Skullduggery in peer-to-peer networks and the need for a new cyber-social theory

Donna Champion[1]

[1] *Nottingham Trent University, Nottingham, NG1 4BU, United Kingdom.*

Abstract

Distributed ledgers (DL) and 'blockchains' are being applied to manage planetary-scale information systems, such as the ledgers for cryptocurrencies, transactions across critical infrastructures for energy, food and water, and for managing public documents such as registries of land holdings. DL/blockchains are operationalised through the combined actions of complex software algorithms and digitally distributed Peer-to-Peer (P2P) networks which act together to validate data and transactions, and then create and hold the record of transactions and asset holdings (the ledger). P2P digital networks are both cyber and social in nature; these new organizational forms also exhibit political intentionality, exclusionary behavior, and at times require extra payments (or bribes) to prioritize certain transactions. This paper examines various examples of skullduggery which digital P2P networks have perpetrated, and argues socio-technical theories are not enough to explain these cyber-social collectives, we need a new cyber-social theory.

Keywords

Distributed Ledger Technology, Blockchain, Peer-to-Peer, P2P, Cyber-social, Cyber-politics.

1. Introduction

Distributed Ledgers (DL) are often considered to have game-changing potential for managing large data sets, particularly where there is an exchange of valuable assets between two parties. One type of implementation of DL are 'blockchains' which use cryptography to validate transactions and keep the ledger as a secure record, or 'chain' of transactions. This type of DL/blockchain underpin cryptocurrencies, such as Bitcoin and Ethereum, and offer a 'tamper-evident' record of transactions that occur between parties who do not necessarily know or trust one another [1]. In practice, the functionality of distributed ledgers is achieved through complex software protocols and a distributed peer-to-peer network (P2P) acting together to validate transactions, and to create and hold the record of transactions and asset holdings (the ledger). This paper argues that these combined software/P2P networks are best described as 'cyber-social collectives' (CSCs) which communicate and transfer information and assets across globally distributed systems with little regard for sovereign boundaries and different jurisdictions. Many of these CSCs (though not all) are designed to operate with no central authority and some have an underpinning motivation and in-built protocols designed to elude state-control, making legislation and accountability an area of risk and concern for future implementations and applications [2].

[1] Dr Donna Champion
7th International Workshop on Socio-Technical Perspective in IS development (STPIS 2021) 11-12 October 2021, Trento, Italy
EMAIL: donna.champion@ntu.ac.uk
ORCID: 0000-0003-1657-6349

New and emerging technologies are often 'over-hyped' and DL/blockchains are no exception. Some have suggested that DL/blockchain offer an 'immutable and tamper-proof' record of transactions [3], but at best this record is 'tamper-evident'. DL/blockchain ledgers have been rewritten and have separated into different entities ('hard forks'), at times allowing the 'double-spend' that such technologies were purportedly designed to prevent. Examining the circumstances where such action has occurred give us insight into the political aims underpinning different cyber-social collectives. These instances also suggest that, over the long term, trading anonymously and without trust could irreversibly erode trading relationships and have serious consequences for wider society. This paper is call for a new theory that provides insight into the misuse of power that occurs in some of these new organizational forms and sets out two founding principles needed to keep these CSCs accountable to democratic society.

In section 2, the paper explores the cyber-social nature of DL/P2P networks through some examples of unscrupulous, dishonest and underhand behaviour (skullduggery) which has occurred in cryptocurrency ledgers of Ethereum and Bitcoin and discusses the consequences of this behaviour for the applications underpinned by DL/blockchains. In section 3, sociotechnical and sociomateriality theories are critiqued and are argued as not being sufficient to explain the activities of the P2P networks which underpin these cyber-social globally distributed systems. In section 4, the political intentionality built into P2P supported distributed systems is further explored through the example of the TOR operating system and then in section 5 a prototype theory for the cyber-social is set out which incorporates the principles of equitable access to resources and accountability as foundational to holding power to account. The conclusion sets out a research agenda for the sociotechnical/IS discipline.

2. The cyber-social nature of distributed systems

2.1 How DL/blockchains are operationalised

DL/blockchains comprise a combination of technologies which work to create a validated, distributed record of transactions which is then replicated, shared, and synchronized digitally, across a network of participating nodes (the peer-to-peer network, or P2P) [4]. In blockchains, transactions are gathered in 'blocks', with each block being validated before being added to the ledger, and the blockchain is then maintained as a linear, sequential record (chain) of the transactions, incorporating cryptographic hashes [5] and Merkle Trees [6] to secure the data and its place in the chain. For both distributed ledgers and blockchains, functionality is achieved through the actions of software protocols and the digitally distributed P2P network who work as a cyber-social collective (CSC) to validate transactions and keep the ledger secure.

Each DL/blockchain operates in a slightly different way according to the protocols and rules set out by the underpinning P2P network and coded into the associated software algorithms. Some DL/blockchains have been set up to monitor the transfer of assets between a specific group of participants and so only designated members have access and permission to validate transactions; these ledgers operate according to rules agreed by their participants. This type of blockchain is often referred to as 'permissioned'. But other distributed ledgers/blockchains were set up to be 'open', which means anyone with the knowledge and resources can participate in the process of validating the transactions. In open blockchains, (such as those for the Bitcoin and Ethereum cryptocurrencies), theoretically anyone with the right equipment, skills and access to the internet can participate in the P2P network supporting the ledger. Bitcoin and Ethereum reward people participating in activity to validate transactions (referred to as mining) by awarding tokens.

One of the features of open blockchains, is they were designed to operate as a decentralized network, with no single person, or node, in control of the actions of the P2P network. This idea is embedded in

the aims of the original group of developers for the first blockchain, Bitcoin, who called themselves Cypherpunks, and whose political aim was to create a currency beyond control of the state, and regulatory controls [7, 8]. The idea of a decentralized, distributed consensus forming, without a central control authority, around managing transactions/data has also been incorporated into other distributed systems such as the TOR operating system. Indeed, the concept of 'no centralised control' has caught the public imagination, leading to a great deal of media discussion around the idea that transactions recorded on DL/blockchains do not require people to trust one another, and so will remove intermediaries such as bankers, lawyers, accountants, from the processes of commerce and introduce a new leaner, less expensive way of doing business [1]. Few people have stopped to question if this is a desirable situation in practice.

Despite all of the press coverage, and hype, there are currently few full scale, large implementations of blockchains. Bitcoin (an open blockchain) has been the most successful and the largest scale implementation to date. The peer-to-peer (P2P) network underpinning the cryptocurrency Bitcoin is considered particularly robust and has successfully offered an undisputed record of the transactions that have occurred using Bitcoin since its inception [4]. (This currently holds true even with the development of Bitcoin Cash). In the context of business implementations of DL/blockchains, most projects to date are focused on developing private or permissioned blockchains, because these types of blockchain provide an environment where the business partners retain control over the ledger, rather than cede control to the 'wild west' of the internet.

2.2 Skullduggery on Ethereum

Different blockchains apply different types of consensus protocols and are constructed using different programming languages, each of which can impact on the way the respective P2P network operates, how data validation is managed, and how the P2P addresses dissent and security flaws. Such operational details are often forgotten in the blockchain hype [9]. One example of how programming language ambiguity can lead to issues across a blockchain can be found in the case of the very first Ethereum 'hard fork' (a hard fork is where the chain of transactions splits into two records which are then maintained separately according to different rules, by different P2P networks). In June 2016, an anonymous attacker hacked into the Ethereum blockchain and took millions of dollars' worth of 'ether', the Ethereum digital currency. This was achieved by exploiting ambiguities in the software code used to design Ethereum (a programming language called 'Solidity') and by creating a hard fork in the Ethereum blockchain, so there are now two Ethereum blockchains: the original Ethereum, (or Ethereum Foundation) run according to the rules set out by the DAO (Distributed Autonomous Organization, the originators of Ethereum) and 'Ethereum Classic', a new blockchain, sharing the ledger before the fork with Ethereum Foundation, but after the fork, being developed by a different team and in a different way. Note: since this original hard fork in the Ethereum chain, there have been others, but this first example of a 'hard fork' is fully documented and so is available for analysis [10].

Examining the context and history leading up to the hard fork, and the activities and decisions that followed this first Ethereum hard fork is instructive to reflect upon when considering governance frameworks for DL/blockchains. In early 2016, a crowdfunding initiative had raised over $150 million to invest in developing Ethereum to support the DAO. This investment was intended to develop the Ethereum blockchain to support smart contracts and enable new business applications. The hack into Ethereum used a valid action in the code to withdraw the funds and put them into an alternative DAO (with a new digital address) which the hacker had control over [10]. The person (or persons) undertaking this 'hack', (or valid action, depending on your viewpoint), had therefore taken investment away from the original Ethereum project. Although this action was 'valid' in terms of the code and the smart contracts then set up around the investments, the action was against the interests of investors who had donated funds [10]. The community forming the P2P network underpinning Ethereum disagreed over what action should be taken to address this issue, and so they decided by a vote. The majority voted to change the Ethereum code, so the state of the ledger was the same as just before the hard fork. This approach resulted in the investment funds being reinstated. This decision meant the majority of the P2P

network had voted to say the Ethereum blockchain was not immutable, (an important stated characteristic of blockchains prior to this hack) and that the ledger could be altered if enough people had the incentive to agree to a change. There were, however, a significant group of Ethereum developers who fundamentally disagreed with this approach. This alternative group argued that for blockchain projects to gain trust, the ledger needed to be free from alteration (they viewed any alteration of the chain as censorship) and rewriting the ledger was against the founding principles of blockchain development [9, 10]. This smaller group of developers have continued to develop the Ethereum fork, now called 'Ethereum Classic'; this group argue they are remaining true to the idea that a blockchain ledger should be free from tampering.

This situation means Ethereum Classic is a blockchain where the funds were never returned to the investors, and Ethereum Foundation is a blockchain where these same funds were moved to another address, the original ledger was restored and the investment was protected. This action also meant anyone with funds in the original Ethereum Foundation blockchain, could open an account with Ethereum Classic and double the number of 'ether', (Ethereum's cryptocurrency) they held. Both forms of ether have value that can be traded. Hertig [10] explains, "to traders, this is essentially free money". This situation results in people holding ether before this Ethereum hard fork effectively being able to 'double-spend' their money, exactly the situation cryptocurrencies are supposed to prevent. Vitalik Buterin, the originator of Ethereum Foundation, admits there are problems with governance on the blockchain and suggests this is because people are using cryptocurrencies as commodities (and so trading in them for only monetary gain) [11].

The Ethereum Foundation blockchain project was originally focused on the idea of providing an infrastructure for 'smart contracts'. Smart contracts are software protocols, that once implemented, deploy the 'contract' written into the software in a manner immune to human interference [12]. But the Ethereum hard fork demonstrates 'immutability' is not, in practice, a characteristic of blockchains, and in any case is not particularly desirable because such a condition does not allow for mistakes to be corrected. Levy [12] argues, even with perfect coding, smart contracts will not be able to capture the social and legal obligations they are intended to represent. The problem for DL/Blockchains operated as 'open' systems, is how to manage disagreement and how to impose a governance structure. Without agreed rules, useful applications of open DL/blockchains start to disappear.

2.3 More skullduggery and governance issues on Bitcoin

When adding new transactions to a DL/blockchain, the rules for validating a transaction are set out in published protocols to determine 'who decides what data is added to the ledger'. The Bitcoin blockchain uses a 'Proof of Work' (PoW) consensus protocol, where the miners who make up the P2P network for Bitcoin compete to be the first to solve a set of cryptographic puzzles. In the PoW consensus protocol, only the first miner to successfully guess the correct hash and validate the data, is rewarded with some of the cryptocurrency for that blockchain. This process is wasteful of both time and energy. To succeed, miners need access to a large amount of computing power, and increasingly also use specially designed computer chips. This has led to groups of miners collaborating and pooling their computing resources for a share in the reward.

In March 2017, three large mining pools controlled over 50% of the Bitcoin hash rate [13]. The main mining pools in Bitcoin operate a cartel, and it is conceivable, in the future, there could be a single owner for the Bitcoin network [13]. There are other security concerns too. To *profitably* mine on the Bitcoin blockchain, the hardware used requires specific types of computer chips and over 80% of these are made in a single country, China. By January 2021, there were five mining pools for Bitcoin, but the work to guess the hash is concentrated in China [14], an interesting situation, as China has a state policy of disapproval towards cryptocurrencies and mining activity. This raises the prospect of future unanticipated attacks on blockchains, in the manner of the Ethereum hard fork, where there is a bid for

control of the ledger. Developing a set of governance principles on how to address such attacks is needed if DL/blockchains are to achieve their potential for secure and robust enterprise applications.

The Proof of Work (PoW) protocol for validating transactions is not then without issues, but other validation protocols have problems too. The most commonly suggested alternatives to PoW for achieving consensus are the 'Proof of Stake' (PoS) protocols [11], used in Ethereum, and the Proof of Elapsed Time (PoET) consensus protocol on Sawtooth (a collaboration between Intel and Hyperledger developed by IBM), both of these protocols favor those with most capital invested in that blockchain and so do not treat all their participants equally.

Bratton [15] has argued that current theory does not help us think through how software algorithms, platforms and protocols are altering the nature of communication, action and purpose across the social world, impacting upon politics, geography, sovereignty, economics and culture. In the case of DL/blockchains, current regulation efforts are focused on licensing. One of the problems with designing new approaches for governance for DL/blockchains (and also for other software algorithms such as those used in artificial intelligence) is that our current socio-technical theories do not offer us insight into the actions and political ambitions of P2P networks.

3. Theoretical frameworks and cyber-social P2P networks

3.1 Sociotechnical theories

Sociotechnical theory has traditionally focused on finding ways of designing the social aspects of work and the technology, so they work in harmony [16, 17]. The aim is to put the concerns of end-users first and allow users to design their own systems and processes. The focus on adaptability and understanding the local context in these approaches offers end-users a position as key-players and stems from a belief that workers must control productive assets to develop the most effective and efficient way of operating and producing goods. Clegg [18] focused on four levels of design work:

1. Designing the content and process of each part of the system
2. The interconnections across the social and the technical system
3. Ensuring end-users were involved in design work
4. Ensuring well-designed job roles resulted from the process.

One of the main assumptions in sociotechnical approaches is that the design and operation of 'the system' will occur within a reasonably bounded organizational context, with an identifiable set of end-users, making the involvement of end-users a relatively straight forward process. Sociotechnical design assumes any conflict that occurs during the design or operation of the system, will be managed through negotiation amongst a specified group of workers who are known to each other. Jasanoff [19, p. 12] argues for better conceptions of "how power is delegated to technological systems" in sociotechnical approaches, and Bijker [20] makes the case for further developing sociotechnical theory so economic and political questions are also considered in design. But this work is yet to be done, and Winter et al [21] highlight the lack of research examining sociotechnical systems in an inter-organizational context, where groups can have constantly changing membership. Sociotechnical approaches focus on contexts where there are formal, acknowledged processes for managing conflict and disagreement. The governance structures applied in sociotechnical design reflect the bureaucratic, traditional hierarchies found in latter day Co-operative societies, with various types of worker committees and Boards of Directors/Trustees, overseeing decisions for workers/members. The literature on sociotechnical systems then, offers rich insight into the experience of human workers, but focuses on human activity supported by technology within defined organizational boundaries, and so is currently of limited application in the context of globally distributed systems such as DL/blockchains, where ambiguities in programming code can be an invitation to an opportunistic hack.

3.2 Sociomateriality

The work on sociomateriality in the Information Systems (IS) discipline has further developed ideas of how the social and the technical interconnect. Leonardi [22] makes the case for an approach to sociomateriality underpinned by a substantialist ontology, where "the social and material are separate but are put into relationship with each other" (p. 69). Leonardi [22, p. 70] uses the metaphor of 'imbrication' to describe the process whereby the social and material intertwine and interact to create a distinct structure, but such a framing cannot explain why a particular organizational form makes a specific decision, and also does not offer a frame to evaluate the impact of the decision. An alternative perspective on sociomateriality, has been proposed by Orlikowski and Scott [23] who adopt an 'agential realist' philosophy and so regard the social and material as being inherently inseparable and accepts non-human actors are participants in the production of knowledge, thereby acknowledging practices have ethical consequences, but there are problems here too. Performativity in agential realism, does not privilege human action, and so regards humans and technology (non-humans) to be ontologically inseparable, and as Cecez-Kecmanovic et al [24] point out "recognizing the co-constitution between the social and the technical does not imply equality", and they argue for IS research that explores these ethical dimensions.

The Cyborg Manifesto [25] seems to predict much of what has happened in the development of decentralized and distributed systems in recent years. Haraway argues the prevalence of micro-electronics, that are invisible to the human eye, makes their impact and influence hard to see, not just materially, but politically also. She predicts "a cyborg world is about the final imposition of a grid of control on the planet" (p. 154), suggesting machines are becoming "disturbingly lively", whilst our minds have "become disturbingly inert". She also criticises progressives for their tendency to fight against technics and their call for a return to nature and organic living, she argues convincingly there is no way back to a time before these technologies were invented.

Haraway argues as a feminist and Marxist, and so focuses on stories of domination in western, masculinist narratives. She suggests the problem with these distributed, decentralized systems (the cyborg in her writing) is not technological determinism, but that we are dealing with a historical system underpinned by structured relations needing new analysis and political action. She acknowledges that different groups have different and specific political imperatives, and she calls for unity and affinity amongst people with similar political beliefs with the aim of disarming and demilitarizing the state. Wajcman [26] criticises Haraway for giving insufficient consideration, to how to create a government that supports inclusive, diverse structures, and there is certainly a lack of discussion in Haraway's work on the value of democracy, or how the contract between the citizen and the state can also be a force for good, particularly for the vulnerable. Haraway [25] does however, set out some useful questions that help us to begin understanding cyborg forms, asking us to consider 'how we construct boundaries', particularly between humans and non-humans. She also asks us to consider 'what is at stake in those boundaries?', (Who wins, who loses?). As distributed systems, artificial intelligence and 'edge' devices become more common, there is a great deal of research waiting to be done to develop answers to these boundary questions, but socio-technical and sociomateriaity studies (from either a substantialist, or agential realist ontological position) seem focused on small, localized systems found in office settings, rather than trying to grapple with the planetary-scale distributed systems which underpin modern commerce and communications. Work within socio-technical theory and sociomateriality frames usually acknowledge ethical questions, but evade issues of power and the political implications of sociomaterial performativity. To understand the behavior of digitally distributed P2P networks, we need to further explore their underpinning political intentionality.

4 Political intentionality in P2P networks

4.1. The TOR operating system

In addition to DL and blockchain cryptocurrencies such as Ethereum and Bitcoin, other types of distributed, decentralized systems, are underpinned by P2P networks. For example, TOR (The Onion Router), this web browser facilitates anonymous browsing of the internet and has enabled the activities of activists (or whistle blowers depending on your viewpoint) such as Edward Snowdon releasing information through Wikileaks. TOR can be argued to be an essential tool in bringing corrupt state officials to account, but also facilitates criminal activity on the dark web [8]. For example, the TOR platform facilitated the sale of goods on the Silk Road website, where trade in drugs (and other illicit goods) was enabled by anonymous browsing in TOR and anonymous payments being made with Bitcoin. Silk Road had the stated aim of helping people to avoid paying taxes. Although Silk Road was shut down by the US authorities in 2013, similar platforms immediately appeared online (including Silk Road 2.0. which was shut down in November 2014) and continue to proliferate. Digital P2P networks are employing software algorithms to enable action which has political consequences (such as crime). Indeed, political intentionality is embedded in the design and development of digitally distributed P2P networks and the systems they enable.

Golumbia [2] in discussing the development of the first blockchain, which underpins the Bitcoin currency, makes a convincing case that the politics of the Bitcoin designers (the Cypherpunks) derives from the more extreme end of right wing politics drawing on the ideas of authors such as Ayn Rand [27] who argues each person should have the complete freedom to act without interference from the state. These ideas around implementing anonymous, decentralized systems to evade state control, have entered the mainstream carried on the hype surrounding new technologies such as the blockchain, and more recently artificial intelligence. For example, in the preface of Clippinger and Bollier [3, p x], they go as far as to suggest that the "enlightenment ideals of democratic rule seem to have run their course". Such complacency about the long term consequences of new technologies is commonplace in development circles. These distributed P2P networks are facilitating the operation of software algorithms for DL and AI, which operate at lightning speed, on a global scale, taking decisions (such as the distribution of value in assets and resources) all of which have wide ranging ethical, moral and political implications for society. What is needed is a theory of the cyber-social to help us consider what ethical, moral and legal framework is required to keep political intentionality embedded within these cyber-social collectives, accountable to democratic society.

5 A prototype theory of cyber-social collectives

5.1. Governance and managing 'power' in cyber-social collectives

A theory of the cyber-social needs to offer a framework through which to judge the actions and impact of these new organizational forms which are a conglomeration of software algorithms and P2P networks (a cyber-social collective, or CSC) across global distributed systems. Such a theory also needs to encompass a view of how to construct a set of governance principles to manage power wielded by these CSCs and keep them accountable to society. Ayn Rand's idea that each person should have the complete freedom to act without interference from the state has become embedded in the development of many of new formulations of DL/blockchains, cryptocurrencies and AI. For anyone who believes in liberal democracy, this is problematic. In the literature on Jurisprudence, Dworkin [28] argues that there is a difference between the notion of 'complete freedom' for a citizen to do whatever they like with no constriction from the state, and "liberty, which is that part of [a citizen's] freedom that government would do wrong to constrain" [28, p. 4]. Dworkin acknowledges there will be interpretive differences between groups on how the structures of law, governance and the state are designed to fulfil this ideal in practice, but in this view, the state is justified on moral grounds to impose taxes for instance, to enable state institutions to show equal concern for all citizens. This view of the law and governance, that there are acceptable limitations that the state can place on the behavior of a citizen, is in direct opposition to the libertarian view propounded by Ayn Rand and the Cypherpunks.

The two principles set out below, are a first attempt to question the "grid of control on the planet" [25, p. 154], these decentralized, distributed systems might exert. These principles are the foundation of a prototype 'cyber-social theory' and make a clear statement that cyber-social collectives underpinning DL/blockchains and AI algorithms should be judged according to a conception of value that incorporates ethics (how we behave) and morals (how we treat others). By bringing together ethics and morality in a 'unity of value' [28], the political intentionality of the actions of cyber-social collectives can be analyzed and judged.

5.2 Principle 1: Equality of Access to Resource and Services should be enabled

MacKinnon argues the disadvantaged in society are rarely permitted to ask for anything that does not suit the elite [29]. She states: "equality is valued nearly everywhere, seldom practiced, and nowhere yet achieved" [29, p. 305], and so she refuses to reduce inequality to merely a conception of human dignity, arguing "inequality is relentlessly material first, a system of hierarchical social meanings second" [29, p. 307]. Tufekci [30] has argued that no-one can tell what machine learning will enable us to achieve with data in the future, so there is no "informed consent" around these technologies. And within the literature on Jurisprudence, Mackinnon has also made a substantive argument for an equality that recognizes the "irrelevance of difference […and refuses] to be distracted by consent under conditions under which it is meaningless" [29, p. 324].

Applying this principle in practice, requires that services and resources controlled and managed through DL/blockchains/CSCs must have mechanisms in place to demonstrate they facilitate equality of access, and that they practice equal concern for every citizen in the relevant constituency, or milieu. Such a principle should apply to AI algorithms too.

5.3 Principle 2: Accountability:

In considering how to keep democratic processes honest and open to challenge, Benn [31] asks us to consider: to whom people, processes and institutions are accountable, and how those in positions of power can be over-ruled, and if necessary, removed from power. Reflecting on who a specific group is accountable to and how we can stop their activities, if necessary, is particularly challenging when considering cyber-social collectives. This is because attributing specific behavior to specific individuals in online environments is difficult. Attribution can also be challenging when investigating the activities that become associated with open blockchains, such as, the Silk Road marketplace, or cryptocurrency wallets such as Mount Gox. Work in cyberforensics is making attribution in these types of environments easier but the process is slow and expensive. The accountability principle requires us to oversee the activities of cyber-social collectives *and* ensure any governance structures set in place are open to review, question and critique [31].

To put even just these two principles into practice requires a new field of research. Current technology works on a premise of users giving technology and service providers a broad range of permission in order to use the services they provide. This is problematic for two reasons. First, distributed systems increase the number of sites where information is stored, and although the 'pro-blockchain' argument insists privacy will be protected, this is not a situation anyone can currently guarantee. (The affordances literature in IS has not even begun to grapple with this issue yet, issues of power and control are simply ignored). The second problem is the issue raised by MacKinnon [29] and Tufecki [30] in that there can be no informed consent around potential uses of data in globally distributed systems.

What is needed is much more robust approach to accountability than is currently evident in any area of data management [32]. To meet the requirements of *accountability* across DL/blockchain

development (and AI applications), there will need to be formal structures for audit and reporting, that are, if necessary, enforced. These procedures for holding cyber-social collective enabled systems to account will have to include meaningful review by diverse groups of citizens, and not just by elite-controlled mechanisms of a state, or of a world institution not accountable to democratic processes. Private and commercial interests push back against regulation. The innovation and fast pace of development has been exhilarating, but as business applications for DL/blockchains and AI move forward, issues of intellectual property and competitive advantage come to the fore. There is no reason, however, why trade on blockchains, data stored on DL, or applications of AI should be exempt from meaningful scrutiny.

One way to ensure 'equality of access' and 'accountability is to go back to the first principles of the sociotechnical movement and embed end users in the design, implementation and ongoing evaluation of such systems. The technological complexities of such systems should not be a stumbling point. End-user engagement is not currently practiced effectively for such systems [33], but even if software protocols need to be designed by experts, the services they facilitate can be judged by the community of stakeholders they impact. There is a role here for sociotechnical researchers to develop approaches to facilitate user engagement in large, complex, transnational environments, not just the smaller, less complex systems found described in journal papers for the IS discipline.

6 Conclusions

Sociotechnical researchers need to engage with the development of standards for how the different types of DL/blockchains (open and permissioned) deliver decentralization. This might be expressed in terms of how much of the hash rate specific players can control in consensus protocols to prevent a monopoly developing that could give a small group of partners overall control of the ledger. Another area for regulation and standards to address would be around what type of consensus protocols could be used for specific applications. Research to develop less energy intensive ways to achieve consensus would certainly help. But for the United Nations, for example, to achieve their aim of employing blockchains to help achieve sustainability objectives, there should be consideration given to what constitutes acceptable energy consumption, how many nodes should be used for storing the ledger, how P2P membership should be overseen etc., and each decision will inevitably involve trade-offs, and will need to be open and accountable through a democratic process.

In examining the way software protocols are used to analyze big data sets for establishing people's credit scores, Pasquale [32] comments that regulation has made little difference to the quality of these systems as "penalties for erroneous information on credit reports are too low to merit serious attention from credit bureaus" (p. 191). In addition to regulation and governance, we will need to be serious in our intent to hold these cyber-social collectives to account. History does not offer many optimistic parallels. Discussing the reasons for the financial crises in 2008, McGee [34, p. 306] suggests a financial system where people are rewarded for "pursuing maximum levels of profits and return on equity, without heed to systemic risk or the interests of all the stakeholders" is a path to continued inequality and future crises. Such a lack of concern for other citizens is reflected in the politics of the Cypherpunks and is also becoming embedded in the way these technologies are being designed and implemented. In her work on smart contracts Levy [12] suggests there is a "thin conception of what the law does" amongst smart contract developers. The position I take here, is we cannot leave the design, implementation and governance of these cyber-social collective-enabled technologies to the technics alone, we must be proactive to ensure citizens have an equal say in the design and rules embedded in these systems, taking into account, the social and political implications over the long-term.

These two principles for governance for cyber-social collectives are consistent with Dworkin's view of law and governance as 'integrity', and as requiring those in a position of power to treat those they have power over equally and with dignity, incorporating an ethical and moral approach to behavior by which we can judge their political intentionality.

7 References

[1] D. Tapscott, A. Tapscott, Blockchain Revolution: How the technology behind Bitcoin is changing the world, Penguin Random House, UK, 2016.
[2] D. Golumbia, The politics of Bitcoin: software as extremism, University of Minneapolis Press, Minneapolis. 2017.
[3] J.H. Clippinger, D. Bollier, (Eds) From Bitcoin to the burning man and beyond: the quest for identity and autonomy in a digital society, ID3 and Off the Common Books, Boston, 2014.
[4] A. Narayanan, J. Bonneau, E. Felton, A. Miller, S. Goldfeder, Bitcoin and cryptocurrency technologies: a comprehensive introduction, Princeton University Press, Princeton NJ, 2016.
[5] S. Nakamoto, Bitcoin: a peer-to-peer electronic cash system, https://bitcoin.org/bitcoin.pdf, 2008.
[6] R.C. Merkle, A digital signature based on a conventional encryption function, Advances in Cryptography, CYPTO '87. 293, p. 369, 1988.
[7] Cypherpunks Mailing List, https://mailing-list-archive.cryptoanarchy.wiki/ Accessed 29/07/2021
[8] J. Bartlett, The dark net, Windmill Books, London, 2015.
[9] D. Gerard, Attack of the fifty foot blockchain: Bitcoin, Ethereum and smart contracts. 2018.
[10] A. Hertig, Ethereum's two Ethereums explained. Coin Desk, 2017.
[11] V. Buterin, Notes on blockchain governance, 2017.
[12] K. Levy, Book-smart, not street-smart: blockchain-based smart contracts and the social workings of law. Engaging Science, Technology and Society, 3(1), 1-15, 2017.
[13] Y. Nakamura, L.Y. Chen, Bitcoin miners signal revolt and sluggish blockchain, Bloomburg, 13/3/2017.
[14] R. Huang, The 'Chinese mining centralization' of Bitcoin and Ethereum, Forbes, 2020.
[15] B.H. Bratton, The Stack: on software and sovereignty, MIT Press, Cambridge, Massachusetts, 2016.
[16] E. Mumford, Effective systems design and requirements analysis: the ETHICS approach, Palgrave, Basingstoke, 1995.
[17] E. Ostrum, Governing the commons: the evolution of institutions for collective action, Cambridge, University Press, Cambridge New York, 1990.
[18] C.W. Clegg, Sociotechnical principles for systems design, Applied Ergonomics, 31, 463-477, 2000.
[19] S. Jasonoff, The ethics of invention: technology and the human future, W.W. Norton, New York, 2016.
[20] E.W. Bijker, Constructing worlds: Reflections on science, technology and democracy (and a plea for bold modesty). Engaging Science, Technology, and Society, 3, 315–331, 2017.
[21] S. Winter, N. Berente, J. Howison, B. Butler, Beyond the organizational "container": Conceptualizing 21st century sociotechnical work. Information and Organization, 24, 250–269. 2014.
[22] P.M. Leonardi, P.M. Theoretical foundations for the study of materiality. Information and Organization. 23(2), 59-76, 2013.
[23] W. Orlikowski, S. Scott, Sociomateriality: Challenging the separation of technology, work and organization. The Academy of Management Annals. 2(1), 433-474, 2008.
[24] D. Cecez-Kecmanovic, R.D. Galliers, O. Henfridsson, S. Newell, R. Vidgen, The sociomateriality of information systems: current status, future directions. MIS Quarterly, 38(3), 809-830, 2014.
[25] D. Haraway, D., A Cyborg Manifesto: Science, Technology, and Socialist-Feminism in the Late Twentieth Century. In Simians, Cyborgs and Women: The Reinvention of Nature, New York, Routledge, 149-181, 1991.
[26] J. Wajcman, Automation: Is it really different this time? British Journal of Sociology. 68(1), 119-127, 2017.
[27] A. Rand, Atlas Shrugged. Penguin Books, 1957.
[28] R. Dworkin, Justice for Hedgehogs. The Belknap Press of Harvard University Press, Cambridge Massachusetts, 2011.
[29] C.A. MacKinnon, Butterfly Politics, The Belknap Press of Harvard University Press, Cambridge Massachusetts, 2017.

[30] Z. Tufekci, Z. The latest data privacy debacle. *New York Times*, 30/1/18. Accessed at: https://www.nytimes.com/2018/01/30/opinion/strava-privacy.html 2018.
[31] T. Benn, Arguments for Democracy, (C. Mullins Ed.), Penguin Books, London, 1982.
[32] F. Pasquale, The Black Box Society: The secret algorithms that control money and information, Harvard University Press, Cambridge Massachusetts, 2015.
[33] D. Champion, S.K. Cibangu, M. Hepworth, M., End-user engagement in the design of communications services: lessons from the rural Congo. Information Technologies and International Development, 14(1), 18-32, 2018.
[34] S. McGee, S. Chasing Goldman Sachs: How the masters of the universe melted down Wall St. Crown Business, New York, 2011.