Check for updates

JIT

*Research Paper*

Journal of Information Technology
1–23
© Association for Information Technology Trust 2020
Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/0268396220944406
Journals.sagepub.com/jinf
SAGE

# Those who control the code control the rules: How different perspectives of privacy are being written into the code of blockchain systems

**Robin Renwick[1] and Rob Gleasure[2]**

**Abstract**

Blockchain systems afford new privacy capabilities. This threatens to create conflict, as different social groups involved in blockchain development often disagree on which capabilities specific systems should enact. This article adopts a boundary object perspective to make sense of disagreements between collaborating social worlds. We perform a case study of privacy attitudes among collaborating actors in Monero, a cryptocurrency community that emphasises privacy and decentralisation alongside a set of values sometimes described as anti-establishment, crypto-anarchist, and/or cypherpunk. The case study performs a series of interviews with users, developers, cryptographic researchers, corporate architects, and government regulators. Three novel and important findings emerge. The first is that none of the social worlds express a desire to monitor routine transactions, despite the obvious business and tax-collection value of such data. The second is that regulators are happy to postpone active involvement, based on the flawed assumption they can impose privacy-related regulation later, once risks have become clear. Such regulation may not be possible as protocols and rulesets currently being coded into the system may be impossible to amend in the future (unless they can obtain either developer or network consensus). The third is that regulators assume methods for overseeing extraordinary transaction are necessary to avoid widespread, near-effortless money laundering. Yet, each of the other social worlds is operating under the assumption that this trade-off has already been accepted. These findings demonstrate subtle power transitions and changes in privacy attitudes that have implications for research on blockchain, management, and boundary objects in general.

**Keywords**

Blockchain, cryptocurrency, privacy, boundary objects, Monero

## Introduction

Blockchain technology emerged at the beginning of 21st century, becoming renowned for its role in enabling cryptocurrencies such as Bitcoin (Underwood, 2016; Zohar, 2015). While many view blockchain as revolutionary (Beck et al., 2017; Beck and Müller-Bloch, 2017; Elias, 2011; Garrod, 2016; Risius and Spohrer, 2017; Walsh et al., 2016; Zyskind et al., 2015), individual expectations of this revolution differ. Many anti-establishment supporters, investors, and developers perceive blockchain as affording hegemonic shift in societal and economic structures, liberating individuals from centralised state control and constant surveillance (Antonopoulos, 2016; Garrod, 2016). Others take a more ideology-light perspective, viewing the technology as a driver of innovation and a valuable source of competitive advantage for individual firms (Beck and Müller-Bloch, 2017; Li et al., 2018; Risius and Spohrer, 2017; Walsh et al., 2016). Meanwhile, regulators see the lack of control around blockchain as a potential blind spot for criminal activity such as money laundering and terrorist financing (cf. Amarasinghe et al., 2019; Bordo and Levin 2017; De Filippi, 2014; Elias, 2011; European Banking Association (EBA), 2019; Ferreira, 2020; Foley et al., 2019; Genkin et al., 2018; Goodell and Aste, 2019;

[1]Trilateral Research Ltd, UK
[2]Copenhagen Business School, Denmark

**Corresponding author:**
Robin Renwick, Trilateral Research Ltd, UK.
Email: robin.renwick@trilateralresearch.com

Gruber, 2013; Juels et al., 2016; Miller et al., 2017; Molloy, 2018; Möser et al., 2013; Rueckert, 2019; Weber et al., 2019; Zyskind et al., 2015).

These different perspectives are meaningful when one considers the range of privacy-related capabilities presented by blockchain. A central feature of these technologies is the concept of a 'distributed ledger', that is, a public record of interactions visible to all nodes on the network (Nakamoto, 2008). These ledgers have the potential to create complete reservoirs of data that could increase individual and/or corporate accountability (see Anderson et al., 2018; De Filippi, 2014; Goodell and Aste, 2019; Karlstrøm, 2014; Politou et al., 2019; Rieger et al., 2019; Weber et al., 2019). Yet, this distributed structure also removes the need for centralised oversight and governance, creating new opportunities for anonymity at the interface between different digital and physical systems (De Filippi, 2016; Dierksmeier and Seele, 2018). The range of diverging possibilities threatens to create tension among collaborating social worlds, each of whom is contributing to the development of blockchain, either directly (as is the case for academic researchers and protocol developers) or indirectly (as is the case for investors and regulators). Yet, existing research has done little to pre-empt or manage these tensions.

The objective of this article is therefore *to explore how different attitudes to privacy create tension in the development of blockchain technologies*. The next section provides a brief overview of blockchain technologies, including the contextual origin of the technologies and the proposed motives for their creation. Following this, we present a boundary object (BO; Huvila et al., 2016; Star and Griesemer, 1989) perspective that treats the development of blockchain as a community-spanning system of behaviours, operating within and across distinct techno-political social worlds (De Domenico and Baronchelli, 2019; Gikay and Stanescu, 2019; Golumbia, 2015). The research method is presented which details how qualitative data are gathered and analysed from five key social worlds, specifically users, cryptographic researchers, protocol developers, corporate architects, and regulators. We then present findings, which identify and differentiate various consensus-building (robust) commonalities, non-harmful (complacent) differences, and more problematic (internecine) differences. Finally, we discuss the contributions and implications from the study.

## The emergence of blockchain technologies and cryptocurrencies

An anonymous actor or group called Satoshi Nakamoto (2008) proposed the decentralised peer-to-peer cryptocurrency Bitcoin and launched its genesis block in 2009. Bitcoin was built on prior work by several technologists, including many involved in the cypherpunk and/or crypto-anarchist movements of the late 20th century (De Filippi, 2014; Karlstrøm, 2014; Narayanan and Clark, 2017). At the heart of Bitcoin was the idea that read permissions are granted to participants according to a predetermined protocol ruleset, while write authorisation is determined through a protocol dependent and network agreed consensus mechanism (Zohar, 2015). This removed the need for trusted intermediaries and thus centralised ownership (Nakamoto, 2008).

Blockchain technologies have since evolved from anti-establishment digital currencies operating outside mainstream financial systems to a 'revolutionary' technological blueprint for distributed computing architectures, such as Ethereum (Buterin, 2014; Szabo, 1994). A variety of communities are attempting to use blockchain to redesign data structures in fields such as finance, politics, supply chain management, identity management, commodities markets, and capital markets, to name a few (Beck et al., 2017; Beck and Müller-Bloch, 2017; Chong et al., 2019; Li et al., 2018). Indeed, blockchain has become a marketing buzzword as effective in the boardroom as it is on the sales floor (Risius and Spohrer, 2017; Rossi et al., 2019; Walsh et al., 2016). Some have even called for the abandonment of the term 'blockchain' altogether, in favour of the more neutral 'distributed ledger technology' (cf. Olnes et al., 2016) given overuse and marketing hype has drowned the term in a 'hyperglyphic' gloop of semantic satiation (Carter, 2018).

The pragmatic business-driven adoption of blockchain does not mean the dissent-based socio-technical origins of the technologies have disappeared. Blockchain technologies were created as artefacts of resistance (Antonopoulos, 2016; Atzori, 2015; Currie et al., 2018; De Filippi, 2014, 2016; Foley et al., 2019; Rueckert, 2019), tools affording freedom from archaic, hierarchical, centralised, politicised, and ultimately flawed systems (Markey-Towler, 2018). The genesis block of Bitcoin contains a specific message, an indelible digital carving; an ode to its proposed purpose: 'The Times 03/Jan/2009 Chancellor on brink of second bailout for banks' (Singh and Singh, 2016: 464). The intended message is seen as marker for the proposed macro-economic impact the newly developed self-sovereign financial system initiated: a monetary system divorced from the perceived politicked mis-management of the incumbent (Maurer et al., 2013). This countercultural interest remains (De Filippi, 2014; Garrod, 2016; Markey-Towler, 2018), even if it has been diluted by the arrival of more mainstream business perspectives. Thus, at least two conflicting value systems appear to be working together on revolutionary blockchain technologies with the diverging goals of reinvigorating and circumventing large existing institutions.

## Privacy and the regulation of emerging technologies

Concerns over privacy are common when discussing emerging technologies, as digital systems often integrate

and exchange personal and/or sensitive information. Many of these concerns transcend specific technologies, instead focusing on the increasing entanglement of analogue and digital lives and the need to protect against unwanted encroachment by third parties into the latter (see Belanger and Crossler, 2011; Davison, 2012; De Filippi, 2016; Schultze and Mason, 2012; Smith et al., 2011; Zuboff, 2015; Zyskind et al., 2015, among others). Other concerns are directed towards specific technologies or trends, such as the adoption of electronic health records (Angst and Agarwal, 2009), employee monitoring (Moore, 2000), open government data (Janssen and van den Hoven, 2015), the Internet of things (e.g. Roman et al., 2013), or indeed blockchain (Bonneau et al., 2015; Chanson et al., 2019; Gozman et al., 2019; Zhang and Liu, 2019).

The obvious solution to these concerns is to regulate information privacy, yet at least four factors complicate attempts to design effective legislation. First, defining and measuring privacy is not straightforward. There are many contrasting definitions, and each lend themselves to competing measurement proxies (Belanger and Crossler, 2011; Finn et al., 2013; Moore, 2008; Pavlou, 2011; Ryngaert and Taylor, 2020; Smith et al., 2011; Van Den Hoven, 2008). Second, many individuals are willing to concede privacy as part of an economic exchange for products and services (Acquisti et al., 2016; Awad and Krishnan, 2006; Posner, 1981; Sutanto et al., 2013). This makes it difficult to define what is acceptable, given this may vary based on personal perceptions of value and personal willingness to exchange long-term costs against short-term gains (Acquisti and Grossklags, 2005). Third, individuals' need to protect personal information varies by country, as do attitudes towards the different public and private institutions seeking that information (Morey et al., 2015). For blockchain-based systems, this creates a close link between privacy concerns and perceptions of specific public overseers for example (Gozman et al., 2019). This further complicates efforts to generalise acceptable levels of privacy threat across different users and contexts. Fourth, designing regulation is challenging when technologies are still maturing, as the nature and scale of risks are typically unclear, and governments do not want to act prematurely and impede innovation (Ferreira, 2020; Hamburg, 2012; Kiviat, 2015; Roca et al., 2017). This reticence by governments could open the door for other regulators, but it is not clear which other entities, if any, have the right or means to impose regulation. As Julia Black (2002) notes, 'Once regulation is not seen as something tied exclusively or even predominantly to the state, it is not clear where its boundaries lie either as a social practice, or an academic discipline' (p. 1). Thus, the trend in recent decades has been to avoid government regulation in the early stages of technologies, instead allowing multiple parties from different fields to define the use of those technologies, the risks, and the acceptable trade-offs between value, privacy, and other social and individual costs (cf. Ashford, 2002; Black and Anderson, 2013; Irwin and Vergragt, 1989; Roca et al., 2017). Inevitably, avenues appear for ideologies to be built into technological structures, absent from regulatory oversight, as entities weave politicised positions directly, or indirectly, into softwares (Brunton and Nissenbaum, 2015; De Filippi, 2014, 2016; Lessig, 1999, 2003, 2009).

From the perspective of blockchain technology, efforts have been made to standardise design through specific bodies, at both international and national level. Technical reports such as ISO/TR 23244:2020 (International Standards Authority, ISO, 2020) provide recommended minimum considerations for blockchain system privacy, while national bodies such as the German Standards Authority propose a distinct design methodology: DIN SPEC 4997 (German Standards Authority, DIN, 2020), which directly addresses inherent tradeoffs at the intersection of cryptography, privacy, and existing regulatory grey-areas (cf. European Parliamentary Research Service (EPRS), 2019].

## Social worlds and BOs

Finding a shared view on privacy, and the way emerging technologies may affect privacy affordances, requires multiple parties negotiate what is acceptable. Yet, the alignment of contextual incentives among these parties is questionable. For example, organisations are naturally inclined to seek user data as a source of value, even at the expense of privacy (Morey et al., 2015). Similarly, technologists and researchers may overestimate the value of new technologies and downplay the dangers (Baskerville and Myers, 2009; Zuboff, 2015).

The systems that allow heterogeneous actors/groups to come together and share resources and practices can been described as 'boundary objects' (Baggio et al., 2015; Barrett and Oborn, 2010; Burnett et al., 2009; Star and Griesemer, 1989). A BO is described as an abstract or physical artefact existing 'in the liminal spaces between adjacent communities of people' (Huvila et al., 2016: 1) or, alternatively, as 'things that exist at junctures where varied social worlds meet in an area of mutual concern' (Clarke and Star, 2008: 121). The concept emerged as sociologists attempted to understand cooperative design processes that took place between actors in different 'social worlds', that is, groups that would otherwise have limited direct interaction (Huvila et al., 2016; Jacob, 2005). Researchers found amalgamated groups of individuals usually work towards a common goal without necessarily sharing consensus on project specifics (Kaplan, 2017; Star and Griesemer, 1989). Divergences in these groups do not necessarily remove the potential for projects to be successful for all parties. Yet, this required different collaborating social worlds establish some common mode of operation, enacted through effective communication, cooperation, and, most importantly, the reconciliation of differences as and when they emerge.

Such reconciliation requires effort by all involved – due mainly to internecine divergences of opinion, or ideology that manifest throughout the project timeline (Ciborra and Andreu, 2001; Huvila et al., 2016; Kaplan, 2017; Star and Griesemer, 1989).

Assuming divergences can be managed; BOs may be formed from a wide spectrum of tangible, intangible, physical, and abstract ideas and resources. Thus, researchers have used the concept of BOs to discuss topics as varied as archival standards (Yakel, 2004), cancer (Fujimura, 1992), gender (Burnett et al., 2009), resilience (Baggio et al. 2015), musical scores (Winget, 2008), medicine (Frost et al., 2002), water (Carroll, 2012), room/space (Jornet and Steier, 2015), simulation games (Van Pelt et al., 2014), and even disciplinary boundaries for IS research (Winter and Butler, 2011).

Many IS scholars have used the BO perspective to inform system design (e.g. Bergman et al., 2007; Gal et al. 2008; Jacob, 2005). This allows IS scholars to engage with different motives and understandings of a system, hence helping to understand if and how a BO can sustain the collective purposes of those involved (cf. Doolin and McLeod, 2012; Levina and Vaast, 2005).

## A BO view of privacy attitudes and blockchain development

The analysis and understanding of collaborating social worlds' attitudes to privacy is key to the evolution of blockchain technologies. This is because hidden divergences within such social worlds will likely give rise to tensions that break down collaborations as they mature. Evidence of such breakdowns have already been observed as 'contentious forks' within the Bitcoin community, where deep unforeseen conceptual, abstract, and practical splits in the community force actors to split projects into competing systems (Andersen et al. 2018; De Filippi and Loveluck, 2016; Tschorsch and Scheuermann, 2016). These splits can create significant setbacks for the development of blockchain systems, given the need to establish critical mass if they are to enact systemic change. This is true of cryptocurrencies but also other blockchain applications, such as logistic systems (Jensen et al., 2019) and second-hand markets (Zavolokina et al., 2020). Thus, the earlier problematic divergences can be detected, the earlier misaligned collaborators can negotiate changes, or adjust or cease their involvement where appropriate.

Placing privacy at the centre of this exploration makes sense, given the centrality of privacy-related motivations for many collaborators in blockchain projects (Chong et al., 2019; Gozman et al., 2019; Mattke et al., 2019), and the seemingly incompatible privacy-related ideologies that may be involved (Rieger et al., 2019). Identifying divergences requires modelling different social worlds, which then allows the intersection of collaborating groups to be better understood (Strauss, 1978). This is because consensus is often internalised through sensemaking from external interaction with others (Star, 1998). Thus, the edges of boundaries are often the site for 'intense controversy and competition for the power to define [BOs]' (Clarke and Star, 2008: 121).

## Method

### *A single case approach*

This study adopts a case-study (Eisenhardt, 1989) approach, using the BO perspective as a sensitising lens. Case studies are suitable when exploring loosely bounded or rapidly changing environments (Feagin et al., 1991; Noor, 2008; Sarker et al., 2013). This is because the adaptability of data gathering and analysis in case studies encourages researchers to dig deeper into the underlying causes of phenomena, hence helping them to answer 'why' and 'how' questions (Sarker et al., 2013).

This study focused on the Monero cryptocurrency platform. Monero is a privacy-focused proof of work-based cryptocurrency, secured with the CPU optimised RandomX algorithm, designed by the community to specifically disincentivise deployment of application-specific integrated circuit (ASIC)–based cryptocurrency mining hardware. This lowers the barrier to entry into profitable cryptocurrency mining for mainstream users, which is viewed by the Monero development community as integral for maintaining decentralisation in the Monero mining ecosystem (Monero, 2019). The Monero protocol has undergone several development improvements since its initial emergence. Originally, it was established in 2014 as a rebranding of BitMonero, itself a codebase fork of the original implementation of the anonymously authored CryptoNote protocol whitepaper named ByteCoin (Buntinx, 2017). Since 2014, Monero has established itself as the most widely adopted privacy-focused blockchain implementations, respected for its strong commitment to open-source methods, its bespoke cryptographic schemes, and referenced within a number of research publications, policy advisories, and standardisation technical reports concerning information security, data protection, and the development of central bank digital currencies (cf. European Central Bank (ECB), 2020; EPRS, 2019; Federal Office, 2019; German Standards Authority, DIN, 2020; International Standards Authority, ISO, 2020; WEF, 2020). At the time of writing (June 2020), the network has a market capitalisation value of $1.14 billion, a current unit token price of $64.63, and a 24-h trade volume of $61 million, residing in 18th place, as per market capitalisation rankings at CoinRanking (2020). This makes Monero the highest ranked privacy-preserving blockchain network.

We adopted a single-case research design for two reasons. The first was opportunistic (cf. Patton, 1990). The lead researcher in this study possessed established relationships

with members of the Monero community (developers, users, and corporate architects) due to a long-term personal interest and involvement in the project. This natural build-up of trust and mutual understanding presented opportunities for research access and frankness of discussion that otherwise may have been challenging to obtain. Coupled with this, the authors have established relationships with large financial services organisations and national regulators. This created a unique combination of (1) empirical reach and (2) moral obligation for critical balance.

The second reason for the single-case design is the tendency for single-case approaches to boost researchers' immersion and allow the data to 'talk', hence increasing the sensitivity to emerging variables, or observations, that conflict with expectations (Flyvbjerg, 2006). A single-case analysis also helps the researchers to provide a less-reductive description of the phenomena under study (Darke et al., 1998; Patton, 1990). Thus, the ability to generate value from the serendipitous circumstances and opportune sampling were brought into focus by the single-case approach.

The authors initially identified six social worlds, based on based on explicit and implicit description in existing literature. These were (1) users, (2) protocol developers, (3) researchers, (4) corporate architects, (5) regulators, and (6) Monero miners. Feedback from participants confirmed that the first five groups represented the social worlds actively participating in Monero development. The third group 'researchers' were further narrowed into the social world of 'cryptographic researchers', as these were the only researchers we observed directly contributing to Monero development.

The sixth group, Monero miners, described those individuals or groups that run software to validate third-party[1] Monero transactions in exchange for newly minted 'coins'. Preliminary exploration of these groups suggested they divided into two types. The first type consists of casual or hobbyist miners who experiment with mining for curiosity, or to top-up their wallets in a 'trustless' manner. These casual miners were almost impossible to differentiate from general users, many of whom experiment with mining as a type of moral-obligation for decentralisation and network security, leveraged by the CPU friendly RandomX algorithm deployed on the Monero network. The second type are professional miners that operate mining pools, data centres, and/or malware that secretly run mining software on host machines, or Internet browser-based mining 'plugins' in leu of standard ad-based webpage revenue (cf. Mondschein, 2020). These individuals are often operating in isolated, socio-politically complex Monero-related contexts, meaning they have little impact on the development activities of the other five social worlds. Equally importantly, the short-term economic motivations of large-scale professional mining create a potential for behaviours the research team deemed ethically and legally problematic. Thus, we merged casual miners into the broader social world of 'users' and determined that professional miners were out of scope.

## *Data gathering*

The primary means of data gathering was a series of interviews conducted from May 2018 to March 2020. Other forms of participation were also used to generate a sense of context and acclimate the various norms of different social worlds. This included attending multiple international academic and industry-focused blockchain-based events in Europe, North America, and East Asia. These events helped the authors sensitise preliminary concepts and triangulate or challenge emerging themes throughout the analysis. The close personal interest in the project presented a possible bias, which we managed in three ways. First, one researcher was actively involved in each interview, while the other only reviewed transcripts and participated in analysis and coding. Second, both authors performed coding independently, with differences identified and reconciled as they emerged. Third, both authors regularly discussed emerging findings with researchers and practitioners involved with different cryptocurrencies. This allowed us to challenge our assumptions and interpretations throughout the study.

A minimum of two interviews were conducted from each of the social worlds. This included six regulators and policy advisors from four different public institutions in Northern Europe and North America, four corporate architects from four companies in Northern Europe and Asia, two of which were drawn from Monero specific businesses, and one from a large mainstream financial services provider. It also included four users, two developers, and two cryptographic researchers, approached through cryptocurrency events, or drawn directly from the Monero developer and research community. Five of these interviewees participated in a second round of data gathering, where we 'back-tracked' (Gioia et al., 2013) to vent findings and return to topics of interest that emerged after the initial interview. This resulted in a final set of 22 interviews. At this point, theorising plateaued and sampling ceased. Interviews used different communication media depending on interviewee preference. Ten participants participated through text-based media: Wire,[2] Telegram,[3] and Internet Relay Chat[4] (IRC). We did this to reassure privacy-sensitive interviewees who wanted to maintain pseudonymity. The seven remaining participants were interviewed in person or using voice-based interfaces.[5]

Data gathering and analysis used techniques from grounded theory (GT), in particular the pragmatic coding and analysis techniques (open, axial, and selective) proposed by Strauss and Corbin (1990). This study uses these techniques to expand upon existing concepts identified in the BO literature. Recent techno-centric formalizations of BOs distil the framework down to three distinct areas of concern: (1) concepts, (2) artefacts, and (3) practices (Huvila

**Table 1.** Subcategories of blockchain-related privacy concepts and differing attitudes among social worlds.

| | Users | Protocol developers | Regulators | Corporate architects | Cryptographic researchers |
|---|---|---|---|---|---|
| Right to privacy | + | + | + | + | + |
| Decentralised revolution | + | + | + | + | + |
| Government development involvement | – | – | + | – | * |

View as positive = +; view as negative = –; view as neutral = *.

et al., 2016). We adopted this preliminary set of high-level categories as a starting point for questioning, translation, and interpretation. Thus, BO provided a sensitising tool or 'frame' for the analysis (cf. Blumer, 1954; Clarke, 2003), affording a level of theoretical persuasion, that is, a vocabulary to understanding complex systems; a level of enquiry within, and into, research comprised of social-actor interactions.

### *Coding and analysis*

Interviews were collated and transcribed, then analysed using a combination of open, axial, and selective coding (Corbin and Strauss, 1990; Matavire and Brown, 2013; Strauss and Corbin, 1990). We used these techniques to help identify patterns in the data from which categories could be discovered, refined, or abandoned, and overarching theory could be built. This approach allowed us to maintain an exploratory approach during analysis and avoid prematurely narrowing into any specific privacy concepts in existing privacy literature. Such use of open, axial, and selective coding to expand upon high-level preliminary theorising is common (Matavire and Brown, 2013; Thornberg, 2012), even though these techniques were originally developed to support 'grounded theory' approaches (see Charmaz, 2000; Urquhart et al., 2010).

We used repeated and exhaustive reading of the data in open coding to identify different possible sub-categories of privacy-related concepts, artefacts, and practices. Axial coding continuously compared emerging sub-categories and further examined whether and how each sub-category manifested for each of the five social worlds. This created a comparative mapping that ultimately determined whether each sub-category was considered as consensus-building (robust), harmless diverging (complacent), or harmfully diverging (internecine). Selective coding then looked for specific instances of data that could test and refine solidifying categories, sub-categories, and comparative mappings. This constant iterative coding adds validity and reliability to the analysis and thus the emergent theory (Denzin and Lincoln, 2000).

With the final set of categories and sub-categories defined, we characterised interviewees according to their attitudes to each sub-category of privacy. Interviewees were characterised as positive (+) if they felt this sub-category was important, negative (–) if they felt it was unimportant, or neutral (*) if they were unsure or indifferent. We then aggregated individual attitudes within each social world, noting differences, and began comparing attitudes across social worlds. Converging attitudes across social worlds were considered 'robust', while diverging attitudes were viewed as 'plastic', with further differentiation as either 'complacent' (harmless) or 'internecine' (harmful).

## Findings

### *Privacy-related concepts for blockchain technologies*

This category contains three sub-categories, summarized in Tables 1 and 2.

*Right to privacy.* Each social world viewed information privacy as an area in which blockchain might be used for the benefit of society. Each world also agreed this right to privacy was something for which blockchain may play an important role. Where disagreement existed, it concerned the meaning of privacy and who should protect it. These disagreements are not viewed as incendiary, neither does any individual perspective appear to contradict the range found in privacy literature (cf. Acquisti et al., 2015; Belanger and Crossler, 2011; Belanger and Xu, 2015; Brunton and Nissenbaum, 2015; Moore, 2008; Nissenbaum, 2004; Pavlou, 2011; Smith et al., 2011). Variance nonetheless exists with respect to the priority of privacy protection relative to other concerns, the reason for this importance, and who is responsible for privacy protection (state or system).

The most internally consistent social world for right to privacy is that of users. Users have almost complete agreement on the right to privacy, and the affordances of blockchain technology for privacy preservation. Interviewees perceive threats to privacy as having different origins, for example, some are concerned about 'unchecked governments', others on social norms, while others focus on business and 'a couple of bad actors'. However, these differences do not appear of consequence.

Other social worlds present similar perspectives, though the emphasis moves away from 'techno-political' leanings into more practical aspects of functional privacy and data security. For example, while corporate architects view privacy as paramount, this is less for personal reasons and more for fair and functioning economic markets. Some

further noted the value that consumers increasingly place on privacy, creating a service-level commercial incentive for privacy in the marketplace.

The social world of the cryptographic researchers emphasises the functional and mathematical challenges of privacy, and the need to ensure cryptography implemented into the protocols is both secure and 'fit-for-purpose'. Their perspective is firmly grounded in the importance of maintaining the ability to transfer information (regardless of context) from one party to another, securely and privately. Political leanings do exist for Cryptographic Researcher#2, but these leanings are secondary to the belief in functionally operating cryptography, ensuring a baseline level of information privacy for society – especially from within the context of blockchain systems.

Regulators also treat the consideration of right to privacy as an important concern for them and others. The interviewees were quick to acknowledge that information privacy is a major ethical and practical concern for modern society and that blockchain technology could in some way act as a resistance technology to the gradual erosion that has been occurring. Interestingly, several spoke directly of personal experience and referenced examples from their daily life to illustrate the need for privacy, not only in financial transactions but also more broadly. They also all confirmed the obligation on regulators to protect the consumer; to provide the important regulatory oversight to ensure players in the market maintain fairness and lawfulness as they engage in business. The view that market-led demand for enhanced privacy preserving solutions was integral to ensuring the maintenance of this right was also communicated. Thus, the right to privacy is a robust concept. It remains solid across boundaries, without any concrete points of divergence (Table 1).

*Decentralised revolution.* All social worlds agreed that blockchain systems afford fundamental and systemic change in how information, data, financial systems, and value networks operate and are organised. However, some viewed this more as a change in the financial system, while others viewed it as a change in the structure of government and society.

Users and protocol developers put most emphasis on the importance and impact of a larger social 'revolution'. These social worlds felt technologies could fundamentally alter the relationship between state and civilian. Several of these individuals presented a 'crypto-anarchist' perspective, which tied the technology closely to their own socio-political views. For these individuals, the very essence of blockchain was to devalue the presence of bureaucracy and 'rule-makers' in society, by facilitating a slight shift towards algorithmic-based governance mechanisms.

Less political views were observed among regulators and corporate architects. These individuals viewed the 'revolution' at a practice level, rather than a value level. This meant new networks, new assets, new businesses, new markets, and new instruments for collaboration and exchange, but not necessarily radically new relationships between individuals, businesses, and government. This social world was also more sceptical as regards the overall potential of blockchain for social good. Instead, individuals tended more towards the idea that blockchain, as with many new technologies, would advantage some people/businesses and disadvantage others. This was especially the case for the regulators, who were experienced enough to realise that blockchain-based payment systems were ultimately just an example of the continued evolution of payments systems technology, an evolution that is predominantly always 'market-led'.

This means that while there is congruence among all worlds that some level of 'change' will be affected, especially with respect to how society, networks, financial systems, information and data systems will operate in the 21st century – divergences exist regarding the depth and scope of that change. These differences do not appear to create any tensions between the different social worlds, as each group seems content to progress the technology under the assumption the depth and scope of change will resolve itself over time. Thus, we view *decentralised revolution* as plastic but complacent.

*Government development involvement.* The role of government in the development of blockchain technology presented the third and final recurring privacy-related concept. It is perhaps unsurprising, given the varying motives within and across social worlds, that perspectives also vary on government development involvement. The least interested group were the cryptographic researchers, for whom the presence or absence of government development involvement was less important than the shared commitment to quality and information-sharing among collaborating worlds. However, they did note that regulators and state actors should not have special rights to decide what gets implemented or not. Rather, different social worlds should make decisions collectively based on 'what makes sense'.

The users, corporate architects, and protocol developers felt that government and regulators should remain separate from development, regardless of whether they wished to participate or not. For protocol developers and corporate architects, this was typically because these systems were intended to operate without need for government oversight. Hence, government participation was unnecessary and likely to confuse the process. Interviewees argued there was no need for the 'special role' played by government. This was not overtly shaped by hostility towards government entities – one protocol developer even noted that many state bodies are pro-privacy. Neither was there any sense that the need for government involvement was likely to change in the future, unless some major systemic flaws were discovered or 'folks are being swindled'.

Regulators have a predictably different view, arguing that while they have no present appetite to become involved in

**Table 2.** Examples of selective coding for privacy-related concepts for blockchain.

| Category | Sub-category | Social world | Illustrative extracts |
|---|---|---|---|
| Privacy-related concepts for blockchain technologies | Right to privacy | Users | 'As long as people live in fear of being persecuted for who they are or what they believe, then i think privacy is an absolute must'. (User# 2)<br>'. . . in societies with large bureaucracies that encourage (directly or subtly) extreme conformity, i think that privacy is necessary [as] a check to allow people to experiment and thus to allow society at large to grow'. (User#3) |
| | | Corporate architects | '. . . financial privacy is paramount to everyone . . . Knowing someone's financial information can give you huge advantages'. (Corporate architect#1)<br>'Many business opportunities, technological [advancements] and regulatory/social questions will revolve around privacy'. (Corporate architect#2)<br>'I think [privacy] . . . is definitely one of the top three considerations in anything we do'. (Corporate Architect#3) |
| | | Crypto. researchers | 'I am of the opinion that the ability to keep secrets and communicate safely are fundamentally important, and using cryptography to allow these things is important'. (Crypto. Researcher#1)<br>'I believe that there are people in the world right now [whose] safety could be guaranteed if they were granted financial privacy, and I believe projects like Monero are doing the work of the angels in that regard'. (Crypto. Researcher#2) |
| | | Regulators | 'From a personal perspective I would agree completely . . . I think there are huge data issues, privacy issues, not just in relation to banking or finance, I would put it much more broadly than that'. (Reg.#1)<br>'I'm increasingly concerned about privacy. You know, whenever you go online, you leave your trail. We all know Facebook, Google . . . They all have tracers and trackers'. (Reg.#4) |
| Privacy-related concepts for blockchain technologies | Decentralised revolution | Users | 'blockchains . . . are a necessary check against central authorities getting too strong'. (User#3)<br>'I decided to involve myself with decentralized blockchain technologies and communities because I believe people should have an option to the already established system . . . provide society with an alternative financial system that doesn't depend on the current system and its rule-makers/players'. (User#2)<br>'I have family and friends around the world, some of them live under government regimes that are less than friendly. The ability to get money to these people (or from them) without permission, intervention, or snooping oversight is a big deal for me'. (User# 4) |
| | | Corporate architects | '. . . this sort of technology is very important to decentralize transferrable information property, such as money and securities'. (Corporate architect #1)<br>'So blockchain, we see it really on two levels. one is the architectural back end technology, and the other is the creation of a new type of distributed distance model with all the elements that come with it. The creation of the network, the creation of native assets, the creation of new type of cash, a new type of money, new instruments, new assets and how that evolves. So, these are the few angles that we see blockchain from the market and the financial space'. (Corp. Architect#2) |

*(Continued)*

**Table 2.** (Continued)

| Category | Sub-category | Social world | Illustrative extracts |
|---|---|---|---|
| | | Protocol developers | 'I see the move in money from no ledger (cash, bearer instruments) to centralized ledgers (credit, debit, bank payments) to decentralized ledgers (blockchain based cryptocurrency) to be driven primarily by technological change . . .' (Protocol Developer#1)<br>'It's just the way they're [governments] constantly trying to increase control over people that's just ethically and morally wrong'. (Protocol developer#2) |
| | | Regulators | 'I am really excited about it; I am really interested in blockchain. I think it's going to be much bigger than it is today'. (Reg.#1)<br>'Payment systems as a whole are going through big changes right now, and some of those changes are letting new players come in and do payments that weren't able to do it before . . . Banks effectively had a monopoly over retail payments, and that monopoly is being hacked away . . .' (Reg.#3)<br>'If cash really disappears, then two people can't interact without involving a third party on commercial terms . . . do we, as a society have an obligation to provide something that enables interaction that does not mean we need to purchase something from a third party?' (Reg.#5) |
| Privacy-related concepts for blockchain technologies | Government development involvement | Users | 'I don't think governments should play a role at all. See, the "rules" in a decentralized blockchain are mostly mathematical rules – which could be interpreted by amoral rules and this is good when you're talking about a financial system. You can't trust that humans will always behave in the interest of everyone and people will do things for their own interest. You can't have the risk for someone with bad intentions or self-interest to have a role in creating rules. These should be mathematical'. (User#2) |
| | | Protocol developers | 'I do not see much impact on government'. (Protocol Developer#1)<br>'I think I'd be (1) surprised, (2) apprehensive, (3) depending on what they [governments] change, possibly a lot of other feelings:) You never know. Some government affiliated [organisations] are pro privacy, like the information commissioner's office. But I wouldn't expect them to contribute unless they want to get sacked, heh'. (Protocol Developer#2) |
| | | Cryptographic researchers | 'Good research can come from anywhere: academia, government, business. Modern scientific research, for example, often depends heavily on collaboration from all of these types of entities'. (Crypto. Researcher#1)<br>'A government is free to fork an open-source project if their development is in line with the license; that's the entire point of open source'. (Crypto. researcher#1)<br>'. . . I think governments should feel free to participate in the discussions involving pull requests [changes to protocol code]. but that a government agency is the one making the request should have no bearing on the decision to implement or not, if that makes sense'. (Crypto. Researcher#2) |
| | | Regulators | 'it's important to understand I think, a lot of regulations are made too quick in general. So, the first point would be definitely to understand how it works, what is it? What kind of species is blockchain when it comes to the financial services?' (Reg.#5)<br>'. . . politicians and governments tend to react to what comes at them from below. They tend not to lead, they tend to follow, to put the finger in the dam once the hole has appeared. That is very much a personal view. Again, I don't see governments leading on this kind of thing. I would see them generally probably as more reactive to it than pre-emptive if I can put it that way'. (Reg.#1) |

**Table 3.** Enactment of blockchain-related resources with respect to privacy values.

| | Users | Protocol developers | Regulators | Corporate architects | Cryptographic researchers |
|---|---|---|---|---|---|
| Existing development-level resources | * | + | * | + | + |
| Existing market level resources | + | * | + | + | * |

View as positive = +; view as negative = –; view as neutral = *.

low-level development activities, they may need to step in later. Regulators highlighted the need to align blockchain-based systems with wider social environments. They referenced existing financial regulation impacting on cryptocurrencies (cf. 5th Anti-Money Laundering Directive (AMLD5); Financial Action Task Force (FATF); Revised Payment Services Directive (PSD2)], suggesting blockchain-based systems are simply a new form of payment system that must be allowed to grow before they can be understood and evaluated. Once the social and economic implications of blockchain are clearer, regulators must react and ensure individuals and organisations are using systems responsibly, with the role of the government to ultimately ensure that (1) necessary safety mechanisms are in place should payments systems 'go wrong', and (2) ground rules are in place so that competing systems can interact fairly.

This view that government development involvement should only occur once technologies have matured was complicated by assertions from members of the technically minded social worlds that the passage of time made government development involvement impossible. Instead, regulators will be forced to regulate surrounding systems and the entities using the cryptocurrencies:

> They [governments] can't stop people from using these currencies [digital private currencies]. Eventually, I believe, when the cash of the information age crystalizes, people will switch to it. It just makes economic sense. Why have a currency that needs to work through banks and other productivity hogs in addition to have your money lose 3% of its value every year when I can send you money instantly, quickly and my money doesn't lose its value? (Corporate Architect # 1)

> Most networks will be able to self-regulate. That is after all the whole point . . . We must keep in mind that the protocols are created. Most essentially fail and become insignificant. The handful that become something require a significant economic and technical acceptance. Even if there is disagreement, it gets resolved in a ledger fork and the market picks the winner. I see the role of governments here more in regulating the service providers rather than the crypto currency itself. (Protocol Developer # 1)

> If they [governments] can't regulate the institution [due to the decentralised property], and they can't in this case, they can always make it impossible for the institution to operate because . . . Bitcoin doesn't work, at least for the foreseeable future, unless it has links back into the regular payment systems, and governments can sever those links. (Regulator # 3)

Varying perspectives among social worlds is attributable partly to the multi-purpose affordances of blockchain technology. On one hand, blockchain offers efficiency when creating and securing data, financial or otherwise. On the other hand, it affords a radically different system of exchange for which no one entity has authority. Separating these affordances does not appear straightforward, neither does it appear to be a priority for many individuals and institutions participating in the development of blockchain technologies. Whatever the outcome, the use of the technology will not fulfil the expectations of some social world. Thus, we consider *government development involvement* plastic and internecine (Table 1).

## *Privacy-related resources for blockchain technologies*

This category contains two sub-categories, summarized in Tables 3 and 4.

*Existing development-level resources.* One of the sub-categories that attracted significant attention among interviewees was the actual technical resources used in Monero to enable privacy. However, these resources were not of interest to all social worlds. Perhaps predictably, users and regulators, that is, the social worlds that were less involved in the actual coding of blockchain systems, showed limited interest in the specific privacy-related resources used for development. More technically knowledgeable social worlds, that is, the protocol developers and the cryptographic researchers, tended to be more aware of these resources. Cryptographic researchers were keen to discuss the cryptographic primitives underlying the Monero code, as well as the value of practical project management tools and code versioning software. These demonstrated little or no disagreement, presumably because such disagreements had already been resolved as part of ongoing larger collaboration activities (Table 3).

Corporate architects were also quick to discuss these resources, though their interest focused less on mathematical and project management resources and more on the accommodating software platforms and standards. These platforms and standards were often not blockchain-specific, instead representing the interface between blockchain systems and established tools such as programming languages and operating systems. Those blockchain-specific resources that were discussed tended to be the platforms and packages that provided the base for subsequent development, for example, 'official' wallet software, and open source

**Table 4.** Examples of selective coding for privacy-related resources for blockchain.

| Category | Sub-category | Soc. world | Illustrative extracts |
|---|---|---|---|
| Privacy-related resources for blockchain | Existing development-level resources | Corporate architects | '. . . the Monero protocol, the Bitcoin protocol. Their "official" wallet software. Python, C++. Hardware wallets. Encryption tools. Linux. IRC also for most communication things. Slack for blockchain professional stuff'. (Corp. Architect # 2)<br>'We have been doing due diligence on any other blockchain and any other really start-up that have been coming up with their own solutions. Now I think the solutions are really Fabric being one, two Corda, three any Ethereum based solution that could be Theamatics, that could be Ethereum itself, or it could be Quorum, which started as Ethereum or a branch of it, and really that is mainly it'. (Corp. Architect # 2) |
| | | Protocol Developers | 'I use websites of course Tor, Linux, Development tools'. (Protocol Developer # 2)<br>'My direct involvement is with the subset of crypto currency and its application as a digital form of money'. (Protocol Developer # 1) |
| | | Crypto. researchers | 'When I _work on_ assets, I interact more deeply with the math and code that underlies the protocols and their implementations'. (Crypto. Researcher # 1)<br>'. . . the more you use github, the more you get out of it'. (Crypto. Researcher # 2) |
| | Existing market-level resources | Users | 'I have a couple of mobile wallets that I use, Copay and Jaxx. In terms of exchanges I did have quite a few accounts because some coins are only on specific exchanges'. (User # 1)<br>'I've been using Bitcoin and Monero blockchains in a constant basis . . . I'm more interested in crypto currencies at the moment although I understand the value decentralized applications can have in the future'. (User # 2) |
| | | Corporate architects | 'We are subject to, as a bank in a multifaceted world, . . . trust bank, deposit bank, and different types to AML regulations that are there, so we are doing big work internally with our compliance and AML departments'. (Corp. Architect # 2) |
| | | Regulators | 'There is the original payments services directive (usually called PSD . . . There is also another piece of legislation, the Safe Effected Payments, generally referred to as the SEPA regulation'. (Reg. # 1)<br>'So, for it to be viable in the European Union. It needs to comply with the GDPR. But it's not possible [with Monero] . . . There are DLT networks out there trying to comply with GDPR but you could argue, some of those, whether they really are blockchain'. (Reg. # 5) |

**Table 5.** Subcategories of blockchain-related methods as enacted by social worlds.

| | Users | Protocol developers | Regulators | Corporate architects | Cryptographic researchers |
|---|---|---|---|---|---|
| Methods for overseeing typical transactions | + | + | + | + | + |
| Methods for overseeing extraordinary transactions | – | – | + | * | – |

View as positive = +; view as negative = –; view as neutral = *.

software projects such as the modular Hyperledger architectures and the Ethereum or Quorum platforms.

None of the social worlds appears to have conflicting views on the development-related resources. This may be because these resources are naturally complementary. Equally likely, it may be because each social world either is interested in different technological layers, meaning conflicts emerge and are reconciled with individual social worlds. In any case, the lack of observed tension means we view *existing development-level resources* as plastic and complacent.

*Existing market-level resources.* In addition to the resources used to develop blockchain systems, there are also key resources that allow those systems to interact with external environments. Regulators and corporate architects focused primarily on the fit between blockchain systems and the constraints imposed by related environments. Regulators must balance legislation across numerous domains simultaneously; thus, they assume the burden of ensuring each set of regulations is both externally consistent, and internally capable of managing unique domain-specific complexities. Several pointed out the challenges of General Data Protection Regulation (GDPR) compliance. This legislation has a significant impact on corporate architects, meaning they also develop sophisticated multi-domain understanding of regulation in order to ensure compliance.

Users were more focused on the related technologies that allowed them to interact with different markets, typically 'wallets' and mobile applications. Some had also experimented with development environments as a means of creating blockchain-based distributed applications, though this was done out of casual curiosity, rather than any serious intention of developing functional software. Five of the six interviewees from the regulator social world acknowledged that strong technical knowledge would be useful but felt it was impossible to maintain such knowledge without the time and background to specialise in blockchain development. Regulator # 2 was an exception, as he did possess detailed technical understanding of Monero and other cryptocurrencies. He attributed this to a personal interest and his day-to-day role in managing the regulators' information technology stack. This placed this individual at the intersection of the regulators and users, as he spent large amounts of time engaging with a larger privacy-focused digital ecosystem using more of his personal profile than professional. He listed some key technologies he believed would impact the privacy capabilities of blockchain technologies:

> . . . things like zero knowledge proofs, zk snarks, and technologies or currencies like Monero, ring signatures, confidential transactions, stealth addresses. There is a whole bunch of different privacy enhancing technologies there including I2P, or even sometimes Tor, which affect how you propagate transactions over a network . . . (Regulator # 2)

The multiple membership of Regulator # 2 is interesting. However, the general trend appears to be that different social worlds are either in agreement or they are disinterested in the specific resources being used. This disinterest does not appear problematic, nor does it present obvious future tensions. Thus, we view *existing market-level resources* as plastic and complacent (Table 3).

## *Privacy-related methods for blockchain technologies*

This category contains two sub-categories, summarized in Tables 5 and 6.

*Methods for overseeing typical transactions.* Users and developers were the social world with strongest views on methods for overseeing typical transactions. Some plasticity emerges between these worlds concerning the source of perceived threats. Users tended towards an anti-government 'cypherpunk' perspective, viewing the state as the predominant threat. Several individuals referenced 'capital controls' and the ability for governments to deter or outright ban transactions with different countries. One user gave the example of buying forbidden literature in North Korea

> It would be naive to think people in power [aren't] using massive amounts of data to keep themselves in power. I'm not saying that everyone who is in power is doing that, but it would be naive to not think some are . . . I guess one recent example would be North Korea, where most western literature (like 1984 from George Orwell) was 'forbidden' and unavailable anywhere, even libraries. With an alternative financial system that is not spied upon, like Monero, you would be able to acquire the book. (User # 2)

In contrast, protocol developers tended to believe corporations present the largest threat, due to the growing intrusiveness of data-based revenue models. Several of these protocol developers even viewed governments as allies in

**Table 6.** Examples of selective coding for privacy-related methods for blockchain.

| Category | Sub-category | Soc. world | Illustrative extracts |
|---|---|---|---|
| Privacy-related methods for blockchain | Methods for overseeing typical transactions | Users | 'If you can't preserve anonymity for your financial transactions, then you're a possible target for capital controls . . . it only takes a couple of bad actors to make bad use of this data'. (User#2)<br>'The ability to get money to these people (or from them) without permission, intervention, or snooping oversight is a big deal for me. It also allows them to hide or shield some of their property from the whims of the state'. (User#4)<br>'Forced reduction of privacy by people you do not consent to it with, and for reasons you do not control is out of the question for me. I cannot expect the government to do this on my behalf . . . so I must take back that power myself'. (User#4) |
| | | Corporate architects | 'Then comes blockchain . . . It places privacy back at the center of everything, which would otherwise slowly drift away mostly unnoticed. So blockchain-product customers will tend to be much more privacy [savvy] than normal internet ones'. (Corp. Architect#2)<br>'I think privacy is within everything that we do in any project that we do, and I may even say top two. Security and privacy and then making those two things work from a technology perspective'. (Corp. Architect#3) |
| | | Protocol Developers | 'I see the issue here as centralized control over technology . . . Blockchain can take back some if not most of what has been lost if it remains decentralized. In order for this to work people also have to take back control over the technology that surrounds them. That for starters means using Free Libre Open Source software for example. Also, government also has a role to play here . . . I see the biggest threat to privacy to come from big monopolistic business'. (Protocol Developer#1) |
| | | Crypto. researchers | 'We are walking around in this society where your doctor authenticates with you using your date of birth, and we put our date of birth into our Starbucks apps to get free drinks . . . it can't end well. One of the only ways we can start to get a handle on the situation is to try to treat every piece of data transmitted on the internet as an encrypted blob. Anything else is wildly dangerous'. (Crypto. Researcher#2) |
| | | Regulators | 'I don't think we should. And I mean, that's not the case today either. And I actually have my opinion, but I actually think it would be the opinion of most authorities both here and in the rest of Europe'. (Reg.#4) |
| Privacy-related methods for blockchain | Methods for overseeing extraordinary transactions | Users | 'I believe that anonymity is a condition of any fungible currency'. (User#3)<br>'I accept a variety of coins via Globee, but it is settled 100% in Monero for me. Fungibility is no joke'. (User#4) |
| | | Corporate architects | 'When it comes to money, it is absolutely crucial that it has privacy as its fundamental property. Otherwise there's no fungibility. So, I am absolutely convinced that the cash of the information age has to be a private, decentralized and electronic currency. When it comes to securities and other information property, privacy is optional, but the choice should be there'. (Corporate Architect#1)<br>'. . . and to create a system that offers users the privacy benefits of cash and removes the burdens of banks, privacy is necessary to ensure fungibility'. (Cryptographic Researcher#2) |
| | | Protocol developers | 'I see privacy centric blockchain technology as one way to stem the flow in one of the holes, whoever is on the other side'. (Protocol Developer#2)<br>'So, while privacy was not *required* before for fungibility, it may now be, due to this new practicality implying someone can check a central db. So, the argument has merit: if you don't have privacy, then such a list can be maintained, and therefore fungibility is destroyed. I don't know whether it's a fully solid argument though. It'd need thinking a lot to work out all the ramifications'. (Protocol Developer#2) |
| | | Crypto. researchers | 'A major point of applied cryptography in general is provide individuals and entities with the option to keep data and information safe . . . The application of it to distributed ledgers opens up new challenges . . . most major blockchain-based assets have public ledgers, where anyone can get a copy, but financial transactions and asset transfers are often sensitive, so the need for privacy in those transactions becomes extremely important'. (Cryptographic Researcher#1) |
| | | Regulators | 'Take the analogy with money laundering of cash . . . same sorts of things arise there. Is it hard to do any enforcement of that? Yeah, for precisely the same reasons. Does that mean enforcement is impossible? Well it's very difficult . . . what do law enforcement agencies do? They try to gather the patterns anyway . . .' (Reg#3)<br>'What we want is to be able to, if probably not us but the FIUs and the police, if they become aware of something, we want to be able to go to them and say "now you need to show us, not necessarily let us into your code or your system, but you need to extract this information."' (Reg.#4)<br>'if we're assigned to particular bank then we have to be aware of what transactions are taking place in regard to that institution . . . From a supervisory perspective, it's fundamental'. (Reg.#6) |

this struggle, referencing new laws such as the European General Data Protection Regulation (EU GDPR)[6] as efforts to curtail the intrusion of privacy. Others were also suspicious of governments, suggesting both private and public institutions were quick to abuse spying technology wherever possible. One individual described their view on data mining, harvesting, and surveillance in heated terms:

> Well, as everyone well knows by now, it's by every government and corporation, towards everyone that can get away with, and in all the ways get they can find. It's been massively helped by tech networked computers allowing sharing in real time, huge amount of storage so you can slurp and keep everything, fast processing so you can compare, intersect, analyse. Pretty much anything you do nowadays with tech is saved by govts/corps for later use. This did not use to be the case before that explosion in spying computer tech enabled. There are many companies nowadays whose sole purpose is enabling spying on you Experian, Equifax, Choice point. Their entire business model is getting as much information on people as they can, and then resell that to others, corps or govts. Corps can make more money by knowing who their customers are and predicting what they will want, and what kind of advertisement will trick them into buying more s**t. (Protocol Developer#2)

Regulators and corporate architects were largely in agreement that the temptation of monitoring and data harvesting technologies would inevitably appeal to unscrupulous public and/or private entities, with all the societal dangers that come with that. One participant was keen to point out the importance of ensuring 'anonymity', as it strongly relates to the constructs of privacy and identity:

> I think anonymity is a key element of the spectrum of privacy and identity. It's a missing piece . . . If you think of the spectrum of privacy ranging from complete and definitive identification and transparency of data and so forth to complete anonymity, in my view we need the entire spectrum . . . it's part of the fabric of human beings to utilise both ends of the spectrum. (Corporate Architect#4)

The cryptographic researchers are perhaps the most optimistic and least adversarial. These individuals suggest that the ideological commitment to privacy is so fundamental as to be a given. Why else use cryptographic technologies in the first place?

One recurring topic was that of tax and government scrutiny of assets. Perhaps surprisingly, social worlds appeared largely aligned on the matter. None of the individuals disagreed that the governments should collect tax. Furthermore, each assumed that individuals could choose to make taxable assets visible as they saw fit and in accordance with applicable law. This was typically compared with historical cash-based systems, where assets were seemingly invisible, yet tax was nonetheless collected.

Thus, methods for overseeing typical transactions were robust across each of the social worlds. Differences exist in the actual potential of blockchain-enabled systems to realise privacy, as well as how each social world perceives the interests of others, yet these differences do not change the actual individual perceptions possessed by each social world.

*Methods for overseeing extraordinary transactions.* Methods for overseeing extraordinary transactions were more divisive than those for overseeing typical transactions. Regulators are keen that 'dirty' money is discernible in some way to avoid facilitating crime. However, they understand this is complicated by the need for 'fungibility'[7] either at the practical or legal level. Many see fungibility as a necessary condition for any asset functioning as money, as all units of the currency must be equally valued in the open market. If units of a currency were to be valued differently, their interchangeability would be questioned (cf. Goodell and Aste, 2019; Kroeger and Sarkar, 2017; Möser et al., 2016). Thus, interviewees treat the need to balance the ability to identify 'dirty money' and the requirement to maintain currency fungibility as an open problem, which must be solved. One regulator was keen to point out blockchain data analysis was, and will continue to be, a fruitful avenue for criminal investigations, with both source and meta-data being available as and when required to law enforcement agencies. Although they did not comment on the veracity of these methods, they likened meta-data analysis to cash transaction investigations, when ancillary information was used to form a picture of illegal money flows. They agreed that methods for analysis were a problem, but they were not sure of the solution, or how effective specific meta-data analysis may be in the digital realm.

The remaining social worlds appear less interested in resolving this need to identify 'dirty money'. Many of them view this as an assumed trade-off if Monero is to function as a fungible currency. Protocol Developer#2 summarised this link as follows:

> So, while privacy was not *required* before for fungibility, it may now be, due to this new practicality implying someone can check a central db [database]. So, the argument has merit: if you don't have privacy, then such a list can be maintained, and therefore fungibility is destroyed. (Protocol Developer#2)

Corporate architects have varied perspectives on the importance of oversight methods. Some believed that making distinctions between transactions would inevitably lead to bifurcated networks, while others understood the tension as an unresolved trade-off between privacy and security – even noting it as being a potentially lucrative opportunity for any entity that could provide a working solution appropriate for the evolving demands and needs of privacy conscious consumers, but also satisfying law enforcement agencies and criminal investigators.

Thus, *methods for overseeing extraordinary transactions* present a significant source of internecine plasticity. Those developing and using the platform are assuming methods for overseeing extraordinary transactions are never to be included. Indeed, many of the functional building blocks appear to explicitly forbid them. Regulators are operating under the assumption future solutions will be possible, given the existence of meta-data, and increasingly powerful

analysis techniques (cf. Weber et al., 2019), while corporate architects understand the fundamental tension at the heart of the problem. It is not clear how these tensions may be resolved. The introduction of chain-based transparency/investigatory methods means users, developers, corporate architects, and cryptographic researchers may no longer value the currency. The absence of methods creates unacceptable conditions for regulators and investigators as 'dirty money' can disappear into the ledger at will. Neither anticipates any compromise, nor does a semi-fungible option appear technically feasible, given the manner in how 'strong' cryptographic schemes operate. At this stage, it appears one perspective must win out, potentially alienating one, or more, of the presently participating social worlds.

## Discussion

Blockchain systems have the potential to revolutionise a host of industries and financial markets (Beck and Müller-Bloch, 2017; Chong et al., 2019; Gozman et al., 2019; Risius and Spohrer, 2017; Rossi et al., 2019). The movement away from custodian-controlled, centrally secured data/networks into distributed and decentralised structures is arguably one of the most 'revolutionary' aspects of the technology (De Filippi, 2016; De Kruijff and Weigand, 2017; Olnes et al., 2017). Such decentralisation is predicated on the idea that every node has equal access to information on the network. Hence, any additional capabilities for oversight can have significant implications, as the ability to link an individual to one of their transactions opens up all of their interactions to scrutiny. Privacy and decentralisation are therefore closely coupled in blockchain systems. Nowhere has this been more controversial and polarising than in the development of privacy-enabling cryptocurrencies, such as Monero. Yet despite polarised opinions, development is nonetheless progressing on these cryptocurrencies with limited signs of inter-group conflict. This study explores this puzzling lack of conflict. We characterise the privacy attitudes of the different groups that are directly or indirectly participating, and we identify key divergences likely to foster conflict in the future. These findings have implications for privacy research, for blockchain regulation, and for blockchain designers.

### *Implications for privacy research*

For privacy research, the first major finding is the converging privacy attitudes around the *right to privacy* and *methods for overseeing typical transactions*. The tension between these ideas has been a topic of research for many years (Rubenfeld, 1989; Warren and Brandeis, 1890), particularly as it relates to digital technologies (see Brunton and Nissenbaum, 2015; Campbell and Carlson, 2002; Finn et al., 2013; Franzak et al., 2001; Nissenbaum, 2004; Van Den Hoven, 2008; Zuboff, 2015). This means privacy and supervision often become topics of heated debate as new network technologies emerge (cf. Clarke, 2019; Davison, 2012; Goodell and Aste, 2019; Hey Tow et al., 2010; March, 2019; Rueckert, 2019). These concerns seem especially salient for blockchain systems. This is because the privacy enabling capabilities of blockchain threaten business models around user data (see, for example, Morey et al., 2015; Täuscher and Laudien, 2018) and typical means of preventing tax avoidance (e.g. Anderson et al., 2018; Fulmer, 2018; Gozman et al., 2019; Hyvärinen et al., 2017; Marian, 2013; Molloy, 2018; Möser et al., 2013). Yet, we observed no disagreements among interviewees from different social worlds. No one argued systems should force individuals to disclose routine information. Instead, several likened Monero/blockchain transactions to a return to cash-based systems; systems that have a sound historic record of protecting confidentiality while still facilitating tax collection. This finding helps to dispel false perceptions of conflict in privacy attitudes that may otherwise create distraction, and so refocuses attention on other interesting discussions of financial privacy in the payments sphere (see Agarwal, 2016; Balgobin et al., 2016; Berg, 2018; Kahn et al., 2005; Kahn, 2018; McElroy, 2016). More importantly, the realisation that all collaborating social worlds see these transactions as private should expedite systematic protection against the growing threats of transaction surveillance and price discrimination associated with digital payments and cryptocurrencies (Horn et al., 2020).

Despite areas of overlapping privacy attitudes, this study also identified two problematic divergences in privacy attitudes; divergences that may become increasingly meaningful if privacy-focused blockchain systems become more popular.

The first problematic divergence of privacy attitudes concerns the level of government involvement in development. While all social worlds agree that near-term government involvement is undesirable, regulators are operating under the assumption they may join the development at a later stage when necessary restrictions have been identified. The nature of blockchain systems means such a strategy may not be possible, as protocols that are coded into the system currently may be impossible to remove or replace later on, especially given the decentralised nature of system governance, and the lack of any identifiable controlling entity.

The second problematic divergence of privacy attitudes concerns the methods for overseeing extraordinary transactions. The regulators assume such methods are necessary to avoid widespread, near-effortless money laundering, even at the expense of privacy (cf. Anderson et al., 2018; De Filippi, 2014; EBA, 2019; Elias, 2011; Foley et al., 2019; Fulmer, 2019; Genkin et al., 2018; Gruber, 2013; Juels et al., 2016; Miller et al., 2017; Molloy, 2018; Möser et al., 2013; Zyskind et al., 2015). Yet, each of the other social worlds are operating under the assumption that the potential misuse of the system for money laundering has already been accepted to accommodate the essential mechanics that

make a cryptocurrency work, that is, the explicit compound of privacy, data protection, and fungibility. No obvious technological middle ground is presented, leaving no discernible path to negotiation at a later date. Instead, it seems the privacy attitudes common to developers and users are becoming part of the foundational layer of the technology.

### *Implications for blockchain regulation*

Regulators have typically been slow to regulate the alternative finance systems, as there are concerns such regulation stifles innovation and fails to predict the actual issues once a system is in use. They appear to have therefore adopted a 'wait and see' approach before stepping in to make changes. However, two important features of blockchain-based systems complicate this regulation strategy:

1. Policy and code cannot be separated (cf. Lessig, 1999, 2003, 2009). This is how blockchain systems avoid reliance on third parties, as rules are written into the programmatic logic of the system (Bordo and Levin, 2017; De Domenico and Baronchelli, 2019; De Filippi, 2014; De Filippi and Hassan, 2018).
2. The consensus code is difficult to alter. Just as the rules are written into the code, the code is embedded into the system and layered into the mechanism for network consensus. This is a key feature of their security, as the scale of resources required for consensus change prohibits minority groups from altering network consensus.

This suggests it may not be possible to layer existing systems onto systems such as Monero after-the-fact. Therefore, regulators may not be able to actually impose any changes on cryptocurrencies already in circulation, limiting their eventual policy implementations to the introduction of new cryptocurrencies in the future.

For existing cryptocurrencies, in the absence of a clear and transparent legislative framework to dictate which privacy attitudes can and cannot be built into cryptocurrencies, the perspectives of developers and researchers are being written into the industry at 'lower' levels of interaction. We view this 'hard-coding' of regulation as internecine, as incompatibilities are also likely to create tensions with other privacy laws. The EU GDPR is a case in point. For example, the 'right to be forgotten' does not seem to be compatible with GDPR (cf. Buocz et al., 2019; EPRS, 2019; Humbeeck, 2019; Rieger et al., 2019; Schwerin, 2018). Some have argued efforts to afford anonymity (and thus anonymised transaction data) within the Monero protocol potentially provide a mechanism for ensuring that information recorded on the public viewable ledger falls outside of scope of the GDPR (cf. Recital 26, EU GDPR, 2018), but even this is not clear given the intricacies of anonymisation from both cryptographic and data protection viewpoints (cf. German Standards Authority, DIN, 2020; European Data Protection Board (EDPB), 1997, 2014; International Standards Authority, ISO, 2020). Several regulators in this study suggested it may come down to banning these privacy-centric cryptocurrencies, though also noted this may be difficult to enforce, given users are difficult to identify and infrastructure providers operate from countries all over the world. Those regulators hope that users will only use cryptocurrencies like Monero if they can exchange it for compliant currencies, at which point regulators may track these exchange transactions. However, this assumes a critical mass is not reached where uses are happy to both receive and spend Monero without exchanging it for other currencies.

The alternative strategy is that regulators should become actively involved in the development of cryptocurrencies in the near-term – essentially providing a mechanism for proposing consensus level protocol change. Yet this not only requires extensive technical training for experienced regulators, it also requires future issues are accurately predicted, and (perhaps most problematically) those citizens and corporations developing the systems welcome participants and their privacy-related recommendations into development projects. The challenge is how to foster trust in development communities to effectively communicate regulatory goals in a way that makes developers 'want' to include them, avoiding the danger of society perceiving regulatory imposition as an algorithmically enforced 'post-political' condition: government policy woven into the technological infrastructure (Husain et al., 2019).

### *Implications for managers and system design*

The idea of a generational divide in organisations is well-documented, as are the resulting challenges for management (e.g. Burke and Ng, 2006; Hershatter and Epstein, 2010; Thompson and Gregory, 2012). This study showed signs of an inconspicuous transfer of power from experienced business leaders and law makers to technologically knowledgeable groups. It is not clear the extent to which all actors are aware or complicit in this transfer of power. On one hand, experienced business leaders and law makers appear to be operating under the assumption that *ex post* changes are possible, when this may not actually be the case. On the other hand, those same individuals appear happy to defer to technologically knowledgeable groups when discussing the specifics of such future changes. This suggests the former expects the latter to take responsibility for how these systems enact privacy, albeit the handover is taking place earlier than expected. Thus, by action or inaction, regulators and corporate architects are, at best, allowing privacy-related values of these blockchain systems to supersede those of traditional frameworks, and at worst,

failing to recognise that traditional regulatory frameworks may be impotent to enact change at the protocol layer.

This study also highlighted challenges in separating the social worlds that participate in the development of blockchain systems. Building on established wisdom, we separated these worlds by professional and practical competency, under the assumption professional learning and identity development were key motivators for participation (e.g. Handley et al., 2007; Harris et al., 2004; Probst and Borzillo, 2008; Ranmuthugala et al., 2011; Wenger and Snyder, 2000). Yet, multiple membership existed for several participants – blurring the boundary edge. Moreover, the source of multiple membership in most cases were either the users (which included individuals in all other social worlds) or the developers (which included corporate architects and cryptography researchers), arguably the two most ideologically charged social worlds. This reflects a growing view these social worlds should be viewed as socio-relational loci of learning, rather than competency-based communities (see Omidvar and Kislov, 2014). This is an important distinction moving forward, assuming blockchain development continues to combine personal beliefs, politics/ideologies, and technological decisions.

An additional interesting finding is the lack of tension observed around several areas of genuine divergence. These include the complementary technologies used in different markets and the extent of decentralisation anticipated as more blockchain-based systems take hold. The development of blockchain has often shown clear evidence of infighting and hostility with regard to technology choices (e.g. Andersen and Bogusz, 2019; De Filippi and Loveluck, 2016). One may, therefore, reasonably assume the same conflict exists between the participating social worlds. Yet, this does not appear to be the case. Instead, each is focused on different technological layers, with few signs of unforeseen issues arising in the future. Again, this finding clarifies the nature of conflict in these communities and helps to better understand the collaboration taking place.

### *Limitations and future research*

This study represents an exploratory study into variances of perspectives that exist surrounding the development of blockchain technology. We acknowledge the qualitative analysis and limited sample size means caution must be taken when generalising findings. This trade-off was made consciously; our focus being on immersion with a smaller number of individuals over more superficial contact with a larger number. Nevertheless, having done such immersive research, the need for larger numbers and more formalised theory should be considered in future studies.

We also acknowledge that we focused on a particularly privacy-centric cryptocurrency, that is, Monero. The merging of technology-enthusiasm and politics is not new (Brunton and Nissenbaum, 2015; Mitchell, 2002), but the Monero community have an especially strong reputation for political discourse as privacy-advocates, sometimes associating themselves with 'crypto-anarchist' and 'cypherpunk' movements (Karlstrøm, 2014; Rid, 2016). However, these individuals are clearly not representative of all blockchain development communities. Rather, this study treats them as an index case to shine a light on potential tensions across the broader cryptocurrency and blockchain space. Future studies should build on this foundation to explore privacy perspectives and tensions around other cryptocurrencies such as Bitcoin, Ethereum, as well as emerging privacy centric protocols and protocol improvements such as MimbleWimble,[8] Lelantus,[9] Zether,[10] Enigma,[11] and platforms for confidential assets, such as Tari.[12]

## Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

## Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

## ORCID iD

Rob Gleasure https://orcid.org/0000-0002-4265-4665

## Notes

1. Miners predominantly validate third-party Monero transactions. However, their own transactions are more often than not included in this set, depending on their level of interaction with the network.
2. See https://app.wire.com/auth/
3. See https://telegram.org/
4. See https://en.wikipedia.org/wiki/Internet_Relay_Chat
5. The interviews were conducted over telephone, recorded with consent, and later transcribed.
6. The General Data Protection Regulation (GDPR) is a regulatory framework concerned with how personal data is collected and processed in the European Union (EU) and the European Economic Area (EEA). This includes the transfer of personal data outside the EU and EAA.
7. Fungibility describes whether or not each individual unit of a currency is equally interchangeable and wholly indistinguishable from another (cf. Amarasinghe et al., 2019).
8. MimbleWimble is a privacy-focused protocol authored by an anonymous author. More information may be found here: https://tlu.tarilabs.com/protocols/grin-protocol-overview/MainReport.html
9. Lelantus is a trustless privacy-preserving protocol which is being integrated into ZCoin. More information may be found here: https://zcoin.io/tech/
10. Zether is a privacy-focused mechanism designed for the Ethereum ecosystem. More information may be found here: https://ethresear.ch/t/zether-the-first-privacy-mechanism-designed-for-ethereum/5029

11. Enigma is a second layer privacy-focused proposal designed for the Ethereum ecosystem. More information may be found here: https://docs.ethhub.io/built-on-ethereum/infrastructure/aztec-protocol/
12. Tari is a digital assets focused blockchain protocol being architected as a merge-mined sidechain with Monero. More information may be found here: https://www.tari.com/

## References


5th Anti-Money Laundering Directive (AMLD5) Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (Text with EEA relevance). Available at: http://data.europa.eu/eli/dir/2015/849/oj (accessed 20 May 2019).

Acquisti A and Grossklags J (2005) Privacy and rationality in individual decision making. *IEEE Security & Privacy* 3(1): 26–33.

Acquisti A, Brandimarte L and Loewenstein G (2015) Privacy and human behaviour in the age of information. *Science* 347(6221): 509–514.

Agarwal S (2016) Bitcoin transactions: A bit of financial privacy. *Cardozo Arts & Ent. LJ*, 35, 153.

Amarasinghe N, Boyen X and McKague M (2019) A survey of anonymity of cryptocurrencies. In: *ACSW 2019: Proceedings of the Australasian computer science week multiconference*, Sydney, NSW, Australia, 29–31 January, pp. 1–10. New York: ACM.

Andersen JV and Bogusz CI (2019) Self-organizing in blockchain infrastructures: Generativity through shifting objectives and forking. *Journal of the Association for Information Systems* 20(9): 1242–1273.

Anderson R, Shumailov I and Ahmed M (2018) Making bitcoin legal. In: Matyas V, Svenda P, Stajano F, et al. (eds) *Cambridge International Workshop on Security Protocols*. Cham: Springer, pp. 243–253.

Angst CM and Agarwal R (2009) Adoption of electronic health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion. *MIS Quarterly* 33(2): 339–370.

Antonopoulos A (2016) *The Internet of Money*, Vol. 1. Middletown, DE: Merkle Bloom LLC; CreateSpace Independent Publishing Platform.

Ashford NA (2002) Government and environmental innovation in Europe and North America. *American Behavioral Scientist* 45(9): 1417–1434.

Atzori M (2015) Blockchain technology and decentralized governance: Is the state still necessary? Available at: https://pdfs.semanticscholar.org/bc1c/abd366fce6d3e1fe39cd58cf699114d9d13b.pdf (accessed 3 June 2018).

Awad NF and Krishnan MS (2006) The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quarterly* 30(1): 13–28.

Baggio JA, Brown K and Hellebrandt D (2015) Boundary object or bridging concept? A citation network analysis of resilience. *Ecology and Society* 20(2): 2.

Balgobin Y, Bounie D, Quinn M, et al. (2016) Payment instruments, financial privacy and online purchases. *Review of Network Economics* 15(3): 147–168.

Barrett M and Oborn E (2010) Boundary object use in cross-cultural software development teams. *Human Relations* 63(8): 1199–1221.

Baskerville RL and Myers MD (2009) Fashion waves in information systems research and practice. *MIS Quarterly* 33(4): 647–662.

Beck R and Müller-Bloch C (2017) Blockchain as radical innovation: A framework for engaging with distributed ledgers. In: *Proceedings of the 50th Hawaii international conference on system sciences*, Hawaii, 4–7 January.

Beck R, Avital M, Rossi M, et al. (2017) Blockchain technology in business information systems research. *Business & Information Systems Engineering* 59(6): 381–384.

Belanger F and Crossler R (2011) Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly* 35(4): 1017–1041.

Belanger F and Xu H (2015) Editorial: The role of information systems research in shaping the future of information privacy. *Information Systems Journal* 25: 573–578.

Berg C (2018) *The Classical Liberal Case for Privacy in a World of Surveillance and Technological Change*. Cham: Palgrave Macmillan, pp. 181–194.

Bergman M, Lyytinen K and Mark G (2007) Boundary objects in design: An ecological view of design artifacts. *Journal of the Association for Information Systems* 8(11): 546–568.

Black J (2002) Critical reflections on regulation. *Australian Journal of Legal Philosophy* 27: 1–29.

Black J and Anderson K (2013) *Creating an Ethical Framework for the Financial Services Industry*. London: Herbert Smith Freehills; London School of Economics.

Blumer H (1954) What is wrong with social theory? *American Sociological Review* 19(1): 3–10.

Bonneau J, Miller A, Clark J, et al. (2015) Sok: Research perspectives and challenges for bitcoin and cryptocurrencies. In: *2015 IEEE symposium on security and privacy*, San Jose, CA, 17–21 May, pp. 104–121. New York: IEEE.

Bordo MD and Levin AT (2017) Central bank digital currency and the future of monetary policy (No. w23711). *National Bureau of Economic Research*. Available at: https://www.nber.org/papers/w23711 (accessed 20 May 2018).

Brunton F and Nissenbaum H (2015) *Obfuscation: A User's Guide for Privacy and Protest*. Cambridge, MA: MIT Press.

Buntinx JP (2017) The early history of Monero in 500 words. Available at: https://themerkle.com/the-early-history-of-monero-in-500-words/ (accessed 20 May 2018).

Buocz T, Ehrke-Rabel T, Hödl E, et al. (2019) Bitcoin and the GDPR: Allocating responsibility in distributed networks. *Computer Law & Security Review* 35(2): 182–198.

Burke RJ and Ng E (2006) The changing nature of work and organizations: Implications for human resource management. *Human Resource Management Review* 16(2): 86–94.

Burnett K, Subramaniam M and Gibson A (2009) Latinas cross the IT border: Understanding gender as a boundary object between information worlds. *First Monday* 14. Available at: http://firstmonday.org/ojs/index.php/fm/article/view/2581.

Buterin V (2014) A next-generation smart contract and decentralized application platform. *Ethereum whitepaper*. Available at: https://cryptorating.eu/whitepapers/Ethereum/Ethereum_white_paper.pdf (accessed 20 May 2018).

Campbell JE and Carlson M (2002) Panopticon.com: Online surveillance and the commodification of privacy. *Journal of Broadcasting & Electronic Media* 46(4): 586–606.

Carroll P (2012) Water and technoscientific state formation in California. *Social Studies of Science* 42(4): 489–516.

Carter N (2018) Blockchain is a Semantic Wasteland: Why haven't we abandoned it. Available at: https://medium.com/s/story/blockchain-is-a-semantic-wasteland-9450b6e5012 (accessed 20 May 2018).

Chanson M, Bogner A, Bilgeri D, et al. (2019) Blockchain for the IoT: Privacy-preserving protection of sensor data. *Journal of the Association for Information Systems* 20(9): 1274–1309.

Charmaz K (2000) Grounded theory: Objectivist and constructivist methods. In: Denzin NK and Lincoln YS (eds) *Handbook of Qualitative Research*. Thousand Oaks, CA: SAGE, pp. 509–535.

Chong AYL, Lim ET, Hua X, et al. (2019) Business on chain: A comparative case study of five blockchain-inspired business models. *Journal of the Association for Information Systems* 20(9): 1310–1339.

Ciborra CU and Andreu R (2001) Sharing knowledge across boundaries. *Journal of Information Technology* 16(2): 73–81.

Clarke AE (2003) Situational analyses: Grounded theory mapping after the postmodern turn. *Symbolic Interaction* 26(4): 553–576.

Clarke AE and Star SL (2008) The social worlds framework: A theory/methods package. *The Handbook of Science and Technology Studies* 3: 113–137.

Clarke R (2019) Risks inherent in the digital surveillance economy: A research agenda. *Journal of Information Technology* 34(1): 59–80.

CoinRanking (2020) Cryptocurrency market capitalisation statistics. Available at: https://coinranking.com (accessed 14 May 2018).

Corbin JM and Strauss A (1990) Grounded theory research: Procedures, canons, and evaluative criteria. *Qualitative Sociology* 13: 3–21.

Currie WL, Gozman DP and Seddon JJ (2018) Dialectic tensions in the financial markets: A longitudinal study of pre-and post-crisis regulatory technology. *Journal of Information Technology* 33(4): 304–325.

Darke P, Shanks G and Broadbent M (1998) Successfully completing case study research: Combining rigour, relevance and pragmatism. *Information Systems Journal* 8(4): 273–289.

Davison RM (2012) The privacy rights of cyborgs. *Journal of Information Technology* 27(4): 324–325.

De Domenico M and Baronchelli A (2019) The fragility of decentralised trustless socio-technical systems. *EPJ Data Science* 8(1): 2.

De Filippi P (2014) Bitcoin: A regulatory nightmare to a libertarian dream. *Internet Policy Review* 3(2): 43.

De Filippi P (2016) The interplay between decentralization and privacy: The case of blockchain technologies. *Journal of Peer Production* 7. Available at: https://hal.archives-ouvertes.fr/hal-01382006/document (accessed 12 February 2018).

De Filippi P and Hassan S (2018) Blockchain technology as a regulatory technology: From code is law to law is code. *arXiv Preprint*. Available at: https://arxiv.org/ftp/arxiv/papers/1801/1801.02507.pdf (accessed 19 June 2020).

De Filippi P and Loveluck B (2016) The invisible politics of bitcoin: Governance crisis of a decentralized infrastructure. *Internet Policy Review* 5(4): 1–28.

De Kruijff J and Weigand H (2017) Towards a blockchain ontology. Research report, Tilburg University. Available at: https://www.list.lu/fileadmin/files/Event/sites/tudor/files/Training_Center/OTHERS/VMBO2017_paper_5.pdf (accessed 14 May 2018).

Denzin NK and Lincoln YS (2000) *Handbook of Qualitative Research*. Thousand Oaks, CA: SAGE.

Dierksmeier C and Seele P (2018) Cryptocurrencies and business ethics. *Journal of Business Ethics* 152(1): 1–14.

Doolin B and McLeod L (2012) Sociomateriality and boundary objects in information systems development. *European Journal of Information Systems* 21(5): 570–586.

Eisenhardt KM (1989) Agency theory: An assessment and review. *Academy of Management Review* 14(1): 57–74.

Elias M (2011) Bitcoin: Tempering the digital ring of Gyges or implausible pecuniary privacy. Available at: https://ssrn.com/abstract=1937769 (accessed 25 January 2018).

EU GDPR (2018) REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj (accessed 30 January 2018).

European Banking Association (EBA) (2019) On crypto-assets: Report with advice for the European Commission. Available at: https://eba.europa.eu/-/eba-reports-on-crypto-assets (accessed 11 January 2019).

European Central Bank (ECB) (2020) STELLA – Joint research project of the European Central Bank and the Bank of Japan. Balancing confidentiality and auditability in a distributed ledger environment, February. Available at: https://www.ecb.europa.eu/paym/intro/publications/pdf/ecb.miptopical200212.en.pdf (accessed 5 March 2020).

European Data Protection Board (EDPB) (1997) Formally known as the Article 29 Working Party, recommendation 3/97 anonymity on the internet, adopted by the working party on 3rd December 1997. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1997/wp6_en.pdf (accessed 14 June 2020).

European Data Protection Board (EDPB) (2014) Formally known as the Article 29 Working Party, opinion 05/2014 on anonymisation techniques adopted on 10th April 2014. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf (accessed 12 December 2019).

European Parliamentary Research Service (EPRS) (2019) Blockchain and the general data protection regulation: Can distributed ledgers be squared with European data protection law? European Parliamentary Research Service Scientific Foresight Unit (STOA) PE 634.445 – July 2019. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf (accessed 12 September 2019).

Feagin JR, Orum AM and Sjoberg G (1991) *A Case for the Case Study*. Chapel Hill, NC: UNC Press Books.

Federal Office (2019) Towards secure blockchains, concepts, requirements, assessments. Available at: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Secure_Blockchain.pdf?__blob=publicationFile&v=3 (accessed 13 December 2019).

Ferreira A (2020) Emerging regulatory approaches to blockchain-based token economy. *The Journal of the British Blockchain Association* 3: 12270.

Financial Action Task Force (FATF) Recommendations, international standards on combating money laundering and the financing of terrorism & proliferation. Available at: http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html (accessed 19 July 2019).

Finn RL, Wright D and Friedewald M (2013) Seven types of privacy. In: Gutwirth S, Leenes R, De Hert P, et al. (eds) *European Data Protection: Coming of Age*. Dordrecht: Springer, pp. 3–32.

Flyvbjerg B (2006) Five misunderstandings about case-study research. *Qualitative Inquiry* 12(2): 219–245.

Foley S, Karlsen JR and Putniņš TJ (2019) Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies? *The Review of Financial Studies* 32(5): 1798–1853.

Franzak F, Pitta D and Fritsche S (2001) Online relationships and the consumer's right to privacy. *Journal of Consumer Marketing* 18(7): 631–642.

Frost L, Reich MR and Fujisaki T (2002) A partnership for Ivermectin: Social worlds and boundary objects. In: Reich MR (ed.) *Public-Private Partnerships for Public Health*. Cambridge: Harvard Center for Population and Development Studies, pp. 87–113.

Fujimura JH (1992) Crafting science Standardized packages, boundary objects, and translation. In: Pickering A (ed.) *Science as Practice and Culture*. Chicago, IL: University of Chicago Press, pp. 168–211.

Fulmer N (2018) Exploring the legal issues of blockchain applications. *Akron Law Review* 52: 5.

Garrod JZ (2016) The real world of the decentralized autonomous society. *tripleC: Communication, Capitalism & Critique, Open Access Journal for a Global Sustainable Information Society* 14(1): 62–77.

Genkin D, Papadopoulos D and Papamanthou C (2018) Privacy in decentralised cryptocurrencies. *Communications of the ACM* 61(6): 78–88.

German Standards Authority, DIN (2020) DIN SPEC 4997 Privacy by Blockchain Design: A standardised model for processing personal data using blockchain technology. Available at: www.din.de/en/about-standards/din-spec-en/business-plans/wdc-beuth:din21:303231492 (accessed 15 April 2020).

Gikay AA and Stanescu CG (2019) Technological populism and its archetypes: Blockchain and cryptocurrencies. *Nordic Journal of Commercial Law* 2(2019): 66–109.

Gioia DA, Corley KG and Hamilton AL (2013) Seeking qualitative rigor in inductive research: Notes on the Gioia methodology. *Organizational Research Methods* 16(1): 15–31.

Golumbia D (2015) Bitcoin as politics: Distributed right-wing extremism. In: Lovink G, Tkacz N and de Vries P (eds) *MoneyLab Reader: An Intervention in Digital Economy*. Amsterdam: Institute of Network Cultures, pp. 118–131.

Goodell G and Aste T (2019) Can cryptocurrencies preserve privacy and comply with regulations? *Frontiers in Blockchain* 2(4): 1–14.

Gozman D, Liebenau J and Aste T (2019) The role of blockchain regulatory technology: Lessons from Project Maison. *MIS Quarterly Executive* 19(1): 19–37.

Gruber S (2013) Trust, identity and disclosure: Are bitcoin exchanges the next virtual havens for money laundering and tax evasion. *Quinnipiac Law Review* 32: 135208.

Hamburg MA (2012) FDA's approach to regulation of products of nanotechnology. *Science* 336(6079): 299–300.

Handley K, Clark T, Fincham R, et al. (2007) Researching situated learning: Participation, identity and practices in client – Consultant relationships. *Management Learning* 38(2): 173–191.

Harris R, Simons M and Carden P (2004) Peripheral journeys: Learning and acceptance of probationary constables. *Journal of Workplace Learning* 16(4): 205–218.

Hershatter A and Epstein M (2010) Millennials and the world of work: An organization and management perspective. *Journal of Business and Psychology* 25(2): 211–223.

Hey Tow WNF, Dell P and Venable J (2010) Understanding information disclosure behaviour in Australian Facebook users. *Journal of Information Technology* 25(2): 126–136.

Horn M, Oehler A and Wendt S (2020) FinTech for consumers and retail investors: Opportunities and risks of digital payment and investment services. In: Walker T, Gramlich D, Bitar M, et al. (eds) *Ecological, Societal, and Technological Risks and the Financial Sector*. Montreal, QC, Canada: Palgrave Macmillan, pp. 309–327.

Humbeeck AV (2019) The blockchain-GDPR paradox. *Journal of Data Protection & Privacy* 29(4): 1201–1241.

Husain SO, Roep D and Franklin A (2019) Prefigurative post-politics as strategy: The case of government-led blockchain projects. *The Journal of the British Blockchain Association* 3(1): 1–11.

Huvila I, Anderson TD, Jansen E, et al. (2016) Boundary objects in information science. *Journal of the American Society for Information Science and Technology* 68(8): 1807–1822.

Hyvärinen H, Risius M and Friis G (2017) A blockchain-based approach towards overcoming financial fraud in public sector services. *Business & Information Systems Engineering* 59(6): 441–456.

International Standards Authority, ISO (2020) Final text for publication of ISO/TR 23244 privacy and personally identifiable information protection considerations, joint ISO/TC 307 – ISO/IEC JTC 1/SC 27 WG Blockchain and distributed ledger technologies and IT Security techniques. Available at:

https://www.iso.org/standard/75061.html (accessed 19 June 2020).

Irwin A and Vergragt P (1989) Re-thinking the relationship between environmental regulation and industrial innovation: The social negotiation of technical change. *Technology Analysis & Strategic Management* 1(1): 57–70.

Jacob M (2005) Boundary work in contemporary science policy: A review. *Prometheus* 23(2): 195–207.

Janssen M and Van Den Hoven J (2015) Big and Open Linked Data (BOLD) in government: A challenge to transparency and privacy? *Government Information Quarterly* 32(4): 363–368.

Jensen T, Hedman J and Henningsson S (2019) How TradeLens delivers business value with blockchain technology. *MIS Quarterly Executive* 18(4): 221–243.

Jornet A and Steier R (2015) The matter of space: Bodily performances and the emergence of boundary objects during multidisciplinary design meetings. *Mind, Culture, and Activity* 22(2): 129–151.

Juels A, Kosba A and Shi E (2016) The ring of Gyges: Using smart contracts for crime. In: *SIGSAC conference on computer and communications security*, Vienna, 24–28 October.

Kahn CM, McAndrews J and Roberds W (2005) Money is privacy. *International Economic Review* 46(2): 377–399.

Kahn M (2018) Payments systems and privacy, Federal Reserve Bank of St. Louis review. *Fourth Quarter* 100(4): 337–344. Available at: https://doi.org/10.20955/r.100.337-44 (accessed 28 March 2019).

Kaplan S, Milde J and Cowan RS (2017) Symbiont practices in boundary spanning: Bridging the cognitive and political divides in interdisciplinary research. *Academy of Management Journal* 60(4): 1387–1414.

Karlstrøm H (2014) Do libertarians dream of electronic coins? The material embeddedness of bitcoin. *Scandinavian Journal of Social Theory* 15(1): 23–36.

Kiviat TI (2015) Beyond bitcoin: Issues in regulating blockchain transactions. *Duke Law Journal* 65: 569–608.

Kroeger A and Sarkar A (2017) *The Law of One Bitcoin Price?* Philadelphia, PA: Federal Reserve Bank of Philadelphia.

Lessig L (1999) Code is law. *Harvard Magazine*. Available at: https://www.harvardmagazine.com/2000/01/code-is-law-html (accessed 19 June 2020).

Lessig L (2003) Law regulating code regulating law. *Loyola University Chicago Law Journal* 35(1): 1–14.

Lessig L (2009) Code: And other laws of cyberspace. Available at: http://codev2.cc/download+remix/Lessig-Codev2.pdf (accessed 2 June 2020).

Levina N and Vaast E (2005) The emergence of boundary spanning competence in practice: Implications for implementation and use of information systems. *MIS Quarterly* 29(2): 335–363.

Li Y, Marier-Bienvenue T, Perron-Brault A, et al. (2018) Blockchain technology in business organizations: A scoping review. In: *Proceedings of the 51st Hawaii international conference on system sciences*, Hawaii, 3–6 January.

McElroy WF (2016) Closing the financial privacy loophole: Defining access in the right to financial privacy. *Wash. UL Rev.*, 94, 1057.

March ST (2019) Alexa, are you watching me? A response to Clarke, 'risks inherent in the digital surveillance economy: A research agenda'. *Journal of Information Technology* 34(1): 87–92.

Marian O (2013) Are cryptocurrencies super tax havens. *Michigan Law Review First Impressions* 112(2): 38–48.

Markey-Towler B (2018) Anarchy, Blockchain and Utopia: A theory of political-socioeconomic systems organised using blockchain. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3095343 (accessed 19 June 2020).

Matavire R and Brown I (2013) Profiling grounded theory approaches in information systems research. *European Journal of Information Systems* 22(1): 119–129.

Mattke J, Hund A, Maier C, et al. (2019) How an enterprise blockchain application in the US pharmaceuticals supply chain is saving lives. *MIS Quarterly Executive* 18(4): 246–261.

Maurer B, Nelms TC and Swartz L (2013) When perhaps the real problem is money itself! – The practical materiality of Bitcoin. *Social Semiotics* 23(2): 261–277.

Miller A, Möser M, Lee K, et al. (2017) An empirical analysis of linkability in the Monero blockchain. Available at: https://maltemoeser.de/paper/monerolink.pdf (accessed 19 June 2020).

Mitchell T (2002) *Rule of Experts: Egypt, Techno-Politics, Modernity*. Berkeley, CA: University of California Press.

Molloy B (2018) Taxing the blockchain: How cryptocurrencies thwart international tax policy. *Oregon Review of International Law* 20: 623–648.

Mondschein CF (2020) Browser-based crypto mining and EU data protection and privacy law: A critical assessment and possible opportunities for the Monetisation of Web services. *The Journal of the British Blockchain Association* 3: 1–13.

Monero (2019) RandomX is a new ASIC resistant Proof of Work Algorithm used where decentralization matters. Available at: https://www.moneroooutreach.org/stories/RandomX.html (accessed 19 June 2020).

Moore AD (2000) Employee monitoring and computer technology: Evaluative surveillance v. privacy. *Business Ethics Quarterly* 10(3): 697–709.

Moore AD (2008) Defining privacy. *Journal of Social Philosophy* 39(3): 411–428.

Morey T, Forbath T and Schoop A (2015) Customer data: Designing for transparency and trust. *Harvard Business Review* 93(5): 96–105.

Möser M, Bohme R and Breuker D (2013) *An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem*. San Francisco, CA: eCrime Researchers Summit (eCRS).

Möser M, Eyal I and Sirer EG (2016) Bitcoin covenants. In: *International conference on financial cryptography and data security*, 17–18 September 2013, San Francisco, California, pp. 126–141. Berlin; Heidelberg: Springer.

Nakamoto S (2008) Bitcoin: A peer-to-peer electronic cash system. Available at: http://bitcoin.me/bitcoin.pdf (accessed 3 January 2018).

Narayanan A and Clark J (2017) Bitcoin's academic pedigree. *Communications of the ACM* 60(12): 36–45.

Nissenbaum H (2004) Privacy as contextual integrity. *Washington Law Review* 79(1): 119–157.

Noor KBM (2008) Case study: A strategic research methodology. *American Journal of Applied Sciences* 5(11): 1602–1604.

Olnes S, Ubacht J and Janssen M (2017) Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. *Government Information Quarterly* 34(3): 355–364.

Omidvar O and Kislov R (2014) The evolution of the communities of practice approach: Toward knowledgeability in a landscape of practice – An interview with Etienne Wenger-Trayner. *Journal of Management Inquiry* 23(3): 266–275.

Patton MQ (1990) *Qualitative Evaluation and Research Methods*. Newbury Park, CA: SAGE.

Pavlou P (2011) State of the information privacy literature: Where are we now and where should we go? *MIS Quarterly* 35(4): 977–988.

Posner RA (1981) The economics of privacy. *The American Economic Review* 71(2): 405–409.

Probst G and Borzillo S (2008) Why communities of practice succeed and why they fail. *European Management Journal* 26(5): 335–347.

Ranmuthugala G, Plumb JJ, Cunningham FC, et al. (2011) How and why are communities of practice established in the healthcare sector? A systematic review of the literature. *BMC Health Services Research* 11(1): 273.

Revised Payment Services Directive (PSD2) Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance). Available at: http://data.europa.eu/eli/dir/2015/2366/oj (accessed 19 August 2019).

Rieger A, Lockl J, Urbach N, et al. (2019) Building a blockchain application that complies with the EU general data protection regulation. *MIS Quarterly Executive* 18(4): 263–279.

Risius M and Spohrer K (2017) A blockchain research framework: What we (don't) know, where we go from here, and how we will get there. *Business & Information Systems Engineering* 56(6): 385–409.

Roca JB, Vaishnav P, Morgan MG, et al. (2017) When risks cannot be seen: Regulating uncertainty in emerging technologies. *Research Policy* 46(7): 1215–1233.

Roman R, Zhou J and Lopez J (2013) On the features and challenges of security and privacy in distributed internet of things. *Computer Networks* 57(10): 2266–2279.

Rossi M, Mueller-Bloch C, Thatcher JB, et al. (2019) Blockchain research in information systems: Current trends and an inclusive future research agenda. *Journal of the Association for Information Systems* 20(9): 1390–1405.

Rubenfeld J (1989) The right of privacy. *Harvard Law Review* 102: 737–807.

Rueckert C (2019) Cryptocurrencies and fundamental rights. *Journal of Cybersecurity* 5(1): tyz004.

Ryngaert C and Taylor M (2020) The GDPR as global data protection regulation? *AJIL Unbound* 114: 5–9.

Sarker S, Xiao X and Beaulieu T (2013) Guest editorial: Qualitative studies in information systems: A critical review and some guiding principles. *MIS Quarterly* 37(4): iii–xviii.

Schultze U and Mason RO (2012) Studying cyborgs: Re-examining internet studies as human subjects research. *Journal of Information Technology* 27(4): 301–312.

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.

Singh S and Singh N (2016) Blockchain: Future of financial and cyber security. In: *2016 2nd international conference on contemporary computing and informatics* (IC3I), Noida, India, 14–17 December.

Smith HJ, Dinev T and Xu H (2011) Information privacy research: An interdisciplinary review. *MIS Quarterly* 35(4): 989–1016.

Star SL (1998) Working together: Symbolic interactionism, activity theory and information systems. In: Engestrom Y and Middleton D (eds) *Cognition and Communication at Work*. Cambridge, MA: Cambridge University Press.

Star SL and Griesemer JR (1989) Institutional ecology, 'translations' and boundary objects: Amatuers and professionals in Berkeley's Museum of vertebrate zoology. *Social Studies of Science* 19: 387–420.

Strauss A (1978) *A Social World Perspective. Studies in Symbolic Interaction*. Oxford: Oxford University Press.

Strauss A and Corbin JM (1990) *Basics of Qualitative Research: Grounded Theory Procedures and Techniques*. Newbury Park, CA: SAGE.

Sutanto J, Palme E, Tan CH, et al. (2013) Addressing the personalization-privacy paradox: An empirical assessment from a field experiment on smartphone users. *MIS Quarterly* 37(4): 1141–1164.

Szabo N (1994) Smart contracts. Available at: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html (accessed 9 July 2018).

Tajfel H (1978) The achievement of group differentiation. In: Tajfel H (ed.) *Differentiation between Social Groups: Studies in the Social Psychology of Intergroup Relations*. London: Academic Press, pp. 77–98.

Täuscher K and Laudien SM (2018) Understanding platform business models: A mixed methods study of marketplaces. *European Management Journal* 36(3): 319–329.

Thompson C and Gregory JB (2012) Managing millennials: A framework for improving attraction, motivation, and retention. *The Psychologist-Manager Journal* 15(4): 237–246.

Thornberg R (2012) Informed grounded theory. *Scandinavian Journal of Educational Research* 56(3): 243–259.

Tschorsch F and Scheuermann B (2016) Bitcoin and beyond: A technical survey on decentralized digital currencies. *IEEE Communications Surveys and Tutorials* 18(3): 2084–2123.

Underwood S (2016) Blockchain beyond bitcoin. *Communications of the ACM* 59(11): 15–17.

Urquhart C, Lehmann H and Myers MD (2010) Putting the 'theory' back into grounded theory: Guidelines for grounded theory studies in information systems. *Information Systems Journal* 20(4): 357–381.

Van Pelt SC, Haasnoot M, Arts B, et al. (2015) Communicating climate (change) uncertainties: Simulation games as boundary objects. *Environmental Science & Policy* 45: 41–52.

Van Den Hoven J (2008) Information technology, privacy, and the protection of personal data. In: Van den Hoven J and Weckert J (eds) *Information Technology and Moral Philosophy (Cambridge Studies in Philosophy and Public Policy)*. Cambridge: Cambridge University Press, pp. 301–321.

Walsh C, O'Reilly P, Feller J, et al. (2016) New kid on the block: A strategic archetypes approach to understanding the

blockchain. In: *International conference on information systems*, Dublin, 11–14 December.

Warren SD and Brandeis LD (1890) The right to privacy. *Harvard Law Review* 4(5): 193–220.

Weber M, Domeniconi G, Chen J, et al. (2019) Anti-money laundering in bitcoin: Experimenting with graph convolutional networks for financial forensics. Available at: https://arxiv.org/abs/1908.02591 (accessed 19 June 2020).

WEF (2020) Insight report Central Bank Digital currency policy–maker Toolkit January 2020 centre for the fourth industrial revolution. Available at: http://www3.weforum.org/docs/WEF_CBDC_Policymaker_Toolkit.pdf (accessed 28 January 2020).

Wenger EC and Snyder WM (2000) Communities of practice: The organizational frontier. *Harvard Business Review* 78(1): 139–146.

Winget MA (2008) Annotations on musical scores by performing musicians: Collaborative models, interactive methods, and music digital library tool development. *Journal of the Association for Information Science and Technology* 59(12): 1878–1897.

Winter SJ and Butler BS (2011) Creating bigger problems: Grand challenges as boundary objects and the legitimacy of the information systems field. *Journal of Information Technology* 26(2): 99–108.

Yakel E (2004) Encoded archival description: Are finding aids boundary spanners or barriers for users? *Journal of Archival Organization* 2(1–2): 63–77.

Zavolokina L, Ziolkowski R, Bauer I, et al. (2020) Management, governance and value creation in a blockchain consortium. *MIS Quarterly Executive* 19(1): 1–17.

Zhang R, Xue R and Liu L (2019) Security and privacy on blockchain. *ACM Computing Surveys (CSUR)* 52(3): 1–34.

Zohar A (2015) Bitcoin: Under the hood. *Communications of the ACM* 58(9): 104–113.

Zuboff S (2015) Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology* 30(1): 75–89.

Zyskind G, Nathan O and Pentland A (2015) Decentralizing privacy: Using blockchain to protect personal data. In: 2015 *IEE CS symposium on security and privacy workshops*, San Jose, CA, 21–22 May, pp. 180–184. New York: IEEE.

## Author biographies

Rob Gleasure is an associate professor in Digitalization at Copenhagen Business School. He has published in journals such as Information Systems Research, the Journal of the Association for Information Systems, the European Journal of Information Systems, the Journal of Information Technology, Information Systems Journal, the Journal of Strategic Information Systems, and MIT Sloan Management Review. He is an Associate Editor for the European Journal of Information Systems.

Robin Renwick is a research analyst at Trilateral Research Ltd, and is part of the Applied Research and Innovation (ARI) team. He completed his PhD at Queen's University Belfast. His research interests focus on privacy, distributed ledger technology, decentralized identity and cybersecurity.