platform. In a Reddit thread comparing Oasis Labs to Enigma, user Lifeofahero (2019) sides with Oasis Labs because it has a "stronger technical team." Lifeofahero even urges users choosing between the two platforms to compare biographies between Oasis Labs and Enigma, as the Oasis Lab team hosts a superior leadership team. Similarly, Medium user ICOgens (2018) writes the Oasis team excels at "designing products and management" and has "a plethora of industry experience and most related background" (sec. 6). In another evaluation by Medium user Primei.co (2018) characterizes the leadership team as: "world class researchers and serial entrepreneurs with a solid track record" (sec. 2). Particularly with innovation platforms that are attempting to break into the mainstream, reputation is critical in moving an organization forward and creating trust with social agents.

Additional findings in this theme reveal a deep distrust of Chromium, the open-source software that undergirds Brave. Numerous Reddit users expressed their aversion to Google-owned software, with some users choosing to pass on Brave altogether because of this. To social agents, Chromium represents the corporate, multinational, centralized institution that they are actively trying to avoid by moving to a privacy-focused platform. Reddit user meltingspark (2019) made the decision to use FireFox only because Brave is based on Chromium, stating: "the fact that every browser switching to the chromium build and leaving their own open source behind. I dunno...just dosn't [sic] sit well with me. I don't like that everything is sitting under one roof."

User blue_pill_90210 struggles with the idea of using Brave because "by using Chromium I am defacto backing Google - which I don't want to do" (2019). While some users express their indifference to Chromium, the majority of users that mention the software are vehemently opposed to supporting anything Google owned or related. One user chose Firefox over Brave simply because it's "not fucking chromium" (StraightChemical, 2019).

This theme exemplifies the high standard in which social agents hold to blockchain-based innovations for privacy, particularly in areas of trust and ethics.

Despite the work these blockchain privacy platforms put into the technology, usability and overall privacy preserving features, social agents consider trust in the platform and the leadership team to be critical in their decision to adopt the platform. Further, it is not safe to assume that because blockchain is characterized as a “trust machine” that platforms incorporating the technology will therefore be characterized as such.

6.4. Usability

While usability is not a privacy-related theme, I felt it important to discuss. The discourse analysis concluded that usability was a high priority for each blockchain privacy platform. The blockchain platforms framed their platforms as easy to use, intuitive, and user-friendly with phrases such as “security meets simplicity” and “a way to authenticate all our community members with ease” (Brave, 2019 & Civic, 2019). As we saw with the previous theme, just because a platform is framed in a particular way, does not mean this characterization will translate to users. Usability revealed disjointed perceptions of the framed usability versus the ease of use social agents experienced. This theme was coded for 65 times and some of this discourse expressed frustration or disappointment at the technical issues and usability issues users encountered. This is to be expected with beta versions; however, each platform specifically advertised the usability of their platforms. Moreover, during the early adoption phase, ease of use is crucial in retention and when branching out into the mainstream. When innovators and early adopters have a positive experience with an innovation, they are more likely to convince others to adopt the technology. Rogers (2003) characterizes this as the “persuasion stage” (p. 168). This is especially crucial in communities like Reddit and Medium because those interested in an innovation are more likely to seek information from peers. When individuals with similar values express positive evaluation of an innovation, their peers are more likely to adopt it.

Users anticipate minor technical errors when running beta versions of software, but for some, these glitches were too significant to ignore. User ethfiend2064 gave up on the Civic platform after a “pretty awful user experience” (Reddit, 2019). The user

lamented that the Civic registration is limited to mobile devices, which did not actually work:

> Tried scanning my id about 100 times and it always failed OCR. No help available in the app so I ended giving up. The experience felt like being trapped in an IVR voice system on the phone that never gives you the right options and you can´t get additional help (like when you just want to yell "O-P-E-R-A-T-O-R" into the phone" (ethfiend2064, 2019).

In another thread, Reddit user SquirtGunKelly1 blames Civic's user assistance inadequacies on the small team behind the software: "they may be bombarded with tasks and figuring out technology. In my opinion Civic is still a project that is 2-5 years down the road for full adoption" (SquirtGunKelly1, 2019). In response to SquirtGunKelly1, Reddit user PapaRostov8 compares 2-5 years to "20-50 years in crypto." In order to be relevant "Civic absolutely needs to demonstrate this [real life] adoption this year to stay ahead, otherwise investors will move to something else" (PapaRostov8, 2019).

Oasis Labs faced a common problem associated with blockchain technology - its interoperability. Despite the many advantages of using blockchain technology in new software development, interoperability has been a reported challenge. Zhang, White, Schmidt and Lenz (2017) in their analysis of interoperability in blockchain health platforms define it as "the ability for different information systems and software apps to communicate, exchange data and use the information that has been exchanged" (p.1). Blockchain is susceptible to problems in interoperability because there exist hundreds of distributed ledgers and they cannot always communicate with each other. For instance, there may be interoperability between a distributed ledger and legacy systems or interoperability between two distinct distributed ledger platforms such as Corda and Ethereum, a permissioned versus a permissionless ledger (Koens & Poll, 2019). Medium user Primei.co shares that Oasis Labs has received substantial criticism for its interoperability problems, despite the "obvious advantages of the technology" (Primei.co 2018).

The results of Brave's coded content revealed two juxtaposing ideas. First, social agents expressed their frustration at the myriad of technical issues they faced when using the platform. User blue_pill_90210 expresses: "Brave is the new kid on the block with some hiccups as it is just coming out of beta" (2019). The technically savvy users

pinpointed specific technologies that were underperforming such as telemetry, render sandbox and the auto-contribute function of BAT. Other users expressed more straightforward feedback in terms of its usability. In the subreddit r/privacy, a user asked the community if they recommended Brave, to which user ALLyourCRYPTO responded: “no. It still breaks more sites than it works on and it isn't blocking all the ads. Ublock and even ad block plus blocks more ads than this shit” (2019). In the same thread user MindlessComment responded: “Absolutely NOT, the browser uses so much disk space and overheats my computer, googled the problem and I saw that it was pretty common, might be a miner of some sort” (2019). In a post requesting information on the shortfalls of Brave, user lookatmegowee commented: “Brave on desktop is poo and has ugly way of rendering websites” (Reddit, 2019). However, what is interesting about the complaints surrounding Brave, is that users still recommend the platform to privacy novices but pass on the platform themselves. For instance, user lookatmegowee in the same thread states: “[Brave is] easy privacy for noobs who can't into technical privacy or are lazy. There are better alternatives if you can put in the effort.” (2019). In a post comparing Brave to Firefox, user norflowk suggest that Brave is easier to manage for the average Internet user.

> Truth be told, most people I know don't even bother going through their settings for fear of messing things up. Products made specifically for these people are important, as they are the majority and have the most influence over what comes to market (norflowk, 2019).

Similarly, user Szymas255 when asked if they would recommend Brave commented: “For someone who doesn't want to configure Firefox? Yes without a doubt” (2019). Interestingly enough, because privacy communities on Reddit are made up of users who have a keen interest on the subject, they are much more critical of platforms than the average user. What is acceptable to the average Internet user does not always meet the standard of those who are particularly technically savvy. For user Raphty101, Firefox is more privacy-focused than brave with “heavy modifications”; however, “when I have to choose what browser I recommend to my mom I would point her to brave 9/10 times” (2019).

Now, not all comments regarding the usability of these platforms expressed frustration about beta issues and technical problems. Out of the 65 coded comments, 29 of them discussed the usability of the platforms in a positive light. Overall, Medium users were far more positive in their reviews of each blockchain privacy platform compared to

Reddit users. Within this theme, only one Medium user criticized a blockchain privacy platform for its usability issues and beta problems. Medium user Charles Bordet (2019) was especially enthusiastic about the speed in which pages load on Brave: On average, they're 2x faster on desktop.. and EIGHT TIMES faster on mobile! That's HUGE!" (sec. 4). Medium user Gokul NK (2018) also compliments the speed of Brave as there was a noticeable difference compared to traditional browsers. Oasis Labs also received praise for its transaction speed, its compatibility with any blockchain and its ease of use for developers (Reddit, 2019; Medium, 2018). There was only one positive comment on Civic's usability, nevertheless, Medium user Devin Soni (2018) characterizes the platform as convenient and safe to use (sec. 4).

6.5. Problems and Solutions: Social Construction in Blockchain Privacy Platforms

This comparative discourse analysis explored the relationship between blockchain privacy platforms and social agents' conception of privacy. This investigation revealed instances of overlapping ideas as well as unexpected dissimilarities between blockchain privacy platforms and its users. By applying SCOT to these findings, we can better understand the importance of comparing these two groups as it can inform platforms on how to improve innovations to better represent conceptions of privacy determined by users.

From Pinch and Bijker (1985), we know that social groups aid in the development of innovations as they identify problems within the technology that can then be reimagined with the help of developers. Additionally, social agents can reaffirm decisions made by developers by demonstrating their agreement on particular features. For instance, this investigation revealed an agreement on ad-blocking as a feature of overall privacy protection. While this theme was exclusive to Brave, it showed that users generally accepted the way this feature was developed, save for the few users who expressed their distrust in the Brave business model. Inherent distrust in the motives of companies and the individuals behind them is a recurring sentiment throughout this discourse analysis and became a theme of its own. Additionally, both parties shared the data ownership theme, which revealed a shared ethos of user empowerment, and

decentralized control. This was the most homogenous theme throughout the content analysis and users appreciate this value that blockchain privacy platforms are built upon. Similarly, users expressed overall optimism in the platforms' ability to shield them from malicious activity. Users generally trust these platforms to protect their data from third parties and hackers, and the coded material revealed congruency in the importance of data security and overall safety as a feature of privacy.

Special attention should be paid to the themes where these two groups disagree. Incongruency in privacy ideas between platforms and users signifies a problem that developers have failed to address. SCOT puts forth a selection and variation process in the multi-directional model of development in technological artefacts. By examining privacy discourse of social agents on Reddit and Medium in regard to blockchain privacy platforms, we can define the function of the artefact according to the users. For instance, according to the discourse analysis, we can conclude that to social agents, blockchain privacy platforms succeed in particular aspects of privacy such as safety and security but do poorly at solidifying trust between social agents and the company. Because this theme is crucial for many social agents, they could reject the artefact altogether because the platforms fail to offer a viable solution to privacy. If blockchain privacy platforms want to capture this social group, they must reimagine the artefact with the help of social agents.

Moreover, this social group is imperative to capture as Reddit and Medium users are self-described privacy enthusiasts, who take great interest in new technology and privacy issues. According to Roger's (1993) diffusion of innovations theory, Reddit and Medium users represent innovators, or early adopters. Innovators can be characterized as a venturesome circle of peers where cliques are common and early adopters are regarded as "the individual to check in with" before using a new idea (p. 264). For an artefact to be further diffused into the mainstream, it is crucial that these groups communicate their recommendations to others and convince them of the benefit in adopting these innovations. This process of deliberation between social agents effectively captures the multi-directional model that Pinch and Bijker described in their investigation of the development of the recumbent bicycle. According to this development process, the next steps include a reimagination of the blockchain privacy platforms, followed by further deliberation by social agents who will determine if the platforms have provided a solution to their problem. In this case, blockchain privacy

platforms must work to create trust between developers and users and solve the beta issues that have become an area of frustration for social agents. Fortunately, by examining the latest releases from each blockchain privacy platform, new beta versions attempt to work out notable usability issues. For instance, Oasis Labs released the Oasis Gateway in September 2019, an improved version of their software for decentralized applications. In the release, the Oasis Lab team states:

> But to compete with centralized applications, decentralized apps — or DApps — must provide more than just the intrinsic properties of blockchain — they must meet the same usability standards of the popular mobile and web apps ubiquitous to today's users" (Auge-Pujadas, 2019).

In this way, blockchain privacy platforms are actively reimagining their technical code to meet the cultural code of its users.

Although Reddit and Medium users represent an important social group that advises the developmental direction of blockchain privacy platforms, it should be noted that this group can share a hive mind mentality (Betteridge, 2010, Workman, 2014). This is a limitation when focusing on such a niche group of users. Reddit and Medium represent a venturesome, privacy-focused and technology savvy individuals enthusiastic about these platforms; however, Reddit and Medium are typically male-dominated spaces. Workman (2014) states the presence of a hivemind, combined with a high number of male users makes it a hostile space for women. According to Betteridge (2010), Internet communities like Reddit tend to attract a largely straight, white, male user base. The nature of this homogenous user base can lead to a hive mind, which causes user content to match the general opinions of other Redditors. This was exemplified in conversations surrounding Brave where users generally opposed the platform and those who supported it were defensive outliers. For example, in a post in the subreddit r/privacytoolsIO, user blue_pill_90210 begins the query with the statement: "So I've noticed it's pretty common for those who support the Brave browser to get down-voted on this sub while there is strong support for hardened FF" (Reddit, 2019). Following this, the user asks:

> So my question is why anybody who supports Brave gets down-voted? And please answer precisely as I am sure this post will get down-voted even though I like aspects of both browsers and am not a Brave fanboy, but it is growing on me" (u/blue_pill_90210, 2019).

The Reddit hive mind generally disproves of Brave in favour of Firefox and downvotes those who show their support for the platform. While this examination of Reddit users represents an important social group in the social construction of blockchain privacy platforms, it must be known that such a hivemind does not accurately represent an all-encompassing perspective of innovators and potential early adopters. Likewise, Medium is a technology focused UGC, and the discrepancies between men and women in technology are well-documented (Crow, 2005; Wånggren, 2017; Vickery & Everbach, 2018). Hackernoon, the crypto-focused offshoot of Medium describes its audience as “younger, wealthier and more educated than the internet’s average” (StartEngine, 2018). The figure below demonstrates the discrepancy between genders in Hackernoon space.

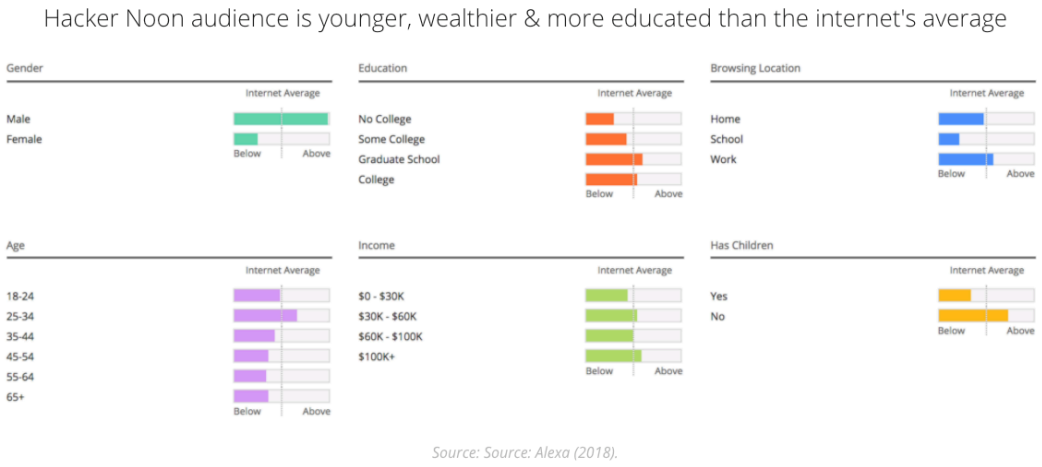

Figure 9. Hackernoon Demographics, StartEngine, 2018

There is a significant gap between male and female audience members of Hackernoon. This represents a larger disparity between men and women in the technology sphere. As we know, technology is a product of the social, economic and political environment in which it is created, meaning important social groups, like women and the underprivileged are often left out of the equation. (Pinch & Bijker, 1985).

6.6. Conclusion

This chapter compared and contrasted themes of privacy between blockchain privacy platforms and users on Reddit and Medium. The discourse analysis revealed both similarities and differences in conceptions of privacy between the two groups. From

the discourse analysis, similarities were noted in the themes of ad-blocking, data ownership and safety and security. Ad-blocking was exclusive to Brave, but most of the feedback on Reddit and Medium regarding this feature were positive and social agents were enthusiastic about Braves' automatic ad-blocking. So much so, that a number of the comments were defensive in nature as other Reddit users attempted to tear down or discredit their business model. Next, not only was data ownership a shared privacy theme, but a shared ethos between blockchain privacy platforms and social agents. Both groups expressed the desire to restructure the current Internet environment for the good of the individual, rather than major centralized conglomerates such as Facebook and Google. Finally, safety and security was a top priority for both platforms. This feature was advertised heavily by blockchain privacy platforms, and users understood that protection from malicious activity, hackers and trackers was crucial in obtaining overall privacy.

Conversely, the areas in which blockchain privacy platforms and social agents differed included ethics and trust and usability. Ethics and trust was a theme that appeared solely on the side of social agents and exemplified the importance of brand and leadership reputation. When reviewing blockchain privacy platforms, it seems users do not experience the platform in a bubble, rather, they take into account all aspects of the platform including leadership team, company ethos and its overall trustworthiness. This was evident in comments made evaluating the trust of the developers and leaders behind blockchain privacy platforms. For instance, Brave co-founder, Brendan Eich, received backlash on Reddit because of his personal views on same-sex marriage. Furthermore, Brave as a platform was often dismissed because it is built on Google's Chromium software. Users either did not trust Chromium and felt the ethos between Google and Brave were disjointed or did not want to inadvertently support a Google product. On the other hand, users also expressed their approval of a blockchain privacy platform if they trusted the team behind it. For instance, users were enthusiastic about the team behind Oasis Labs and considered it to be a reason to adopt the technology. In the nascent stage of blockchain privacy platform development, it appears that companies must work doubly to build trust with their user-base as users are already hesitant to adopt a new technology. To do so, they must not only experience a perceived usefulness and ease of use, they must also trust the figureheads behind the technology. Perhaps because of increasing reports of privacy breaches and unethical activity, such

as the Facebook and Cambridge Analytica scandal, users are becoming inherently distrustful of online platforms. This content analysis revealed that this should be a top priority for blockchain privacy platforms hoping to garner new users and eventually break into the mainstream.

Lastly, usability was coded for in both blockchain privacy platforms and Reddit and Medium users, but oftentimes, for two different reasons. All three blockchain platforms framed their new technology as simple and intuitive for the user. While Medium users tended to be more complimentary of the usability of these platforms, a number of Reddit users expressed their frustration at the technical glitches that come with beta versions of a product. Because these social agents are particularly technically savvy, it can be assumed most understand the flaws that come with a beta version of a platform. Despite this, many users were still disappointed when attempting to use the platform, even dismissing the platform altogether because of its technical faults.

Overall this chapter was imperative in unifying the results of the discourse analysis and revealing similar and disparate themes of privacy between the two groups studied. From the discourse analysis, we have a better idea of what blockchain privacy platforms are doing right to appeal to privacy enthusiasts, and what they can improve on. Furthermore, it shows how discourse can alter the technical code of emerging technologies. The beta updates from blockchain privacy platforms actively incorporated usability feedback from vocal social agents. These blockchain privacy platforms remain in the early stages of technological development and adoption, which is an optimal time for social agents to intercede in the social construction of the artefact.

Chapter 7. Conclusion

The Internet has gone through a number of iterations since its inception in the early 80s. Yet, each iteration demonstrates a compelling case of social construction. Arpanet users altered its technical code by making the chat function a central focus of the technology. Similarly, Minitel users adapted the peripheral chat function, Gretel, to become a wide-spread messaging system. The Internet we interact with today is much different than the original Web 1.0 characterized by hyper-links, decentralization and community. Now, centralized conglomerates driven by data have become information silos, invalidating data ownership and privacy rights of individual users. Fortunately, the Internet remains a fluid and malleable technology that can be altered to better suit our current political, economic and social environment. We are bearing witness to another online shift, where the Internet more accurately reflects the values of motivated social agents. The Internet's technical code is conducive to heterogeneity and can be altered by those motivated enough to do so.

This thesis explored how social agents use privacy discourse to alter the technical code of an emerging technology. The term privacy is notoriously difficult to define. Privacy in the digital age is even more challenging to discern because the Internet is constantly shifting. Web 2.0 saw the increased role of social media and online networking where users grapple with online participation while maintaining a level of privacy. Next, data mining, algorithms and predictive computing created a challenging environment to protect privacy and maintain individual data rights. Our current surveillance society along with big data has created an Internet environment where online privacy is hotly debated. Public awareness of privacy issues have grown as the media consistently publishes stories on the adverse impacts of big data for users. The Cambridge Analytica scandal of 2018 became a catalyst in the growing concern for online privacy rights. The actions of Cambridge Analytica and Facebook demonstrated the nefarious consequences of data mining to not only privacy, but the sanctity of democracy. This scandal is only one of many instances of data manipulation and privacy breaches that characterize our current data-driven Internet environment.

To combat the appropriation of user data and the increasing power of centralized conglomerates, users along with legislators are using privacy discourse to reorient control. The term privacy has grown outside itself and is now used to symbolize the fight to reign in online conglomerates such as Amazon, Facebook and Google. By amalgamating the power struggle between users, legislators and online conglomerates into the umbrella of privacy, those working to reclaim power have a platform to stand on. This is evident in the variety of advocacy groups such as The Electronic Freedom Foundation, that use privacy as grounds to fight for individual rights in the digital world. Through privacy discourse, users are attempting to reclaim their digital rights from the bottom-up, rather than wait for a top-down approach.

Privacy discourse encompasses an ethos of equality, decentralization and control. An emerging technology that shares this ethos is blockchain. Developers have created privacy platforms built on blockchain and offer these applications as a way to protect data and maintain online privacy. Just as the Internet is conducive to change, blockchain invites social construction due to its malleable technical code. Blockchain is a new technology and therefore, in a stage of interpretive flexibility. Social groups are currently vying to see their values represented in blockchain before the artefact reaches closure. This thesis explored the process of social construction in blockchain platforms by analyzing the privacy discourse surrounding these platforms.

This thesis employed a comparative discourse analysis methodology to examine privacy discourse on blockchain privacy platforms and on UGC platforms. I chose to study three blockchain platforms that offered beta versions of their product: Brave, Civic and Oasis Labs. This is a valuable stage to study social construction due to its interpretive flexibility. Conversely, I chose to analyze privacy discourse surrounding these blockchain platforms on Reddit and Medium. Both Reddit and Medium host thriving communities of privacy and technology enthusiasts that are critical in their evaluations of blockchain platforms. The results of the comparative discourse analysis were valuable in understanding how privacy discourse works to reshape the technical code of blockchain platforms. Moreover, this study informs how motivated social agents can reshape online power structures.

I began by examining discourse on the three blockchain platforms. First, I coded for general themes which included: open-source, cost, rewards, usability and privacy.

Next, I parsed privacy into its subcategories: ad-blocking (5%), general privacy (7.5%), decentralization (10%), data ownership (10%), and safety and security (67.5%). Using a keyword search, I followed the same coding process with UGC platforms, Reddit and Medium. Five major privacy themes were identified on Reddit and Medium: data ownership (7%), ad-blocking (9%), general privacy (12%), safety and security (34%) and trust and ethics (38%).

The results of the discourse analysis help to understand the relationship between privacy discourse and technical code in reshaping online power structures. Similar themes demonstrate an agreement between blockchain privacy platforms and social agents on conceptions of privacy. In addition, the discourse analysis shows that these privacy themes are indeed present in the features and overall technical code of Brave, Civic and Oasis Labs. When effective, blockchain privacy platforms are a step toward reimagining the Internet as more decentralized space, where users can reclaim data ownership and overall privacy rights.

Safety and security were a significant theme for both blockchain platforms and users. Blockchain platforms touted their safety and security features most frequently and users responded positively signifying a joint understanding of the importance of safety and security in overall privacy protection. Ad-blocking was a feature exclusive to Brave, and users responded similarly. Users were pleased that Brave offered this feature, and much of the discourse showed that Reddit users were defensive when other users made false claims regarding Brave's ad-blocking model. Both blockchain privacy platforms and its users saw data ownership as imperative in the fight for individual privacy rights. Blockchain privacy platforms emphasized the idea of control when framing data ownership and users were responsive to this feature. Both platforms and users herald safety and security, ad-blocking and data ownership as key features in the fight to maintain individual privacy online. Moreover, similar themes show that user values are represented in blockchain privacy platforms and these platforms are indeed responding to privacy problems brought forth by users. For instance, if there were no similar themes between the two parties, this would not exemplify social construction as user values are not represented in the artefact.

However, there were two themes that revealed divergence between blockchain platforms and users. Trust and ethics was the largest theme for users (38%) and did not

appear at all in the analysis of blockchain platforms. When evaluating blockchain platforms, users take into account the team behind the technology and the values they represent. For instance, users passed on Brave browser because the founder, Brendan Eich does not support gay marriage. Additionally, users were wary of Brave's use of chromium software. They did not want to inadvertently support Google as it represents the centralized conglomerates they are actively trying to divert. However, the consideration of ethics and trust can work in a platform's favour. The team behind Oasis Labs saw positive affirmations from users and users trusted this team because they maintained an exceptional reputation. The data shows that when choosing to adopt an emerging technology such as blockchain, users take into account variables outside of the technology itself, namely, the trustworthiness of the team behind the technology.

The last point of contention in the discourse analysis was the usability theme. While blockchain platforms framed their applications as simple and intuitive, users thought otherwise. Despite knowingly interacting with a beta version of the platform, users were frustrated at the beta problems that came along with it. Technical glitches, a lack of customer service and incompatibility was a source of dismay for users. This demonstrates the importance of usability when users evaluate a new technology. Even though these users are more technically savvy than the average user, this group still became frustrated when applications were not as easy to use as advertised.

While the usability theme revealed discrepancies between blockchain platforms and users, it also reveals important instances of social construction. Developers of these platforms actively responded to these usability issues and worked to improve the technical issues with each new beta release. For instance, Oasis Labs' labs released a new beta version of their software in September 2019 that explicitly stated improved usability for users. In the blog post revealing this beta version, developers addressed the usability issues and this new version was an attempt to resolve these issues. User values were taken into account and developers made an effort to realize these values within the technology.

This research is an important addition to communication literature because it approaches technological innovation and development from a social perspective. This study demonstrates how human communication influences technological construction. More specifically, this study outlines how privacy discourse can be used to leverage

users' preferences within blockchain platforms. The communication patterns and themes that emerged from the discourse analysis provide an understanding of the values users felt should be represented in the blockchain privacy platforms. Much of the literature on blockchain and privacy comes from a purely technological perspective. Scholars identify the role of blockchain in preserving user privacy and outline key opportunities and challenges (Kshetri, 2017; Wolfond, 2017; Yup, Wright, Tian, Liu, 2018). However, these evaluations do not encompass the perspectives of early users, such as technology enthusiasts interacting with beta versions of the technology. This study addresses this gap and provides a deeper look into the black box of technological innovation and development.

A SCOT theoretical framework proved crucial in demonstrating how user values are represented in emerging technologies. SCOT provided a template for understanding the multidirectional development process of blockchain privacy platforms. User discourse was crucial in exploring how users interpret the technology and identify problems within the artefact. Pinch and Bijker's (1984) study of the recumbent bicycle was a key piece of literature that corroborated the process of social construction in blockchain privacy platforms. Approaching new technologies from a SCOT perspective, rather than a purely scientific one, allows researchers to better understand the social, economic and political context in which the technology stems from. Technology is imbued with human agency, and a SCOT theoretical framework was successful in understanding this intersubjective process.

Moreover, this thesis provides a practical evaluation of blockchain platforms as a tool for individual privacy protection. By analyzing user privacy discourse, affordances and constraints of blockchain for privacy are elucidated. For users, this study outlines major features of blockchain privacy platforms such as safety and security, ad-blocking and data ownership. In addition, it introduces users to the overall ethos of blockchain development. Blockchain was developed with individual liberties in mind in an attempt to counter the Internet's increasing centralization. Users that connect with this ethos and value individual privacy, data ownership and decentralization may feel optimistic about the future of their Internet environment. The three blockchain platforms outlined could work as practical solutions for overall user privacy protection for interested users.

At the meso level, this thesis provides policymakers and researchers with a practical solution for securing sensitive information. Blockchain is a decentralized, encrypted and immutable database that can be used for a variety of applications such as identity management, supply chain, smart contracts and much more. Policymakers should consider adding blockchain to their arsenal in conjunction with top-down approaches such as the GDPR when considering how to mitigate the negative impacts of online conglomerates. This study also outlines the importance of user discourse in technology development. This reiterates the importance of interdisciplinary action when attempting to solve a social problem. While scientific truths remain an important part of research, knowledge production is multifaceted and should include various perspectives. This includes academia, government and the community.

More widely, blockchain is considered a tool for social change, and this topic is an emerging research focus. When used by governments, blockchain promotes trust and transparency and gives citizens more opportunity to safeguard and control their records and online identity. For instance, blockchain can be used to facilitate a secure electronic voting system and counteract fraud and corruption through immutable record-keeping. This thesis provides an introduction to the principles of blockchain and its potential to counteract online information silos at the user-level, institutionally and globally.

There are limitations to this study, both ontologically and technically. This thesis focused on a small group of innovative users that do not represent a democratic whole. Reddit has been known to facilitate echo chambers, where users' views are consistently reinforced through a hivemind mentality. This became noticeable especially in users' evaluation of Brave. When users discussed Brave, the overall consensus was one of distrust and disapproval of the platform. Users that spoke highly of the platform had to do so in a defensive manner and were sometimes criticized for their views. Users in favour of Brave could potentially not participate in this discourse in fear their views would be shut down by the rest of the community. While Reddit is an open and participatory platform, it is not necessarily democratic. While the action of social agents rearranging technology to better suit their needs remains example of democratic rationalization, Reddit and Medium users are a limited group of users with a particular worldview. This is a narrow representation of users, even those users who can be categorized as innovators. In the same vein, this study only examined three blockchain privacy

platforms. The ways in which these three platforms are socially constructed cannot be applied to blockchain platforms generally. Too, blockchain remains in a nascent stage. More research must be done to evaluate the affordances and constraints of blockchain platforms for privacy protection.

Additionally, it is difficult to determine the extent of social construction without studying the discourse of developers and the team behind these blockchain platforms. While I observed an effort to better incorporate user values into the technology through updated beta versions of the platform, I did not observe the process. To understand the process of social construction between users and developers, it would be helpful to examine discourse from developers during the development process. While we can assume instances of social construction, I do not know the motives of developers in their decision-making. Future research should examine not only discourse on blockchain platforms, but the discourse from the development process. It would be fruitful to understand how privacy discourse on blockchain privacy platforms shift according to user feedback.

Blockchain is a nascent technology and the beta versions of each privacy platform came with a myriad of technical issues. While studying a technology in this nascent stage is valuable when exploring its interpretive flexibility, user evaluation of the platform could be based on its usability rather than its ethos. For instance, users who have trouble navigating the technology could write it off as impractical for privacy protection without realizing its potential. Once these blockchain platforms release a public version of their product, it would be interesting to examine the general publics' evaluation of these platforms compared to groups of innovators.

This thesis demonstrates the power of privacy discourse when negotiating power on the Internet. By comparing privacy discourse between blockchain platforms and users, I discovered that user values were generally represented in blockchain platforms. When they were not, in the case of usability, developers sought to resolve these issues through new beta versions of the technology. In the future, developers should also consider their own reputation when vying for the adoption of an emerging technology. According to users, organizational reputation is crucial, and platforms should foster a trustworthy reputation before releasing a new technology.

While our current Internet architecture holds little resemblance to the decentralized, community-based Web 1.0, the Internet remains a participatory technology. The technical layers of the Internet are malleable and there is democratic potential within the Internet's architecture. Individual users play a crucial role in restructuring the Internet. Using blockchain technology to protect individual privacy is a step in interacting with a more decentralized and democratic Internet environment.

References

Adoni, H., & Mane, S. (1984). Media And The Social Construction Of Reality. *Communication Research*, *11*(3), 323–340. doi: 10.1177/009365084011003001

Adoni, H. & Cohen, A. A. (1978) Television economic news and the social construction of economic reality. *Journal of Communication, 28*(4). 61-70.

Aiello, M. (2018). *The Web was Done by Amateurs.* Springer.

Akasha (2018). https://akasha.world/

Allen, A. L. (2016). Protecting one's own privacy in a big data economy. Harvard Law Review Forum, 130. 70-78.

Altman, I. (1975). The Environment and Social Behaviour: Privacy, Personal Space, Territory and Crowdfunding. Monterey, California: Brooks/Cole.

Anderson, K. (2015). Ask me anything: What is Reddit? Library Hi Tech News, 32(5). 8-11.

Andrejevic, M. (2002). The work of being watched: Interactive media and the exploitation of self-disclosure. *Critical Studies in Media Communication, 19*(2), 230-248.

Ankerson, M. S. (2015). Social Media and the "Read-Only" Web: Reconfiguring Social Logics and Historical Boundaries. *Social Media + Society*. https://doi.org/10.1177/2056305115621935

Anonymous Ledger. (2018). Ekiden protocol by Oasis Labs. *Medium.* https://medium.com/coinsolidation/ekiden-protocol-by-oasis-labs-2eada7e068af

Ansorge, J. T. (2011). Digital Power in World Politics: Databases, Panopticons and Erwin Cuntz. *Millennium*, *40*(1), 65–83. https://doi.org/10.1177/0305829811409178

"ARPAnet ." Gale Encyclopedia of E-Commerce . Retrieved March 12, 2019 from Encyclopedia.com: https://www.encyclopedia.com/economics/encyclopedias-almanacs-transcripts-and-maps/arpanet

Atzori, M. (2017). Blockchain technology and decentralized governance: Is the state still necessary? *Journal of Governance and Regulation, 6*(1), 45–62.

Azrael, M. L. (1984). Lost Privacy in the Computer Age: Computer Matching Programs Are Turning Uncle Sam into Big Brother. *University of Baltimore Law Forum,*17-25. Retrieved April 18, 2018, from http://scholarworks.law.ubalt.edu/lf/vol14/iss2/5

Bailey, J. (2000). Some Meanings of the Private in Sociological Thought. *Sociology, 34*(3), 381-401.

Baker, M. (2014). Brendan Eich steps down as Mozilla CEO. *Mozilla*. https://blog.mozilla.org/blog/2014/04/03/brendan-eich-steps-down-as-mozilla-ceo/

Baldwin, J. (2018). In digital we trust: Bitcoin discourse, digital currencies, and decentralized network fetishism. *Palgrave Communications*, *4*(1), 1-10.

Barocas, S., & Nissenbaum, H. (2014). Big data's end run around procedural privacy protections. *Communications of the ACM, 57*(11), 31-33.

Bartlett, J. (2016). *The Dark Net: Inside the Digital Underworld.* Melville House Publishing.

Bauman, Z., & Lyon, D. (2013). *Liquid Surveillance.* Polity Press.

Becker, J., Einwiller, S. A., & Medjedovic, J. (2014). The effect of incongruence between CEO and corporate brand personality on financial analysts' attitudes and assessment of a company's performance. *International Journal of Strategic Communication*, *8*(3), 146-159.

Berger, A. A. (2000). *Media and Communication Research.* SAGE.

Berger, P., & Luckmann, T. (1967). *The social construction of reality : A treatise in the sociology of knowledge / Peter L. Berger and Thomas Luckmann.* (Anchor books ed., Anchor books ; A589).

Bessi, A. (2016). Users polarization on Facebook and Youtube. *PLOS ONE, 11*(8). 1-24.

Bordet, C. (2019). The browser that respects your privacy. *Medium.*

Bossewitch, J., & Sinnreich, A. (2013). The end of forgetting: Strategic agency beyond the panopticon. *New Media & Society*, *15*(2), 224–242. https://doi.org/10.1177/1461444812451565

Boyne, R. (2000). Post-panopticonism. *Economy and Society, 29*(2). 285-307.

Braman, S. (2011). The framing years: Policy fundamentals in the Internet design process, 1969–1979. *The Information Society*, *27*(5), 295-310.

Brave. (2019). *Brave. https://brave.com/*

Brumagen, R. (2018). Unsafe at any speed. *Encyclopedia Britannica. https://www.britannica.com/topic/Unsafe-at-Any-Speed*

Buchan, R. (2018). cyber-security. In A Concise Oxford Dictionary of Politics and

International Relations. : Oxford University Press. Retrieved 18 Mar. 2020, from https://www-oxfordreference-com.proxy.lib.sfu.ca/view/10.1093/acref/9780199670840.001.0001/a

Burgess, J., Marwick, A. E., & Poell, T. (Eds.). (2017). The sage handbook of social media. Retrieved from https://ebookcentral-proquest-com.proxy.lib.sfu.ca

Butt, T., & Landridge, D. (2003). The construction of self: The public reach into the private sphere. Sociology, 37(3). 477-492.

Cadwalladr, C. & Graham-Harrison, E. (2018). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian.* https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

Cadwalladr, C. (2020). Fresh Cambridge Analytica leak 'shows global manipulation is out of control. *The Guardian.* https://www.theguardian.com/uk-news/2020/jan/04/cambridge-analytica-data-leak-global-election-manipulation

California Secretary of State (2019). *Brave Software Inc*. https://businesssearch.sos.ca.gov/CBS/Detail

Cavoukian, Ann and Tapscott, Don. 1995. Who knows: safeguarding your privacy in a networked world. Toronto: Random House of Canada

Chakravorty, A., & Rong, C. (2017, January). Ushare: user controlled social media based on blockchain. In *Proceedings of the 11th international conference on ubiquitous information management and communication* (pp. 1-6).

Chow-White, P.A. and Green, S.E. (2013) Data mining difference in the age of big data: Communication and the social Shaping of genome technologies from 1998 to 2007. *International Journal of Communication*, 7, 556-583.

Civic. (2019). https://www.civic.com

Clarke, R. (1994), "Dataveillance by Governments: The Technique of Computer Matching", *Information Technology & People*, Vol. 7 No. 2, pp. 46-85. https://doi.org/10.1108/09593849410074070

Cohen, J. (2018). Exploring echo-systems: How algorithms shape immersive media environments. *Journal of Media Literacy Education, 10(*2). 139-151.

Coin Market Cap (2019). Top 100 Cryptocurrencies by Market Capitalization. https://coinmarketcap.com/

Coussieu, W. (2010). World playful and simulation. The social experiment the role playing online. *Societes, 107*(1), 43-55.

Craig, T., & Ludloff, M. (2011). *Privacy and big data / Terence Craig and Mary E. Ludloff.Crow, B. (2005). Gender and Technology. Canadian Journal of Communication, 30(3).*

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User Acceptance of Computer Technology: A Comparison of Two Theoretical Models. *Management Science*, *35*(8), 982–1003. doi: 10.1287/mnsc.35.8.982

Dean, J. (2005). Communicative capitalism: Circulation and the foreclosure of politics. *Cultural Politics*, *1*(1), 51-74.

Desjardins, J. (2019). How much data is generated each day? *World Economic Forum. https://www.weforum.org/agenda/2019/04/how-much-data-is-generated-each-day-cf4bddf29f/*

Dewey, C. (2016, August 19). 98 personal data points that Facebook uses to target ads to you. The Washington Post. Retrieved from www.washingtonpost.com/news/the-intersect/wp/2016/08/19/98-personal-data-points-that-facebook-uses-to-target-ads-to-you

Doherty, N. F., Coombs, C. R., & Loan-Clarke, J. (2006). A re-conceptualization of the interpretive flexibility of information technologies: redressing the balance between the social and the technical. *European Journal of Information Systems*, *15*(6), 569-582.

Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017, March). Blockchain for IoT security and privacy: The case study of a smart home. In *2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops)* (pp. 618-623). IEEE.

Dunphy, P., & Petitcolas, F. A. (2018). A first look at identity management schemes on the blockchain. *IEEE Security & Privacy*, *16*(4), 20-29.

EcommerceDB (2019). *Store Ranking and Overview. https://ecommerce.db.com/en/ranking/ww/all?search=amazon*

Economist (2015 October). The trust machine. *The Economist. https://www.economist.com/leaders/2015/10/31/the-trust-machine*

Economist. (2017 May). The world's most valuable resource is no longer oil, but data. *The Economist.https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data*

Edgar, A. (2016) Personal identity and the massively multiplayer online world, Sport, Ethics and Philosophy, 10:1, 51-66, DOI: 10.1080/17511321.2016.1168478

Elisa, N., Yang, L., Chao, F., & Cao, Y. (2018). A framework of blockchain-based secure and privacy-preserving e-government system. *Wireless Networks*, 1-11.

Elmer (2013). IPO 2.0: The panopticon goes public. *MediaTropes, 4*(1). 1-16.

Enigma (2018). https://enigma.co/

EPIC. (2020). https://epic.org/

Everbach, T., & Vickery, J. R. (2018). *Mediating Misogyny: Gender, Technology, and Harassment*. Taylor & Francis Limited.

European Parliament and Council (2016). *General Data Protection Regulation. https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504*

Feenberg, A. (2019) The Internet as network, world, co-construction, and mode of governance, The Information Society, 35:4, 229-243, DOI: 10.1080/01972243.2019.1617211

Feenberg, A. (2013). The Internet in question, presented at Dialectics of the Digital World, Athabasca University, 2013. Alberta, Canada.

Feenberg, A., & Bakardjieva, M. (2004). *Consumers or citizens? The online community debate*. na.

Feenberg, A. (1992). Subversive Rationalization: Technology, Power, and Democracy. *Inquiry, 35 (*3-4), 301-322.

Fetscherin, M. (Ed.). (2015). *CEO branding: Theory and practice*. Routledge.

Finley, K. (2019, April 24). This Browser Will Pay You to Surf the Web. Retrieved from https://www.wired.com/story/brave-browser-will-pay-surf-web/

Flanagin, Andrew J., et al. “Technical Code and the Social Construction of the Internet.” *New Media & Society*, vol. 12, no. 2, 2009, pp. 179–196., doi:10.1177/1461444809341391.

Flanagin, A., Flanagin, C., & Flanagin, J. (2010). Technical code and the social construction of the internet. *New Media and Society, 12*(2). 179-196.

Foddy, W. H. (1984) A critical evaluation of Altman’s definition of privacy as a dialectical process. *Journal for the Theory of Social Behaviour, 14*(3). 297-307.

Foucault, M. (1997). *Discipline and Punish: The Birth of the Prison.* (Sheridan, A., Trans). Random House.

Frizzo-Barker, J., Chow-White, P. A., Adams, P. R., Mentanko, J., Ha, D., & Green, S. (2019). Blockchain as a disruptive technology for business: A systematic review. *International Journal of Information Management*.

Frizzo-Barker, J., & Chow-White, P. (2014). Research in Brief: From Patients to Petabytes: Genomic Big Data, Privacy, and Informational Risk. *Canadian Journal of Communication, 39*(4), 615-625.

Fuchs, C. (2010). Labor in Informational Capitalism and on the Internet. *The Information Society*, *26*(3), 179-196.

Fyfe, N., & Bannister, J. (1996). City watching: Closed circuit television surveillance in public spaces. *Area, 28*(1). 37-46.

Galič, M. , Timan, T., & Koops, B.-J. (2016). Bentham, Deleuze and beyond: An overview of surveillance theories from the panopticon to participation. *Philosophy & Technology*. doi:10.1007/s13347-016-0219-1

Gamson, W. A., Croteau, D., Hoynes, W., & Sasson, T. (1992). Media Images and the Social Construction of Reality. *Annual Review of Sociology*, *18*(1), 373–393. doi: 10.1146/annurev.so.18.080192.002105

Gandy, O. (1993) *The Panoptic Sort: A Political Economy of Personal Information.* Routledge.

Gehl, R.W. (2018). Alternative social media: From critique to code. In Burgess, J., et al. (Eds), *The SAGE Handbook of Social Media (p. 330-350*). SAGE Publications.

Gellman, R., Dixon, Pam, & Gale Group. (2011). *Online privacy a reference handbook* (Gale virtual reference library). Santa Barbara, Calif.: ABC-CLIO.

Gil de Zuniga, H. & Coddington, M. (2013). Social media. *Oxford Bibliographies.* (P. Moy, Ed.) https://www-oxfordbibliographies-com.proxy.lib.sfu.ca/view/document/obo-9780199756841/obo-9780199756841-0105.xml?rskey=qM7z53&result=4&q=social+media#firstMatch

Giuri, P., Rocchetti, G., & Torrisi, S. (2002). *Open source software: from open science to new marketing models. An enquiry into the economics and management of open source software* (No. 2002/23). LEM Working Paper Series.

Glum, J. (2018). This is exactly how much your personal information is worth to Facebook. *Money. https://money.com/how-much-facebook-makes-off-you/*

Goldman, B. (2018). Why I'm bullish on BAT and the Brave browser in 2018. *Medium. https://medium.com/hackernoon/why-im-bullish-on-bat-and-the-brave-browser-in-2018-8e2cbc0ce420*

Goux J (1994) The coiners of language. University of Oklahoma Press, Norman, OK

Government of Canada (2000). *Personal Information Protection and Electronic Documents Act. https://www.parl.ca/DocumentViewer/en/36-2/bill/C-6/royal-assent*

Government of Canada (1983). *The Access to Information Act* and the *Privacy Act.* https://laws-lois.justice.gc.ca/eng/acts/P-21/index.html

Habermas, J. (1989). *The structural transformation of the public sphere : An inquiry into a category of Bourgeois society / Jürgen Habermas ; translated by Thomas Burger with the assistance of Frederick Lawrence.* (Studies in contemporary German social thought).

Hackernoon. (2019). Hacker Noon FAQs answered with 6 words or less. *Hackernoon. https://hackernoon.com/hacker-noon-faqs-with-six-word-answers-aw1ls3z1q*

Hayek, F. A. von. (1978) *Denationalization of money: the argument refined.* London: Inst. Of Economic Affairs.

Hier, S. P. (2004). Risky spaces and dangerous faces: Urban surveillance, social disorder and CCTV. *Social & Legal Studies*, *13*(4), 541–554. https://doi.org/10.1177/0964663904047333

Hilbert, M., et al. (2018). Communicating with algorithms: A transfer entropy analysis of Emotions-based escapes from online echo chambers. *Communication Methods andMeasures, 12*(4). 260-275.

Hrynyshyn, D. (2008). Globalization, nationality and commodification: the politics of the social construction of the internet. *New Media & Society*, *10*(5), 751–770. https://doi.org/10.1177/1461444808094355

Hu, J., Cen, J. Video surveillance in public space in China. *Front. Law China* 4, 474–488 (2009). https://doi.org/10.1007/s11463-009-0025-0

Hughes, C. (2019 May). It's time to break up Facebook. *The New York Times. https://www.nytimes.com/2019/05/09/opinion/sunday/chris-hughes-facebook-zuckerberg.html*

Hunter, W. (2016). The social construction of tourism online destination image: A comparative semiotic analysis of the visual representation of Seoul. *Tourism Management, 54*, 221-229.

ICOgens. (2018). Oasis Labs - A new era for scalability and privacy-preserving built with ever smart contracts...*Medium.*

Just, N., & Latzer, M. (2017). Governance by algorithms: Reality construction by algorithmic Selection on the Internet. *Media, Culture and Society, 39*(2). 238-258.

Jacobovitz, O. (2016). Blockchain for identity management. *The Lynne and William Frankel Center for Computer Science Department of Computer Science. Ben-Gurion University, Beer Sheva*.

Koens, T., & Poll, E. (2019). Assessing interoperability solutions for distributed ledgers. *Pervasive and Mobile Computing*, *59*, 101079.

Koonce, L. (2016). The wild, distributed world: get ready for radical infrastructure changes, from blockchains to the interplanetary file system to the internet of things. *Intellectual Property & Technology Law Journal*, *28*(10), 3.

Koskela, H. (2002). 'Cam Era' - the contemporary urban Panopticon. Surveillance and Society. 1. 10.24908/ss.v1i3.3342.

Knoblauch, H., & Wilke, R. (2016). The Common Denominator: The Reception and Impact of Berger and Luckmann's The Social Construction of Reality. *Human Studies, 39*(1), 51–69. doi: 10.1007/s10746-016-9387-3

Kramer A.D.I., Guillory, J.E., & Hancock, J.T. (2014). Experimental evidence of massive-scale emotional contagion through social networks. *Proceedings of the National Academy of Sciences, 111*(24), 8788-8790.

Krippendorff, K. (2004). *Content Analysis: An Introduction to Its Methodology.* SAGE.

Kshetri, N. (2017). Blockchain's role in strengthening cybersecurity and protecting privacy. *Telecommunications Policy, 41(*10), 1027-1038.

Kuchler, H. (2016). Ashley Madison agrees to $1.6m fine for data breach. *Financial Times. https://www.ft.com/content/db7a5c42-c21a-11e6-9bca-2b93a6856354*

Lane, F. (2009). *American privacy the 400-year history of our most contested right / Frederick S. Lane.* Boston, Mass.: Beacon Press.

Larsen, B. von S.-T. (2011). *Setting the watch: privacy and the ethics of Cctv surveillance*. Oxford: Hart.

Lassinantti, J., Bergvall-Kåreborn, B., & Ståhlbröst, A. (2014). Shaping local open data initiatives: Politics and implications. *Journal of Theoretical and Applied Electronic Commerce Research, 9*(2). 17-33.

Latour (1992). Where are the missing masses? The sociology of a few mundane artifacts. In Bijker, W.E. & Law, J. (Eds), *Shaping Technology/Building Society.* (225-258). MIT Press.

Latour, B., Woolgar, S., & Salk, J. (1986). *Laboratory life: the social construction of scientific facts.* Princeton, NJ: Princeton University Press.

Lauritsen, P., & Feuerbach, A. (2015). CCTV in Denmark 1954 – 1982. Surveillance & Society. 13. 528-538. 10.24908/ss.v13i3/4.4560.

Lazarovich, A. (2015). *Invisible Ink: blockchain for data privacy* (Doctoral dissertation, Massachusetts Institute of Technology).

Leeds-Hurwitz, W. (2016). Social Construction. *Oxford Bibliographies Online Datasets*.

Leman-Langlois, S. (2002) The myopic panopticon: The social consequences of policing through the lens. *Policing and Society, 13*(1), 43-58, DOI: 10.1080/1043946022000005617

Li, M., Zhu, L., & Lin, X. (2019, October). CoRide: A Privacy-Preserving Collaborative-Ride Hailing Service Using Blockchain-Assisted Vehicular Fog Computing. In *International Conference on Security and Privacy in Communication Systems* (pp. 408-422). Springer, Cham.

Lim, S. Y., Fotsing, P. T., Almasri, A., Musa, O., Kiah, M. L. M., Ang, T. F., & Ismail, R. (2018). Blockchain technology the identity management and authentication service disruptor: a survey. *International Journal on Advanced Science, Engineering and Information Technology*, *8*(4-2), 1735.

Lingham, V. (2016). Identity theft startup Civic plans to stop identity fraud before it happens. *Civic. https://www.civic.com/blog/identity-theft-startup-civic-plans-to-stop-identity-fraud-before-it-happens/*

Lingham, V. (2017). Civic is redefining digital identity. *Civic. https://www.civic.com/blog/civic-is-redefining-digital-identity/*

Lyon, D. (2018). *The Culture of Surveillance: Watching as a Way of Life.* Polity Press.

Lyon, D. (2002). Surveillance studies: Understanding visibility, mobility and the phenetic fix. *Surveillance and Society, 1*(1). 1-7.

Marwick, A. E., & Boyd, D. (2014). Networked privacy: How teenagers negotiate context in social media. *New Media & Society*, 16(7), 1051–1067. https://doi.org/10.1177/1461444814543995

Massanari, Adrienne. (2015). Participatory Culture, Community, and Play: Learning from Reddit. Peter Lang.

Mathiesen, T. (1997). The Viewer Society: Michel Foucault's `Panopticon' Revisited. *Theoretical Criminology*, *1*(2), 215–234. https://doi.org/10.1177/1362480697001002003

Mayer-Schönberger, V., & Cukier, K. (2013). *Big data : A revolution that will transform how we live, work, and think / Viktor Mayer-Schönberger and Kenneth Cukier.*

Medium. (2019). https://medium.com/

Mills, H. (2018). Avatar Creation: The Social Construction of "Beauty" in Second Life. *Journalism & Mass Communication Quarterly, 95*(3), 607-624.

Moore, P., Piwek, L., & Roper, I. (2017). The quantified workplace: A study in self-Tracking, agility and change management. In B. Ajana (Ed.), *Self-Tracking: Empirical and Philosophical Investigations* (pp. 93-110). [Chapter 7] Springer International Publishing. https://doi.org/10.1007/978-3-319-65379-2_7

Moriarty, D., & Mehlenbacher, A. R. (2019). The Coaxing Architecture of Reddit'sr/science: Adopting Ethos-Assessment Heuristics to Evaluate Science Experts on the Internet. *Social Epistemology*, *33*(6), 514-524.

Murphy, R. (1984). Social distance and the veil. In F. Schoeman (Ed). *Philosophical Dimensions of Privacy: An Anthology.* (p. 34-55). Cambridge: Cambridge University Press. Doi10.1017/CBO9780511625138.003

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

Net Market Share (2019). *Search engine market share.* http://www.netmarketshare.com

Newell P. B. (1998). A cross-cultural comparison of privacy definitions and functions: A systems approach. Journal of Environmental Psychology, 18, 357–371. doi:.10.1006/jevp.1998.0103

N.K. Gokul. (2018). Why I am finally switching from Chrome to Brave. *Medium. https://medium.com/@gokulnk/why-i-am-finally-switching-from-chrome-to-brave-e803495b3375*

Norris, C., & Armstrong, G. (1999). *The maximum surveillance society: the rise of Cctv*. Oxford: Berg.

Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic Analysis: Striving to Meet the Trustworthiness Criteria. *International Journal of Qualitative Methods*. https://doi.org/10.1177/1609406917733847

Oasis Labs. (2019). http://oasislabs.com

Ohm, P. (2014). Changing the Rules: General Principles for Data Use and Analysis. In *Privacy, Big Data, and the Public Good: Frameworks for Engagement* (pp. 96-111). Cambridge University Press.

Openwashing (2019). https://openwashing.org/

O'Reilly, T. (2006, December 10). Web 2.0 compact definition: Trying again. Retrieved from http://radar.oreilly.com/2006/12/web-20-compact-definition-tryi.htmlGoogle Scholar

Pearce, W. et al (2020) Visual cross-platform analysis: digital methods to research social media images, Information, Communication & Society, 23:2, 161-180, DOI: 10.1080/1369118X.2018.1486871

Peterson, G. W., & Peters, D. F. (1983). Adolescents Construction of Social Reality. *Youth & Society*, *15*(1), 67–85. doi: 10.1177/0044118x83015001005

Petrie, C. (2016). The proper use of the Internet: Digital private property. *IEEE Internet Computing, 20*(2). 92-94.

Pinch, T., & Bijker, W. (1984). The Social Construction of Facts and Artefacts: Or How the Sociology of Science and the Sociology of Technology might Benefit Each Other. *Social Studies of Science, 14*(3), 399-441.

Plant, S. (1997) *Zeroes and Ones: Women and the New Technoculture.* Doubleday.

Powers, M. (1996). A cognitive access definition of privacy. *Law and Philosophy, 15*(4), 369-386.

Primei.co. (2018). Oasis Labs ICO review. *Medium. https://medium.com/@Primeico/oasis-labs-ico-review-6ea9c67094b3*

Privacy International. (2020). https://privacyinternational.org/

Raab, C. D., & Mason, D. (2004) Privacy, Surveillance, Trust and Regulation, Information, Communication & Society, 7:1, 89-91, DOI: 10.1080/1369118042000208915

Rainie, L., Kiesler, S., Kang, R., Madden, M., Duggan, M., Brown, S., & Dabbish, L. (2013). Anonymity, privacy, and security online. *Pew Research Center*, *5*.

Record, R. A., Silberman, W. R., Santiago, J. E., & Ham, T. (2018). I sought it, I Reddit: Examining health information engagement behaviors among Reddit users. *Journal of health communication*, *23*(5), 470-476.

Reddit (2019). Reddit About. https://www.redditinc.com/

Redshaw, T. 2017. Bitcoin beyond ambivalence: Popular rationalization and Feenberg's technical politics. Thesis Eleven 138(1):46-64.

Rengel, A. (2013). *Privacy in the 21st Century / by Alexandra Rengel.* (Studies in ntercultural human rights ; v. 5).

Rogers, E. (2003). *Diffusion of Innovations*: *5th ed.* The Free Press.

Rosen, D., & Santesso, A. (2010). The panopticon reviewed: Sentimentalism and eighteenth-century interiority. *ELH, 77*(4), 1041-1059.

Rothsbard, M. N. (1963). *American's Great Depression.* Mises Institute.

Roy, A. (2018). Green marketing. In R. Kolb (Ed.), *The SAGE encyclopedia of business ethics and society* (Vol. 1, pp. 1670-1672). Thousand Oaks,, CA: SAGE Publications, Inc. doi: 10.4135/9781483381503.n547

Scassa, T. (2018). *Data ownership*. Centre for International Governance Innovation.

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a more representative definition of cyber security. *Journal of Digital Forensics, Security and Law*, *12*(2), 53-74.

Schintler, L., & McNeely, C. (2019). *Encyclopedia of Big Data edited by Laurie A. Schintler, Connie L. McNeely.*

Schoeman, F. (1984). Privacy: Philosophical dimensions of the literature. In F. Schoeman (Ed.), *Philosophical Dimensions of Privacy: An Anthology* (pp. 1-33). Cambridge: Cambridge University Press. doi:10.1017/CBO9780511625138.002

Schwerin, S. (2018). Blockchain and privacy protection in the case of the european general data protection regulation (GDPR): a delphi study. *The Journal of the British Blockchain Association*, *1*(1), 3554.

Siddiqa, A., Karim, A., & Gani, A. (2017). Big data storage technologies: A survey. *Frontiers of Information Technology & Electronic Engineering, 18*(8), 1040-1070.

Simona Isabella. (2007). Ethnography of Online Role-Playing Games: The Role of Virtual and Real Contest in the Construction of the Field. *Forum: Qualitative Social Research, 8*(3), Forum: Qualitative Social Research, 01 September 2007, Vol.8(3).

Shahbaz, A. & Funk, A. (2019). Freedom on the net 2019. *FreedomHouse.* https://freedomhouse.org/report/freedom-net/2019/crisis-social-media

Shapiro, M. A., & Lang, A. (1991). Making Television Reality. *Communication Research*, *18*(5), 685–705. doi: 10.1177/009365091018005007

Soni, D. (2018). Securing your identity with Civic. *Medium.* https://hackernoon.com/securing-your-identity-with-civic-7ea0d2f368a0

Smith, H., Dinev, T., & Xu, H. (2011) Information privacy research: An interdisciplinary review. *MIS Quarterly, 35.* 989-1015.

Smythe, D. W. (1981). On the audience commodity and its work. *Media and cultural studies: Keyworks*, *230*, 256.

Song, D. (2019). Devnet 2.0 and the new Oasis SDK. *Oasis Labs. https://medium.com/oasislabs/devnet-2-0-and-our-new-oasis-sdk-c858c25716e7*

Spiller K. et al. (2018) Data privacy: Users' thoughts on quantified self personal data. In: Ajana B. (eds) *Self-Tracking*. Palgrave Macmillan, Cham

StartEngine. (2018). Hackernoon. *StartEngine. https://www.startengine.com/hackernoon*

Steinfeld, N. (2016). "I agree to the terms and conditions": (How) do users read privacy policies online? An eye-tracking experiment. *Computers in Human Behaviour, 55B 992-1000.*

Strandburg, K. (2014). Monitoring, Datafication, and Consent: Legal Approaches to Privacy in the Big Data Context. In *Privacy, Big Data, and the Public Good: Frameworks for Engagement* (pp. 5-43). Cambridge University Press.

Swan, M. (2015). *Blockchain : Blueprint for a new economy / Melanie Swan.* (First ed.).

Swartz, L. (2017) Blockchain Dreams: Imagining techno-economic alternatives after Bitcoin. *Another Economy is Possible*, edited by Manuel Castells. Polity Press.

Swinhoe, D. (2019). What is the cost of a data breach. *CSO. https://www.csoonline.com/article/3434601/what-is-the-cost-of-a-data-breach.html*

Takahashi, D. (2018 July). Oasis Labs raises $45 million for 'privacy first' cloud on blockchain. *Venture Beat. https://venturebeat.com/2018/07/09/oasis-labs-raises-45-million-for-privacy-first-cloud-on-blockchain/*

Tholen, B. (2016). Drawing the Line: On the Public/Private Distinction in Debates on New Modes of Governance. *Public Integrity, 18*(3), 237-253.

Torque. (2018) How blockchain can give us back control of our identity and help avoid another Facebook / Cambridge Analytica scandal. *Medium.*

Trepte, S. (2015). Social media, privacy and self-disclosure: The turbulence caused by social media's affordances. *Social Media and Society, 1*(1). 1-2.

Tsfati, Y. (2011). Media Effects. *Oxford Bibliographies Online Datasets*. doi: 10.1093/obo/9780199756841-0081

United Nations (1948). *Universal Declaration of Human Rights*. https://www.un.org/en/universal-declaration-human-rights/

Vaidhyanathan, S. (2012). *The Googlization of Everything.* University of California Press.

Van Cann, H. (2017). Schluss and Civic, two of a kind? *Medium. https://medium.com/happy-blockchains/schluss-and-civic-two-of-a-kind-5d8edc306ec2*

Van Dijck, J. (2014). Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance & Society, 12*(2), 197-208.

Viseu, A., Clement, A., & Aspinall, J. (2004). Situating privacy online: Complex perceptions and everyday practices. *Information, Communication & Society*, *7*(1), 92-114.

Walby, K. (2009). Ottawa's national capital commission conservation officers and the policing of public park sex. *Surveillance and Society, 6*(4). 367-379.

Wanggren, L. (2017). *Gender, Technology and the New Woman*. Edinburgh University Press.

Warren, S., & Brandeis, L. (1890). The Right to Privacy. *Harvard Law Review, 4*(5), 193-220. doi:10.2307/1321160

Wikipedia. (2019). Brendan Eich. *Wikipedia. https://en.wikipedia.org/wiki/Brendan_Eich*

Whellams, M. (2018). Greenwashing. In R. Kolb (Ed.), *The SAGE encyclopedia of business ethics and society*(Vol. 1, pp. 1677-1679). Thousand Oaks,, CA: SAGE Publications, Inc. doi: 10.4135/9781483381503.n550

Westin AF (1967) Privacy and freedom. Atheneum, New York

Workman, H. M. (2014). Formation of safe spaces in gendered online communities: reddit and "the front page of the internet." *UMI Thesis.* Retrieved from https://repository.tcu.edu/handle/116099117/4558

Yu, Y., Li, Y., Tian, J., & Liu, J. (2018). Blockchain-based solutions to security and privacy issues in the Internet of Things. *IEEE Wireless Communications*, *25*(6), 12-18.

Zhang, A., & Lin, X. (2018). Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain. *Journal of medical systems*, *42*(8), 140.

Zhang, P., White, J., Schmidt, D. C., & Lenz, G. (2017). Applying software patterns to address interoperability in blockchain-based healthcare apps. *arXiv preprint arXiv:1706.03700*.

Zyskind, G., Nathan, O., & Pentland, A. (2015). Enigma: Decentralized computation platform with guaranteed privacy. *arXiv preprint arXiv:1506.03471*.

Reddit User References

0gicbea. (2019). Brave browser privacy.
Reddit. https://www.reddit.com/r/privacy/comments/83sa9v/brave_browser_privacy/

AI-girl. (2019). Civic competitors?
Reddit. https://www.reddit.com/r/civicplatform/comments/7q4cfy/civic_competitors/

ALLyourCRYPTOS. (2019). Would you recommend Brave browser?
Reddit. https://www.reddit.com/r/privacy/comments/8ur89i/would_you_recommend_brave_browser/

atoponce. (2019). Brave vs. Firefox data privacy.
Reddit. https://i.reddit.com/r/privacytoolsIO/comments/a6l3lo/brave_vs_firefox_data_privacy/

bbondy. (2019). Brave privacy browser is whitelisting trackers of Facebook and Twitter.

Reddit.https://www.reddit.com/r/privacy/comments/ap8rnv/brave_privacy_browser_is_whitelisting_trackers_of/

blue_pill_90210. (2019). Brave vs. Firefox data privacy.
Reddit. https://www.reddit.com/r/privacytoolsIO/comments/a6l3lo/brave_vs_firefox_data_privacy/

brave_w0ts0n. (2019). Brave privacy browser is whitelisting trackers of Facebook and Twitter. *Redditt*
https://www.reddit.com/r/privacy/comments/ap8rnv/brave_privacy_browser_is_whitelisting_trackers_of/

chongkwongsheng. (2018). Why I believe Civic will not succeed.
Reddit. https://www.reddit.com/r/civicplatform/comments/7t3zei/why_i_believe_civic_will_not_succeed/

ethfiend2064. (2019). Fundamental flaw in Civic's main use case?
Reddit. https://www.reddit.com/r/civicplatform/comments/96k5v2/fundamental_flaw_in_civics_main_use_case/

imillonario. (2019). Brave browser.
Reddit. https://www.reddit.com/r/privacy/comments/9o6p49/brave_browser/

Lifeofahero. (2019). Engima vs Oasis Labs.
Reddit. https://www.reddit.com/r/EnigmaProject/comments/91chg5/enigma_vs_oasis_labs/

lookatmegoweee. (2019). What are the shortfalls of Brave? *Reddit.* https://www.reddit.com/r/privacy/comments/9p62e4/what_are_the_shortfalls_of_brave/

meltingspark. (2019) Brave vs. Firefox data privacy. *Reddit.* https://www.reddit.com/r/privacytoolsIO/comments/a6l3lo/brave_vs_firefox_data_privacy/

MercuryWhiskey. (2019). Is Tor on the Brave browser legit? https://www.reddit.com/r/privacy/comments/afpbh7/is_tor_on_the_brave_browser_legit/

MindlessComment. (2019). Would you recommend Brave browser? *Reddit.* https://www.reddit.com/r/privacy/comments/8ur89i/would_you_recommend_brave_browser/

norflowk. (2019). Brave vs. Firefox data privacy. *Reddit.* https://www.reddit.com/r/privacytoolsIO/comments/a6l3lo/brave_vs_firefox_data_privacy/

OverallGain. (2019). Brave vs. Firefox. *Reddit.* https://www.reddit.com/r/privacy/comments/9mipm2/brave_vs_firefox/

PapaRostov8. (2018). Why I believe Civic will not succeed. *Reddit.* https://www.reddit.com/r/civicplatform/comments/7t3zei/why_i_believe_civic_will_not_succeed/

Raphty101. (2019). Brave vs. Firefox data privacy. *Reddit.* https://www.reddit.com/r/privacytoolsIO/comments/a6l3lo/brave_vs_firefox_data_privacy/

RobertBartus. (2018). Why I believe Civic will not succeed. *Reddit.* https://www.reddit.com/r/civicplatform/comments/7t3zei/why_i_believe_civic_will_not_succeed/

RoseTheFlower. (2019). Brave vs. Firefox. *Reddit.*https://www.reddit.com/r/privacy/comments/9mipm2/brave_vs_firefox/

Sapphirefragment. (2019). Brave privacy browser is whitelisting trackers of Facebook and Twitter. https://www.reddit.com/r/privacy/comments/ap8rnv/brave_privacy_browser_is_whitelistng_trackers_of/

SquirtGunKelly1. (2018). Why I believe Civic will not succeed. *Reddit.* https://www.reddit.com/r/civicplatform/comments/7t3zei/why_i_believe_civic_will_not_succeed/

StraightChemical. (2019). Brave vs. Firefox.
Reddit. https://www.reddit.com/r/privacy/comments/9mipm2/brave_vs_firefox/

Szymas255. (2019). Would you recommend Brave browser?
Reddit. https://www.reddit.com/r/privacy/comments/8ur89i/would_you_recommend_brav\e_browser/

ThriceHawk. (2019). What should I know about Brave browser?
*Reddit*https://www.reddit.com/r/privacy/comments/abri4g/what_should_i_know_about_brave_browser/

Tyler1492. (2019). Brave vs. Firefox data privacy.
Reddit. https://www.reddit.com/r/privacytoolsIO/comments/a6l3lo/brave_vs_firefox_data_privacy/

Veritasmaximuss. (2019). Is Tor on the Brave browser legit?
Reddit. https://www.reddit.com/r/privacy/comments/afpbh7/is_tor_on_the_brave_browser_legit/