Stream: Interdisciplinary Journal of Communication
2020, Vol 12(1), 70–82

http://journals.sfu.ca/stream

The social construction of blockchain privacy platforms

Jenn Mentanko
School of Communication,
Simon Fraser University

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 paper 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
online privacy, surveillance, blockchain, social construction, disruptive technology.

Corresponding Author: Jenn Mentanko – jenn_mentanko@sfu.ca

Much of the scholarship on privacy begins by acknowledging how difficult the concept is to define (Powers, 1996; Lane, 2009; Craig and Ludloff, 2011; Gellman and Dixon, 2011). It is ambiguous, abstract and can fluctuate depending on who you talk to. Also,new technology can shift the meaning of privacy, as demonstrated by Web 2.0 and the rise of social networks. Users must balance self-censorship with social sharing as social media platforms encourage us to publish the minutia of our day-to-day life. In doing so, we provide online conglomerates such as Facebook and Google with our data, which has become a valuable resource. Perhaps privacy has become so difficult to define because it stands for something outside of itself. Privacy discourse has become a symbol of resistance against the data mining activities of these major corporations. It has given governments and legal institutions the ability to create policy and regulation in an attempt to reign in the power of these major corporations, as seen in the European Union's General Data Protection Regulation (GDPR). In conjunction with law and regulation, it provides users with an ethos to reject the increasing centralization of the internet and a way to discuss privacy rights and data sovereignty on the internet. One such way users are negotiating the meaning of privacy and data sovereignty is through blockchain. Blockchain is an emerging technology that has the potential to restructure the internet into a more equal, decentralized space, harkening back to the original community-centered space of Web 1.0. This article explores the ways in which users negotiate the technical code of blockchain through privacy discourse. Using a social construction of technology (SCOT) framework, this article compares and contrasts notions of privacy between users and blockchain platforms in an attempt to understand how users negotiate online power structures through technology.

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 at the risk of revealing personal information (Clarke, 1994). Today, privacy risks are evidenced by the deluge of large-scale data breaches reported in the media such as the Equifax data breach that exposed sensitive and personal information of 147 million people and the Cambridge Analytica Scandal that affected 50 million Facebook users (Federal Trade Commission, 2020; Cadwalladr & Graham-Harrison, 2018). The Cambridge Analytica scandal was particularly salient as it demonstrated the nefarious consequences that data manipulation can have on democracy. In an attempt to reaffirm trust between corporations and users, privacy has become a buzzword in

marketing, like Apple's "Privacy, that's Iphone" campaign that was released a month after a FaceTime privacy bug was discovered (Gartenberg, 2019). While there are top-down approaches to protecting user privacy, such as company initiatives like Apple's, and the European Union's GDPR implemented in 2018, there are alternative options for users that want to take back control of their data, one of which is blockchain.

Blockchain has the potential to be a solution to the privacy problem and what it stands for. Blockchain is a decentralized ledger that verifies and stores information either publicly or privately through a peer-to-peer network, without the need for a third party intermediary. Information on the blockchain is encrypted and invariable, so no user can alter the information recorded. Blockchain is imperative in the facilitation of cryptocurrency, but has been adapted for a variety of uses including smart contracts, supply chain management, privacy and security and more. According to a systematic review on blockchain for business literature, 7% of the articles collected focused on privacy (Frizzo-Barker et al, 2019). The driving force behind blockchain platforms for privacy is data confidentiality and data sovereignty. For instance, Brave Browser, which will be discussed further, is a privacy-centric browser built on blockchain. Advertisers can only view users' data if given permission and users are rewarded with cryptocurrency if they do. The goal of this article is to understand and compare how these blockchain platforms construct privacy to the ways in which a particular group of users understand the same concept. To inform my research, I present the following research questions, followed by an exploration of theory:

1. What is the relationship between privacy discourse and technical code in reshaping power structures online?
2. Are blockchain platforms solving the privacy problem according to users?
3. What are the affordances and constraints of using blockchain for online privacy protection?

Theoretical Framework

The primary theory that informs this investigation comes from Pinch and Bijker (1984) and their analysis of economic, political and social conditions, along with motivated social agents help to shape new technology. In this article, the social

construction of technology (SCOT), works to explain how blockchain privacy platforms are developed, interpreted and perhaps altered or adapted by groups of users. SCOT comes to fruition in Pinch and Bijker's analysis of the development of the recumbent bicycle. As the recumbent bicycle emerged, different social groups had an impact on how the bicycle took shape. For instance, as the number of female riders increased, safety became a priority over speed. The definition of the recumbent bicycle eventually came to a close as core social groups agreed on an air-tired, low wheeler as it was both safe and fast. Latour (1992) further invigorates this theory of social constructivism by outlining how social values and political goals are realized through the development of technology. A vehicle for instance, alarms the driver when his or her seatbelt is not buckled, forcing the driver to comply with a set of safety standards. This way, the vehicle has safety ingrained within its architecture. Latour goes one step further than Pinch and Bijker and suggests humans and technology both have agency and exist in a constantly shifting relationship. Feenberg (1992) applies SCOT to the Internet age in his theory of technical code - the incorporation of societal demands in technology. To Feenberg, technology is not simply engineered by an isolated team of experts, rather, society aids in shaping technological design by encoding meaning within artefacts. Increasing societal representation in technological design represents democratic rationalization, an improved reflection of human needs in technology.

The development of blockchain is an example of SCOT in itself. The origins of the technology come from a person or persons under the pseudonym Satoshi Nakamoto. In the 2008 white paper, Nakamoto described a paperless currency called bitcoin that operates on a peer-to-peer network, without the need for third parties such as banks and governments. Nakamoto reframed currency, a construct deeply ingrained in modern society, to better represent social values such as decentralization, individual ownership and agency. Swartz (2018) analyzed the initial emails surrounding the launch of bitcoin and surmised that early bitcoin discussion represented anti-government and cryptopunk values made popular in the early 2000s. Bitcoin was a collective effort, an amalgamation of years of crypto discourse, which was revealed in an email connected to Nakamoto that read: "We are all Satoshi" (p. 6). The creation of bitcoin was no singular feat, rather, a representation of social values held by groups of motivated social agents.

Shortly after bitcoin disrupted the financial sector, blockchain began drawing attention of its own. There was a surge of blockchain research beginning in 2016,

with the majority centered around finance, but included other fields such as business, law, governance, healthcare, urban planning and privacy (Frizzo-Barker et al, 2019). Swan (2015), in her early commentary on blockchain, saw blockchain as a disruptive force for current Internet trends such as increasing centralization by major corporations like Google and Facebook. She described blockchain 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). Just as the bicycle was a solution for fast and safe transportation, blockchain could be a solution for increasing centralization online and diminishing data sovereignty that comes as a result. Whereas the riders negotiated safety and speed in an effort to alter the bicycle's technical code, social agents are negotiating privacy to ensure blockchain represents their social, economic and political values.

Methodology

This article employs a comparative discourse analysis to understand how a particular group of technically savvy users negotiate meaning about privacy through blockchain. I first analyze privacy discourse on three blockchain privacy platforms and compare this to how users discuss these platforms in regards to privacy protection. I chose three emerging blockchain privacy platforms to analyze: Brave, Civic and Oasis Labs. Brave is a blockchain-based browser that automatically blocks ads and trackers, providing users with ownership over their data. Additionally, if users give Brave permission to view their data, Brave rewards these users with cryptocurrency called Basic Attention Tokens (BAT) (Brave, 2019). Next, Civic is a secure identity platform that offers decentralized, verified identity solutions through blockchain. Civic aims to make online identity safe and secure while making users in control (Civic, 2019). Lastly, Oasis Labs is a privacy-focused cloud computing platform that provides users with the tools to share data without risking privacy or losing control (Oasis Labs, 2019).

Step one involved capturing the homepage and the features page of each website using Nvivo12 software. Next, I generated an initial coding scheme based on a broad definition of informational privacy: "the ability to determine for ourselves when, how, and to what extent information about us is communicated to others" (Westin, 1968, sec. 1). In step three, I used Nvivo12 to code inductively for themes, meaning, I began with privacy generally, then moved to more specific

themes of privacy such as safety and security and ad-blocking. For instance, much of the content on Brave pointed to advertisement blocking as a theme of privacy such as "Brave blocks unwanted content by default and keeps count" (Brave, 2019). Or, Civic as a "Secure Identity Platform" was coded for the theme "Safety and Security" (Civic, 2019). Overall, five themes were coded for in regards to privacy: ad-blocking, data ownership, decentralization, safety and security and general privacy.

Next, to analyze the ways in which users evaluated these platforms, I turned to two user-generated content (UGC) platforms, Reddit and Medium. I chose these two platforms because they host a thriving community of technically savvy and innovative users. Because blockchain is an emerging technology, it was important to analyze UGC platforms that were technology-focused and featured users that were motivated in testing out and evaluating blockchain platforms. Medium is a platform that publishes content from amateur and professional writers on topics of technology, science, culture and more. Writers must create a profile and submit their work to an editorial team before it is published. On the other hand, Reddit users are anonymous. Reddit is a UGC platform that is organized into communities based on interest where users can post content or leave comments. These posts and comments are ranked via the "upvote" or "downvote" button that indicates 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. Much of the content that was coded came from privacy-related subreddits such as r/privacy and r/privacytoolsIO. To search for discourse regarding Brave, Civic and Oasis Labs in conjunction with privacy, I used a private browser to Google particular search terms. Search terms included variations of "Brave, Privacy and Reddit," or "Brave, Privacy and Medium." Discourse was inductively coded into themes using Nvivo12 software. All content was from the years 2017-2019. The same rationale for themes was used when coding discourse on UGC platforms. For instance, on Medium, a user discussed Civic's identity attestation model as beneficial over centralized systems in terms of security. This discourse was coded under the theme Safety and Security." Privacy themes on Reddit and Medium included: ad-blocking, data ownership, safety and security, trust and ethics and general privacy.

Findings

This discourse analysis revealed important themes in relation to privacy and the overall ethos it represents. The coding revealed blockchain privacy platforms and this particular group of social agents have similar constructions of privacy, which bodes well for the representation of user values in its technical code. For instance, safety and security were significant themes for both parties: 68% of content on blockchain platforms and 34% on UGC platforms. Reddit users often sought recommendations for the most secure platform to use, which would turn into a discussion on the affordances and constraints of particular platforms. For instance: "This is why companies like civic are using Blockchain; because you can secure personal identity data" and

> "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 trust them to store that information" (AI-girl, 2018; chongkwongsheng, 2018).

Data ownership was also a theme shared by both blockchain platforms (10%) and users (7%). instance, Brave states: "Our servers neither see nor store your browsing data - it stays private until you delete it. Which means we won't ever sell your data to third parties" (Brave, 2019). In a Reddit discussion titled "How private is Brave Browser's privacy?" a user came to Brave's defense in regards to data ownership: "I will repeat what I said in #1, Brave does NOT collect, monitor, or store user data. Period" (10gicbear, 2018). Additionally, both blockchain platforms and UGC platforms featured ad-blocking discourse with 5% and 9%, respectively. The data comparison suggests the construction of privacy is similar in both platforms as both felt safety and security, ad-blocking, and data ownership were crucial features in the movement for online privacy.

While blockchain privacy platforms seem to encapsulate a shared privacy ethos, there is an important distinction that became apparent when comparing themes. According to this particular group of users on Reddit and Medium, trust is an important factor in the evaluation of blockchain platforms. When evaluating the affordances and constraints of a blockchain platform, users pay careful attention to the overall trustworthiness of the organization and the team behind it. According to the data, 38% of privacy discourse on Reddit and Medium involved trust and ethics,

the largest theme overall. Oftentimes, users would question the trustworthiness of the team or technology behind the blockchain platform. For instance, when evaluating Brave, users were leery of its ties to Google because it is based on the open-source chromium software: "...it just kinda scares me that it uses chrome as a base because I don't feel like you could ever truly remove everything google is hiding in there…" (Imillonario, 2018). There was also mention of the team behind Brave, particular the CEO and former Mozilla co-founder, Brendan Eich: "In addition to Brendan Eich the team has some great names with each of them being a pro in one critical feature of the project" or "brave browser is a cryptocoin-crank snake oil and this should be surprising to nobody also brendan eich is a loser" (NK, 2018; sapphirefragment, 2019). This theme suggests that when considering the viability of blockchain platforms to further the privacy movement, users take the organization and team behind the platforms into consideration as well.

Broad themes outside of privacy proved valuable to this examination as well. Findings revealed both boosters and skeptics in the evaluation of blockchain platforms. According to Everett Rogers (2003) diffusion of innovations theory, those who are more apt to adopt emerging technologies are innovators - venturesome cosmopolites that can cope with uncertainty, have the financial resources to cope with potential loss and can understand and apply a high degree of technical knowledge (p. 264). Reddit and Medium are important platforms to study in this regard as their user-base hosts a budding community of technophiles (StartEngine, 2018). By examining discourse between users, it is clear they are technically savvy and understand the significance of blockchain in the fight for overall privacy and rejection of current Internet trends such as centralization and data mining. Typically, users are optimistic about blockchain's potential, but usability issues create skepticism about the practicality of blockchain platforms. Users often expressed frustration over the beta issues that come with new technology. For instance, users became irritated when a feature failed to work properly, despite being in beta[1]: "I just checked how to install extensions on Brave. The support is 'experimental' at best. If I cared enough to deal with that, I might as well go and compile IceCat60" (a version of Firefox) (FeatheryAsshole, 2018). Even users who are enthusiastic about these innovations become exasperated at their usability issues:

[1] Beta software refers to computer software that is undergoing testing and has not yet been officially released (Tech Terms, 2013).

> "I'd use brave but the lack of sync between desktop and mobile is a large roadblock for me. I do like the idea of tokens going to the sites I'm visiting, hopefully when it's more developed I'll come back to it" (SirLambda, 2019).

While usability issues come with the territory of beta versions of emerging technologies, it seems that even innovator groups find it difficult to fully accept blockchain platforms if they do not experience ease of use. On a positive note, 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.

Conclusion

This research sought to discover how a subset of innovative users on Reddit and Medium negotiate power structures online through blockchain privacy platforms. By examining privacy discourse, we can understand how users are participating in the reimagination of the Internet's technical code. A comparative discourse analysis shows that both blockchain privacy platforms and users hold similar views on what constitutes privacy. Both blockchain platforms and users consider ad-blocking, safety and security and data ownership to be important features in overall online privacy. Where these two parties differ is in the importance users place on the trustworthiness and ethics of an organization and the team behind the platforms' development. For users to adopt blockchain platforms in the fight to reimagine the Internet's centralized architecture, users must trust the individuals behind its creation and not just the technology itself. Furthermore, usability issues can become a roadblock in the adoption of emerging technology.

Fortunately, blockchain platform developers are receptive to this feedback, and are actively working to rearrange their platform's technical code to meet the needs of its users.

References

AI-girl. (2018). *Civic competitors?*. Message posted to https://www.reddit.com/r/civicplatform/comments/7q4cfy/civic_competitors/

Berger, A. (2000). *Media and communication research methods : An introduction to qualitative and quantitative approaches*.

Berger, P., & Luckmann, T. (1967). *The social construction of reality : A treatise in the sociology of knowledge*. Anchor books.

Brave (2019). *Secure, Fast & Private Web Browser with Adblocker*. Retrieved from: https://www.brave.com

Cadwalladr, C. & Graham-Harrison, E, (2018 March 17). Revealed: 50 million Facebook Profiles harvested for Cambridge Analytica in major data breach. *The Guardian*. Retrieved from: https://www.theguardian.com

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

Civic (2019). *Civic Secure Identity Ecosystem*. Retrieved from: https://www.civic.com

Craig, T., & Ludloff, M. (2011). *Privacy and big data*. O'Reilly Media, Inc.

FeatheryAsshole. (2018). *Brave vs Firefox*. Message posted to https://www.reddit.com/r/privacy/comments/9mipm2/brave_vs_firefox

Federal Trade Commission (2018, June 18). *The Equifax Data Breach*. Retrieved from https://www.ftc.gov/equifax-data-breach

Feenberg, A. (1992). Subversive rationalization: Technology, power, and democracy, *Inquiry, 35*:3-4, 301-322,DOI: 10.1080/00201749208602296

Frizzo-Barker, Julie, Chow-White, Peter A, Adams, Philippa R, Mentanko, Jennifer, Ha, Dung, & Green, Sandy. (2020). Blockchain as a disruptive technology for business: A systematic review. *International Journal of Information Management, 51*, 102029. https://doi.org/10.1016/j.ijinfomgt.2019.10.014

Gartenberg, C. (2019, March, 14). 'Privacy Matter' in Apple's latest Iphone ad. *The Verge*. Retrieved from: https://www.theverge.com

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

Imillonario. (2018). *Brave browser*. Message posted to https://www.reddit.com/r/privacy/comments/9o6p49/brave_browser/

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

Latour, Bruno (1992). Where are the missing masses? The sociology of a few mundane artifacts. *Shaping Technology/Building society; Studies in Sociotechnical Change*, Cambridge, Massachusetts: MIT Press, pp. 225-258.

l0gicbear. (2018). *Brave browser privacy*. Message posted to https://www.reddit.com/r/privacy/comments/83sa9v/brave_browser_privacy/

McLuhan, M. (1964). *Understanding media: The extensions of man*, (2d ed). Signet.

Medium (2019). Retrieved from: https://www.medium.com

NK, G. (2018 Oct. 10). Why I am finally switching from chrome to Brave. *Medium*. Retrieved from https://www.medium.com

Oasis Labs (2019). *Unlock the potential of your data without compromising security or privacy*. Retrieved from: https://www.oasislabs.com

Pinch, Trevor J., & Bijker, Wiebe E. (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.

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

Reddit (2019). Retrieved from: https://www.reddit.com

Rogers, E. (2003). *Diffusion of innovations*, (5th ed.). Free Press.

Sapphirefragment. (2019). Brave browser is whitelisting trackers of Facebook and Twitter. Message posted to

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

SirLambda. (2019). *Brave vs. Firefox data privacy*. Message posted to https://www.reddit.com/r/privacytoolsIO/comments/a6l3lo/brave_vs_firefox_data_privacy/

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

Swan, M. (2015). Blockchain Thinking : The Brain as a Decentralized Autonomous Corporation [Commentary]. *Technology and Society Magazine, IEEE, 34*(4), 41-52.

Swartz, L. (2018). What was Bitcoin, what will it be? The techno-economic imaginaries of a new money technology. *Cultural Studies,*1-28. doi:10.1080/09502386.2017.1416420

TechTerms. (2013). Beta software. Tech Terms. https://techterms.com/definition/beta_software