Article:
Zamani, E. orcid.org/0000-0003-3110-7495 (2022) The Bitcoin protocol as a system of power. Ethics and Information Technology, 24 (1). 14. ISSN 1388-1957

https://doi.org/10.1007/s10676-022-09626-1

The Bitcoin Protocol as a System of Power

In this study, I use the Critical Realism perspective of power to explain how the Bitcoin protocol operates as a system of power. I trace the ideological underpinnings of the protocol in the Cypherpunk movement to consider how notions of power shaped the protocol. The protocol by design encompasses structures, namely the Proof of Work and the Block Selection, that reproduce asymmetrical constraints on the entities that comprise it. These constraining structures generate constraining mechanisms, those of cost effectiveness and deanonymisation, which further restrict participating entities' 'power to act', reinforcing others' 'power over' them. In doing so, I illustrate that the Bitcoin protocol, rather than decentralising and distributing power across a network of numerous anonymous, trustless peers, it has instead shifted it, from the traditional actors (e.g., state, regulators) to newly emergent ones.

Keywords: decentralisation; power; Bitcoin; critical realism

Introduction

The Bitcoin protocol, when first introduced, promised to resolve issues pertaining to anonymity, decentralisation, trustlessness and transparency in digital transactions (Nakamoto, 2008a). Embracing this technology meant that peers could transact directly with one another without having to trust any single intermediary. Instead, trust would be placed on anonymous and untrusted peers thanks to cryptography (Vidan and Lehdonvirta, 2018).

Equally promising were the scenarios where the Bitcoin, as a digital payment system, could support the cause of shifting the power balance from the state and regulatory bodies to a network of peers (Ishmaev, 2020). The protocol envisioned a network of honest, distributed peers around the world, tasked with the production of bitcoins and the confirmation and validation of Bitcoin transactions. Everyone has access to this network and the ledger of transaction, thus ensuring maximum transparency.

These concepts can be traced to the ideological underpinnings of the Cypherpunk Manifesto (Swartz, 2018), where similarly, privacy and anonymity are emphasised (Ishmaev, 2020), and it is these principles that sparked the interest of Bitcoin's early adopters (Hayes, 2019b).

However, a little over ten years after since its introduction, the Bitcoin has gone into the mainstream and much of the discourse is centred around its price and its potential as an investment (e.g., Koutmos, 2019; Mattke et al., 2020; Philippas et al., 2019) rather than the action possibilities it can offer for anonymous, private transactions. The dream about shifting the power balance seems to have been forgotten entirely, which seems counterintuitive considering that digital technologies have always had the ability to disrupt established institutions, such as economic and political (Wedel, 2017).

In this study I present the Bitcoin protocol as a system of power (Palermo, 2007; Tool and Samuels, 1989). I do this by exploring who holds the power in this system, how power is used and what are the consequences of this use. The objective is to illustrate that, by design, purposefully or not, the protocol is in conflict with its original principles.

I advance my arguments as follows. In the next section, I present in detail the ideological underpinnings of the Bitcoin and I discuss how these have influenced the shape and functions of the protocol. The following two sections present an overview of different perspectives of power in relation to technology, paying particular attention to the Critical Realism perspective of power, which I employ for this study. I then provide my analysis of the Bitcoin protocol as a system of power, where I focus on the constraining structures and the constraining mechanisms that comprise this system.

The Ideology of the Bitcoin Protocol

Much of the legacy of the Cypherpunk movement can be observed in the Bitcoin protocol, particularly through the latter's focus on privacy and anonymity and the emphasis on trusting the code (West, 2021). Cypherpunks underline that "each party to a transaction [should] have knowledge only of that which is directly necessary for that transaction" (Hughes, 1993). This level of privacy in digital transactions can only be achieved via "anonymous transaction systems" that empower individuals to "reveal their identity when desired and only when desired" (Hughes, 1993). The Bitcoin protocol materialises this through the use of public key cryptography (Brito and Castillo, 2013), where a sender signs a transaction with their private key and the receiver decode the encoded transaction with their public key (Hayes, 2019b)

Cypherpunks also value openness, transparency (Corradi and Höfner, 2018), and distributed systems that are maintained by the many (Beltramini, 2020). In this light, code should be freely available to all, so that it is auditable and free to use, in the hope that "a widely dispersed system can't be shut down" (Hughes, 1993). The Bitcoin protocol essentially puts forward the idea of a large, peer-to-peer network that anybody can access. The peers are in the network, who 'mine' new bitcoins by executing on their computers computationally-heavy tasks (Corradi and Höfner, 2018). The protocol's code is publicly available, thus auditable.

However, the core tenet of the Cypherpunk Manifesto is that of distrust and scepticism towards central government and the role of corporations, and this is what seems to have primarily influenced most crucially the Bitcoin. Cypherpunks argue that it is unreasonable to "expect governments, corporations, or other large, faceless organizations to grant us privacy out of their beneficence. It is to their advantage to speak of us, and we should expect that they will speak" (Hughes, 1993). It is this scepticism and distrust that anonymity and privacy are perceived as absolute requirements for digital transactions and why it is perceived imperative to resist institutionalized authority (Coleman and Golub, 2008). In a sense, cryptography and code are seen as the means for people to remain autonomous, self-reliant and in control of their data, and their defence against “organized surveillance” (Gürses et al., 2016: 583).

The Bitcoin has been shaped by this distrust towards institutional power (Teng, 2021) as it is meant to be a form of “pure algorithmic governance” (Zook and Blankenship, 2018: 248) that cannot be corrupted, controlled nor affected by governmental interventions (Nakamoto, 2008b). It provides an algorithmic infrastructure that can be trusted without having to trust the peers themselves. In other words, trust is taken away from institutions (Westphal, 2015), and is placed in the code (Vidan and Lehdonvirta, 2018), while circumventing government monopoly (Corradi and Höfner, 2018) and third parties, who are perceived as corrupt (De Filippi and Loveluck, 2016).

Against this background, the Bitcoin protocol has been termed to be the technological expression of a libertarian’s dream (Corradi and Höfner, 2018; De Filippi, 2014; Zook and Blankenship, 2018), which does not necessarily resonates with Cypherpunks, a highly heterogenic group (Beltramini, 2020). What they do have in common, however, is that neither Bitcoin adopters nor Cypherpunks reject the idea of power but rather question its form. Both reject legislation and social norms, question authorities and consider them corrupt, but support the idea of free market and the use of a reputational system, inscribed in code, for regulating the market (Beltramini, 2020; Bertelloni, 2017).

Power and Technology

Power is the ability to do or not to do something (‘power to act’), and the ability to impact another’s actions (‘power over’ somebody). These two forms of power should be considered together against the decision-making set that allows an entity to adopt a potential set of actions (Palermo, 2007). In other words, ‘power over’ suggests that an entity has and may exercise their ‘power over’ somebody only when there is some type of a dependency relationship between them, i.e., the individual depends on the actions of the entity (Palermo, 2007, 2014). What this means is that, ‘power to act’ and ‘power over’ are inevitable intertwined as ‘power over’ depends on and draws from the distribution of ‘power to act’ within a system, such as that of society (Sayer, 2012).

Interest around power has been steadily growing (Rowlands and Kautz, 2021), potentially as a response to the existence of power asymmetries among different groups within a rapidly digitalised society (Kania-Lundholm and Torres, 2018). To date, it has been conceptualised and operationalised from numerous perspectives: from a capitalistic perspective, it is considered as non-existent, whereas this may not be the case for bounded systems (e.g., organisations). Generally, how power is approached depends on how interpersonal relationships are viewed and understood, i.e., the understanding regarding their existence or absence. For example, in capitalism and perfectly competitive markets interpersonal relationships are considered irrelevant, and therefore ‘power to act’ is considered unrestricted (Palermo, 2014); individuals are seen as able to disengage from interpersonal relationships and resist the exercised authority (Vatiero, 2010). Yet, in reality, society is characterised by asymmetries (Gershenson, 2015), where everyone is connected one way or another to everyone else, and power is asymmetrically distributed (Palermo, 2007).

In line with this relational view of power, one of the most influential perspectives is probably Foucault’s. Foucault argues that power can be observed only when enacted (Foucault, 1979). As such, power is not something that can be possessed but only exercised (Rowlands and Kautz, 2021). Therefore it indicates the capacity to act but also necessitates resistance (Willcocks, 2004) which exists on the basis of social relationships

(Doolin, 2004). However, because of these social relationships and practices, power can become internalised and institutionalised, and its impact may be then observed not only when directly enacted by the actor, but as experienced by others via its apparatuses (Doolin, 2004). The Foucauldian approach, however, pays less attention to underlying structures and mechanisms with a bearing on the enactment of power and its outcomes (Sayer, 2012). Therefore the Foucauldian approach does not easily lend itself for the investigation of social actions and structural constraints, where the focus is placed on how technology supports or inhibits material and social constructions.

Another perspective to power is the radical one, which is underpinned by social relationships but further rooted within structures and rules (Bradshaw-Camball and Murray, 1991). Power is a restraining force, when it is exercised as 'power over' (Clegg et al., 2006) and is used to control and coerce (Lawrence et al., 2012) or it can be a productive one when it is envisaged as 'power to' (Clegg et al., 2006). Such a perspective is more aligned with the critical scholarship of technology that approaches it as both an opportunity and a risk, or better put, as "both progressive and regressive", with the ability to empower and disempower (Kania-Lundholm and Torres, 2018: 1168).

This perspective, I believe, is rather pertinent as it draws attention to agency and the technology's constraining/supportive role. On the one hand, technology should be seen as in interaction with its user. As part of this process, both the technology and the user will shape each other through their interaction and as a result of their exposure to each other (Orlikowski and Scott, 2008). On the other hand, technologies can be means to control and monitor, objects with inscribed societal and organisational rules with the intention to communicate them and enforce them (Medaglia et al., 2021).

However, in a world where technologies, entities, rules and structures are enmeshed together and interconnected to each other, it is difficult, if not impossible, to conclusively identify the power asymmetries and dynamics. There may exist multiple relationships among potentially unknown entities as well as known and unknown structures with a bearing on the power dynamics. In other words, and within the context of the Bitcoin protocol in particular, as it currently operates, there could be broader forces, outside of our immediate observation, that determine the distribution of power among its original developers, the miners who maintain the network, states and institutions that seek to regulate it or participate in it, and others who may be impacted by the power differentials. To address and overcome this, in the next section, I adopt the critical realism perspective to power (Palermo, 2007; Sayer, 2012), which considers the constraints of social structures and mechanisms, and allows tracing causality within these power relations (Mingers and Standing, 2017; Sayer, 2012).

A Critical Realism Perspective to Power

Critical realism posits that our world exists independently from our own knowledge of it, but further argues that we are only able to observe solely a fraction of it (Bhaskar, 1997). This suggests that entities and structures can be understood and interpreted through a subjective lens, constructed by our own sociocultural perceptions (Mingers, 2004).

Adopting the Critical Realism perspective entails differentiating between the real, the actual and the empirical domains of reality (Lau, 2004). The actual domain contains generated events and the empirical domain contains a subset of them and specifically those that are observed and experienced (Mingers and Standing, 2017). In other words, the actual domain lends itself to the events that can potentially occur, but the empirical domain encompasses those that both occur and are observable (Mingers et al., 2013). The importance of Critical Realism reveals itself when moving to the domain of the real, which contains the causal generative mechanisms (Lau, 2004). Generative mechanisms are what make things happen and may be things and structures, observable or not, that trigger the events that exist in the actual domain (Blom and Morén, 2011). However, whether the generative mechanisms will be activated or not largely depends on contextual factors (Henfridsson and Bygstad, 2013). In other words, the extent to which the generative mechanisms will lead to changes and events in the actual and the empirical domains depends on underlying factors and prerequisite conditions that characterise the phenomenon. Identifying the generative mechanisms then becomes a theoretical task, as it is impossible to do so otherwise, considering the openness of social structures and the unfeasibility of experimenting directly with these (Lau, 2004). However, experience, knowledge and observations can support the endeavour of appreciating the causal explanations (Volkoff and Strong, 2013).

Critical realism, as an ontology, offers the epistemological basis for exploring power more systematically (Sayer, 2012) and supports an investigation into systemic effects and non-observable structures (Palermo, 2007). The question then becomes whether, how and why power is activated, which rests on identifying the interdependencies and interrelationships among entities within the power system. When power is indeed activated, the question shifts to examine to what extent others are vulnerable to the exercised power (Sayer, 2012).

Bitcoin: A System of Power

I argue that the Bitcoin protocol is a system of power (Palermo, 2007; Tool and Samuels, 1989) and I demonstrate the structures and mechanisms that rule the power distribution within it. Through the lens of Critical Realism, I explore the asymmetric power distribution that exists within the protocol and I unpack the constraining structures and the constraining mechanisms that transfigure the Bitcoin protocol into a system of power. Following the tradition of Critical Realism, I focus solely on those features that transform the Bitcoin protocol into an *observed* system of power[1]. In doing so, I revisit the origins of the protocol and explain why the technology departs from its ideological origins.

Constraining Structures

Sayer emphasises "the importance of structures in the generation of power" (Sayer, 2012: 180) in order to understand power itself. From a Critical Realism perspective, the power of an entity exists "in virtue of the structure of [that entity]" (Sayer, 2012: 181) and draws its influence from exogenous structures, and particularly those that are enduring and interact with endogenous structures.

Positioning this within the context of the Bitcoin protocol, I identify three main structural elements that bear resemblance to such constraining structures. I refer to the *Proof of Work*, the *Block Selection and the concept of trustlessness*[2].

The Proof of Work (PoW) represents the consensus algorithm for confirming transactions and for mining new bitcoins[3] (Reid and Harrigan, 2013). The algorithm requires peers (called miners) in the peer-to-peer network to use computing power to solve mathematical problems towards identifying the next block to be added in the

[1] It is not my intention to offer a detailed technical account of the Bitcoin protocol. For a detailed description, I direct the reader to Narayanan et al. (2016) who offer a comprehensive introduction.

[2] There are additional structures in the Bitcoin protocol, as for example the underlying rules of cryptography; these are not referred to here, because comparatively, they are far less crucial as constraining structures for the protocol.

[3] I refer to the Bitcoin protocol as 'Bitcoin' (capital first letter), and to bitcoins (i.e., the cryptocurrencies) as 'bitcoins' (lower case first letter).

Blockchain (Bitcoin Wiki, 2019). This is a computationally intensive process, which increases in difficulty by design as the computing power of the network increases, so that the rate of block identification remains stable over time (Karlstrøm, 2014).

The Block Selection reflects the process through which miners compete against each other to identify the next block. Miners race against each other to solve a mathematical problem and broadcast their PoW, the latter being essentially the validation of their solution (Aggarwal et al., 2019). Once the solution is confirmed by enough peers, the miner who first broadcasted their solution is rewarded in bitcoins. This, again, is a resource intensive computational task (Eyal and Sirer, 2018), and the probability of a miner identifying a valid block will always be proportional to their computing power relatively to that of the network: *"Anyone's chance of finding a solution at any time is proportional to their CPU proof-of-worker"* (Nakamoto, 2008c).

While the protocol can be updated and revised via improvements following clear network consensus (Parkin, 2019), these structures have remained fairly stable as far as their role in power distribution is concerned, since introduced improvements have not shifted the power balance. As such, the PoW and Block Selection are structures located in the real domain with enduring properties and impacts on where power is located and how it is exercised and distributed. What needs to be examined, in turn are how these structures translate into further power asymmetries in the actual domain, where an entity in the network exercise its 'power over' another by restricting the latter's 'power to act' (Palermo, 2007; Wrenn, 2017).

In combination, the PoW and Block Selection result in adverse events in the actual domain. In the first few years, mining was done via the computer's Central Processing Unit (CPU). As the popularity of the Bitcoin increased, more and more miners started joining the network, boosting its overall computing power, increasing the difficulty of the

PoW (Hayes, 2019a). Soon, mining via CPUs was no longer profitable and miners begun using advanced graphic cards (i.e., GPUs typically used for gaming and creative work) and later Application Specific Integrated Circuits (ASICs), specifically designed for mining. Both solutions carry high costs: the adoption of GPUs resulted in extreme price surges and out-of-stocks, with collateral impacts on individuals and businesses outside the Bitcoin world (Kain, 2021), while mining via ASICs, although comparatively more energy efficient, has a debatable return on investment for independent miners (Cryptimi, 2019). Similarly, Block Selection has had detrimental effects for independent miners. Because the incentives are high (12.5 bitcoins at the time of writing), miners resort to trial-and-error approaches (Maurer et al., 2013), which requires, again, increased computing power to ensure they are the first to broadcast a valid PoW and thus receive the mining reward (Gervais et al., 2014).

Both structures are underpinned by computing power, and as shown, computing power translates in financial resources (Gervais et al., 2016). To lower operational costs while increasing computing power and therefore maximise the prospects of receiving the rewards for their mining efforts, miners opt to join mining pools (Khairuddin and Sas, 2019), i.e., they pool their computing power and mine as a single entity, which ultimately transformed the mining process into an oligopoly (Arnosti and Weinberg, 2018; Gervais et al., 2014). This seems counterintuitive to Nakamoto's mantra of "one-CPU-one-vote" (Nakamoto, 2008a: 3), because power is no longer decentralised nor distributed across many, equal nodes, but rather centralised in and consolidated by powerful nodes (Baldwin, 2018; Vidan and Lehdonvirta, 2018), who are represented by few mining pools. This concentration restricts the decision making set of independent miners ('power to act') and expands that of mining pools ('power over').

Next, trustlessness is “based on cryptographic proof instead of trust (Nakamoto, 2008a: 1). It is this trustlessness that ensures anonymity and privacy and makes third parties (e.g., escrow services) redundant for confirming transactions (Vidan and Lehdonvirta, 2018). It is clear that the participation of third parties for e.g., buying and selling bitcoins, was never envisioned because transactions were designed to take place “directly from one party to another without going through a financial institution” (Nakamoto, 2008a: 1). However, acquiring bitcoins directly through mining is a complex, costly and time consuming task (Khairuddin and Sas, 2019), and requires a certain technical skill set. The above are essentially barriers towards the adoption of the protocol beyond Bitcoin enthusiasts and tech savvy individuals (Zamani and Giaglis, 2018).

Moving from the real to the actual domain, and as the Bitcoin started entering the vernacular, awareness and interest started picking up. Parties, previously intentionally excluded by the peer-to-peer network, identified new opportunities. I refer to the emergence of cryptocurrency exchanges that provide a connection between the Bitcoin protocol and the economy, and through which buyers and sellers can trade bitcoins for fiat money (Li and Wang, 2017). While these exchanges have proven useful, they also have increased ‘power over’ their customers. To gain access to these services, a customer needs to identify themselves by providing name, address, nationality, and often a telephone number, and these personal details need in turn to be verified via a government ID (e.g., passport, driving licence) and documentation that matches the provided address (e.g., a utility bill). While these requirements are part of the service’s regulatory obligations (Know Your Customer - KYC), in effect, these exchanges exercise ‘power over’ their customers, who have less ‘power to act’, especially in cases they have transferred bitcoins to the exchange already: unless the information is provided, the exchange can withhold funds, deny their services and choose to report their customers to the relevant regulator.

Mechanisms that Constrain

Constraining mechanisms lend themselves to explain the phenomena we observe in the empirical domain (Nicholson et al., 2013). With regards to the Critical Realism ontology of power in particular, constraining mechanisms explain how or why constraining structures evolve and get reproduced (Palermo, 2007). These mechanisms will include actors who may be external to the system but with a stake in, and these may comprise of the state, financial institutions, such as central banks, the cryptocurrency exchanges, large mining pools that control the production of bitcoins and others.

The cost effectiveness mechanism

Today, the start-up and operational costs, coupled with the intense competition and the ever decreasing rewards considerably outweigh the potential profits from independent mining (Taylor, 2017). Therefore, joining a mining pool may be the only option as it increases miners' financial prospects (Maurer et al., 2013). Mining rewards, however, are 'won' by the mining pool and then distributed across participating miners based on the reward scheme of the pool (Dziembowski, 2015). In other words, mining is a financially viable operation only when financial gains exceed operational costs (Derks et al., 2018), controlling for the collective computing power of the pool one has joined. I call this the cost effectiveness mechanism. What is interesting is to explore how this mechanism interacts with the miners' decision making for joining a given pool because it helps understand the extent and the intensity of the pool's 'power over' independent miners, and in turn, over the network.

Largely, there are three factors that influence the decision to join a pool: the reward mechanism employed by the pool (Qin et al., 2018); the size of the pool; and the reputation of the pool (Khairuddin and Sas, 2019). However, the cost effectiveness mechanism, once activated, will restrict the decision-making set of independent miners. A pool may have a better reward scheme overall, but choose not to share with miners how rewards are distributed across miners, resulting in low transparency. One could argue that miners could exercise agency (‘power to act’) and join other pools, or switch pools in response, and in fact, many do so. At the same time, however, when it comes to a large pool, miners’ decision-making set is restricted because pool size reflects the pooled computing power, and therefore it is a proxy for the prospects of collaboratively identifying the next block (bitcoin wiki, 2011). Therefore, remaining within a large pool, despite the low transparency, may make financial sense, which indicates that miners’ ‘power to act’ is restricted, whereas large pools’ ‘power over’ expands.

The activation of this mechanism results in further events in the domain of the empirical. Currently, there are some very large mining pools, e.g., Poolin and F2Pool, followed by several, smaller ones (Figure 1). Some have maintained their presence over time, but their size fluctuates and others have vanished altogether (e.g., BTC.com), as miners moved to other pools (Figure 2). At the same time, findings have shown that an increased majority resides in China (Mariem et al., 2020; Stoll et al., 2019), due to the lower electricity costs (Bendiksen and Gibbons, 2019), against the government’s policy and possibly as a form of dissent (Huang, 2020), suggesting that the computing power of the network is anything but decentralised and distributed. Instead, it is mostly concentrated in a single country (Peck, 2017; Tuwiner, 2019).

The concentration of hashing power by few large mining pools has been of concern with regards to the security of the network (Zamani et al., 2020). In theory, if any one entity concentrates more than 51% of hashing power, it can proceed with double spending, i.e., transmit fraudulent transactions. The protocol does not contain any particular mechanisms to safeguard against this, the assumption being that the computing power would always be sufficiently decentralised, and that the costs for executing such an attack would always outweigh the financial incentives (Nakamoto, 2008a). Thus far, such an attack has never been launched against the Bitcoin network but there have been few successful ones against other cryptocurrency protocols (MIT media lab, 2021).

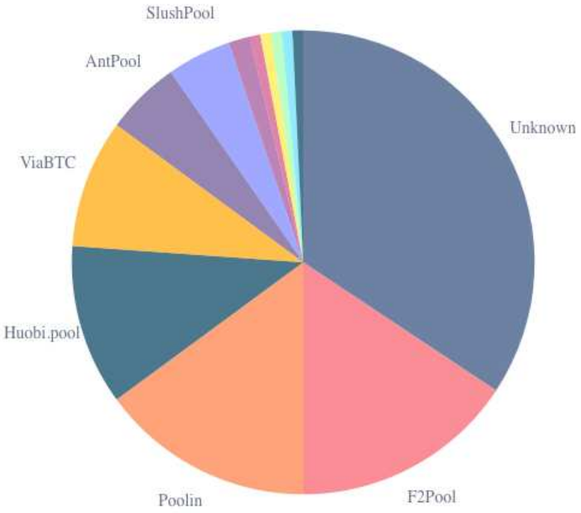

Figure 1. Hashrate distribution in May 7th, 2021. 'Unknown' means that Blockchain.info was unable to determine the origin (Blockchain.com, 2021a).

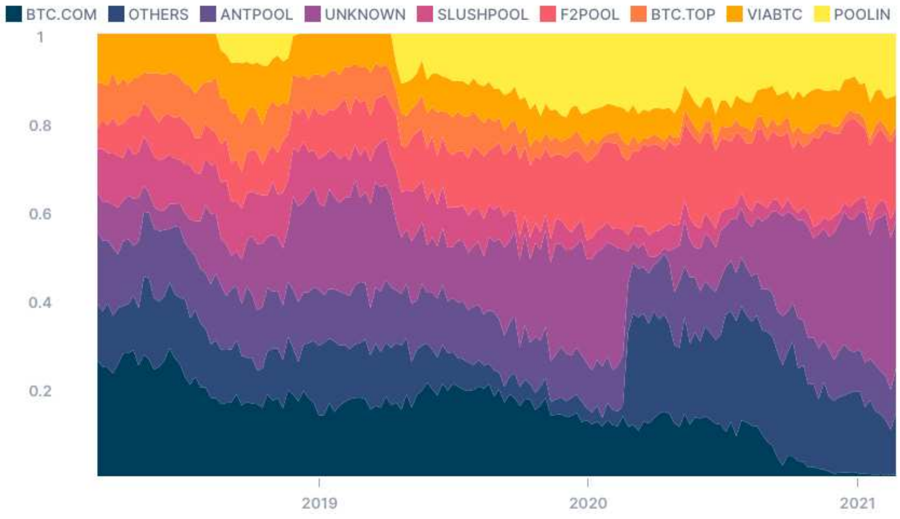

Figure 2. Hashrate distribution over the last three years among the largest mining pools (until March 7th, 2021) (Blockchain.com, 2021b).

The deanonymisation mechanism

The emergence of cryptocurrency exchanges has resulted in market cybermediation: new intermediaries offer their services and allow parties to transact without having to worry for the practicalities of the transaction (Author removed, 2018). For all purposes, these exchanges have created in effect traditional, online marketplaces (Bakos, 1998), where buyers and sellers locate each other, they agree between them on a price for buying and selling bitcoins for fiat money, and the marketplace, i.e., the exchange, monitors and documents the transaction for a fee. While these exchanges offer their services to those participating in the Bitcoin protocol, essentially they operate in the world outside of it and thus are subject to the same regulatory obligations as typical financial services, which is what activates the mechanism of deanonymisation. The activation of this mechanism suggests that these exchanges function as 'gatekeepers' (Vidan and Lehdonvirta, 2018) who act on behalf of the regulator, i.e., the state, for the purpose of tracking fraudulent and illicit activities, because both the state and society have an interest to prevent or intercept them where possible.

Anonymity and the role of the state are core for appreciating the nature of this mechanism and the extent and the intensity of the exchanges' 'power over'. Bitcoin offers nearly perfect anonymity (Meiklejohn et al., 2016). Considering that the state applies taxiation when one's net worth increases, profits from selling Bitcoin should be taxed (Bal, 2015). However, anonymity, coupled with the potential significant profits one can make by trading bitcoins (Feng et al., 2018), pose a challenge for the state in identifying the traders for the purposes of taxation (Bjerg, 2016). In other words, the state has a stake in the system, and for this purpose, it exerts its 'power over' it via its gatekeepers, who activate the deanonymisation mechanism, not only for the purpose of combatting illicit activities but, possibly more importantly, for the purpose of ensuring taxation.

The activation of this mechanism breaks the protocol's promise of anonymity. When seen from a different vantage point, this is a constraining mechanism outside the protocol, within the real domain, that still necessitates the authentication and the integrity of users and the legality of the transactions, with the only difference being that the authority for doing so, and therefore 'power over', has been delegated to the exchanges.

Conclusions

The existence of constraining structures and the emergence of constraining mechanisms influences the decision-making set of the entities participating in a system, which is what makes that system a system of power (Palermo, 2007). Within the Bitcoin protocol, I have emphasised the constraining structures of the Proof of Work, Block Selection and Trustlessness to showcase how these enable and restrict different decision-making sets among the participating entities of the network. Technologies are often used in ways other than originally designed or imagined (Orlikowski and Baroudi, 1991) and all too often it is their very design that affords uses that restrict and constraint (Markus, 1983). In the case of the Bitcoin protocol, each of the three constraining structures limits independent miners' 'power to act' and magnifies large mining pools' 'power over' them, but in addition, these structures interact and reinforce each other further. Mining requirements today are not simply excessively high in terms of equipment and electricity. Mining as part of a mining pool suggests increased computational power for that pool, and in turn significantly increased prospects to receive mining rewards comparatively to mining independently, because it is by design a competitive process ('power over'). As a result, independent mining becomes impossible, and the network's computing power gets concentrated within few very large pools, but also geographically.

The constraining structures provide the background for the emergence of the constraining mechanisms of cost effectiveness and deanonymisation. These two mechanisms, once triggered, they restrict participants' 'power to act' by limiting their decision-making set. I consider these mechanisms to be endogenous, in the sense that, they result from the endogenous structural components of the protocol, despite being subject to exogenous influences, such as the regulatory obligations residing outside of the protocol.

These two mechanisms and, most importantly, to the events that these generate in the empirical domain, bear witness to the fact that essentially the Bitcoin protocol still hasn't delivered on its promise for decentralisation, power distribution, privacy and anonymity. Instead, power (computing power, and thus power to control the network) has been centralised and concentrated both within few very large pools and geographically. The power balance has not shifted either, but rather it has been delegated from the traditional actors, such as the state and central banks, to new actors (cryptocurrency exchanges) who have become the new regulators and function as an extension of the state. In other words, despite the fact that for many the Bitcoin protocol started off as an incarnation of the Cypherpunk movement (Beltramini, 2020; Swartz, 2018), today it has moved away from it, and "is characterized by asymmetries of wealth and power that are not dissimilar from the mainstream financial system" (Dodd, 2018: 35).

Naturally, there may be other constraining structures and mechanisms, which I have not explored in this paper. The ones I identify are those that I consider as being stable, with a persistent influence over the Bitcoin's system of power. In the Critical Realism tradition, they are also those that I have managed to observe based on my subjective lens (Mingers, 2004). The same, and other mechanisms may generate events in the future, which can be both temporary or equally stable (Mingers and Standing, 2017), which would make for an interesting subsequent study on the observed tendencies and consequences of the Bitcoin system, potentially further exploring economic and social relationships among the participating entities of the network.

References

Aggarwal S, Chaudhary R, Aujla GS, et al. (2019) Blockchain for smart communities: Applications, challenges and opportunities. *Journal of Network and Computer Applications* 144: 13–48. DOI: 10.1016/j.jnca.2019.06.018.

Arnosti N and Weinberg MS (2018) Bitcoin: A natural oligopoly. In: *10th Innovations in Theoretical Computer Science Conference (ITCS 2019)*, Cambridge, Massachusetts, 2018. DOI: 10.4230/LIPIcs.ITCS.2019.5.

Bakos Y (1998) The emerging role of electronic marketplaces on the Internet. *Communications of the ACM* 41(8): 35–42. DOI: 10.1145/280324.280330.

Bal A (2015) How to Tax Bitcoin? In: *Handbook of Digital Currency*. Elsevier, pp. 267–282. DOI: 10.1016/B978-0-12-802117-0.00014-X.

Baldwin J (2018) In digital we trust: Bitcoin discourse, digital currencies, and decentralized network fetishism. *Palgrave Communications* 4(1). 1. Palgrave: 1–10. DOI: 10.1057/s41599-018-0065-0.

Beltramini E (2020) Against technocratic authoritarianism. A short intellectual history of the cypherpunk movement. *Internet Histories*: 1–18. DOI: 10.1080/24701475.2020.1731249.

Bendiksen C and Gibbons S (2019) *The Bitcoin Mining Network - Trends, Composition, Average Creation Cost, Electricity Consumption & Sources*. 3 December. CoinShares Research. CoinShares Group.

Bertelloni MB (2017) The Cypherpunk Vision of Techno-Politics. *St. Anne's Academic Review, University of Oxford* (7): 1–7.

Bhaskar R (1997) *A Realist Theory of Science*. Verso.

bitcoin wiki (2011) Mining pool reward FAQ. Available at: https://en.bitcoin.it/wiki/Mining_pool_reward_FAQ (accessed 14 August 2018).

Bitcoin Wiki (2019) Hashcash - Bitcoin Wiki. Available at: https://en.bitcoin.it/wiki/Hashcash (accessed 9 May 2019).

Bjerg O (2016) How is Bitcoin Money? *Theory, Culture & Society* 33(1): 53–72. DOI: 10.1177/0263276415619015.

Blockchain.com (2021a) Hashrate Distribution. Available at: https://www.blockchain.com/charts/pools (accessed 7 March 2021).

Blockchain.com (2021b) Hashrate Distribution Time Series. Available at: https://www.blockchain.com/charts/pools-timeseries (accessed 7 March 2021).

Blom B and Morén S (2011) Analysis of Generative Mechanisms. *Journal of Critical Realism* 10(1): 60–79. DOI: 10.1558/jcr.v10i1.60.

Bradshaw-Camball P and Murray VV (1991) Illusions and Other Games: A Trifocal View of Organizational Politics. *Organization Science* 2(4): 379–398. DOI: 10.1287/orsc.2.4.379.

Brito J and Castillo A (2013) *Bitcoin: A Primer for Policymakers*. Mercatus Center at George Mason University.

Clegg S, Courpasson D and Phillips N (2006) *Power and Organizations*. Thousand Oaks, CA: Sage.

Coleman EG and Golub A (2008) Hacker practice: Moral genres and the cultural articulation of liberalism. *Anthropological Theory* 8(3): 255–277. DOI: 10.1177/1463499608093814.

Corradi F and Höfner P (2018) The disenchantment of Bitcoin: unveiling the myth of a digital currency. *International Review of Sociology* 28(1): 193–207. DOI: 10.1080/03906701.2018.1430067.

Cryptimi (2019) How Long Does It Take To Mine Bitcoin? In: *Cryptimi*. Available at: https://www.cryptimi.com/guides/how-long-does-it-take-to-mine-bitcoin (accessed 7 March 2021).

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

https://policyreview.info/articles/analysis/bitcoin-regulatory-nightmare-libertarian-dream (accessed 2 May 2019).

De Filippi P and Loveluck B (2016) The invisible politics of Bitcoin: governance crisis of a decentralised infrastructure. Internet Policy Review. *Internet Policy Review* hal-01382007. Available at: https://hal.archives-ouvertes.fr/hal-01382007.

Derks J, Gordijn J and Siegmann A (2018) From chaining blocks to breaking even: A study on the profitability of bitcoin mining from 2012 to 2016. *Electronic Markets* 28(3): 321–338. DOI: 10.1007/s12525-018-0308-3.

Dodd N (2018) The Social Life of Bitcoin. *Theory, Culture & Society* 35(3): 35–56. DOI: 10.1177/0263276417746464.

Doolin B (2004) Power and resistance in the implementation of a medical management information system. *Information Systems Journal* 14(4): 343–362. DOI: 10.1111/j.1365-2575.2004.00176.x.

Dziembowski S (2015) Introduction to Cryptocurrencies. In: 2015, pp. 1700–1701. ACM Press. DOI: 10.1145/2810103.2812704.

Eyal I and Sirer EG (2018) Majority is not enough: bitcoin mining is vulnerable. *Communications of the ACM* 61(7): 95–102. DOI: 10.1145/3212998.

Feng W, Wang Y and Zhang Z (2018) Informed trading in the Bitcoin market. *Finance Research Letters* 26: 63–70. DOI: 10.1016/j.frl.2017.11.009.

Foucault M (1979) *Discipline and Punish: The Birth of the Prison*. London, UK: Peregrine.

Gershenson C (2015) Protecting Markets from Society: Non-Pecuniary Claims in American Corporate Democracy. *Politics & Society* 43(1): 33–60. DOI: 10.1177/0032329214559182.

Gervais A, Karame GO, Capkun V, et al. (2014) Is Bitcoin a Decentralized Currency? *IEEE Security & Privacy* 12(3): 54–60. DOI: 10.1109/MSP.2014.49.

Gervais A, Karame GO, Wüst K, et al. (2016) On the Security and Performance of Proof of Work Blockchains. In: *2016 ACM SIGSAC Conference on Computer and Communications Security - CCS'16*, Vienna, Austria, 2016, pp. 3–16. ACM Press. DOI: 10.1145/2976749.2978341.

Gürses S, Kundnani A and Van Hoboken J (2016) Crypto and empire: the contradictions of counter-surveillance advocacy. *Media, Culture & Society* 38(4): 576–590. DOI: 10.1177/0163443716643006.

Hayes A (2019a) Bitcoin price and its marginal cost of production: support for a fundamental value. *Applied Economics Letters* 26(7): 554–560. DOI: 10.1080/13504851.2018.1488040.

Hayes A (2019b) The Socio-Technological Lives of Bitcoin. *Theory, Culture & Society* 36(4): 49–72. DOI: 10.1177/0263276419826218.

Henfridsson O and Bygstad B (2013) The Generative Mechanisms of Digital Infrastructure Evolution. *MIS Quarterly* 37(3): 907–931.

Huang R (2020) The 'Chinese Mining Centralization' Of Bitcoin And Ethereum. Available at: https://www.forbes.com/sites/rogerhuang/2021/12/29/the-chinese-mining-centralization-of-bitcoin-and-ethereum/ (accessed 11 March 2021).

Hughes E (1993) A Cypherpunk's Manifesto. Available at: http://www.activism.net/cypherpunk/manifesto.html (accessed 5 February 2019).

Ishmaev G (2020) Sovereignty, privacy, and ethics in blockchain-based identity management systems. *Ethics and Information Technology*. DOI: 10.1007/s10676-020-09563-x.

Kain E (2021) Bad News: Graphics Card Prices Are Skyrocketing And There's No End In Sight. Available at: https://www.forbes.com/sites/erikkain/2021/01/06/bad-news-graphics-card-prices-are-skyrocketing-and-theres-no-end-in-sight/ (accessed 7 March 2021).

Kania-Lundholm M and Torres S (2018) Ideology, power and inclusion: using the critical perspective to study how older ICT users make sense of digitisation. *Media, Culture & Society* 40(8): 1167–1185.

Karlstrøm H (2014) Do libertarians dream of electric coins? The material embeddedness of Bitcoin. *Distinktion: Scandinavian Journal of Social Theory* 15(1): 23–36. DOI: 10.1080/1600910X.2013.870083.

Khairuddin IE and Sas C (2019) An Exploration of Bitcoin Mining Practices: Miners' Trust Challenges and Motivations. In: *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, New York, NY, USA, 2 May 2019, pp. 1–13. CHI '19. Association for Computing Machinery. DOI: 10.1145/3290605.3300859.

Koutmos D (2019) Market risk and Bitcoin returns. *Annals of Operations Research*. DOI: 10.1007/s10479-019-03255-6.

Lau RWK (2004) Critical Realism and News Production. *Media, Culture & Society* 26(5): 693–711. DOI: 10.1177/0163443704045507.

Lawrence TB, Malhotra N and Morris T (2012) Episodic and Systemic Power in the Transformation of Professional Service Firms: Power in the Transformation of Professional Firms. *Journal of Management Studies* 49(1): 102–143. DOI: 10.1111/j.1467-6486.2011.01031.x.

Li X and Wang CA (2017) The technology and economic determinants of cryptocurrency exchange rates: The case of Bitcoin. *Decision Support Systems* 95: 49–60. DOI: 10.1016/j.dss.2016.12.001.

Mariem SB, Casas P, Romiti M, et al. (2020) All that Glitters is not Bitcoin – Unveiling the Centralized Nature of the BTC (IP) Network. In: *NOMS 2020 - 2020 IEEE/IFIP Network Operations and Management Symposium*, Budapest, Hungary, April 2020, pp. 1–9. IEEE. DOI: 10.1109/NOMS47738.2020.9110354.

Markus ML (1983) Power, Politics, and MIS Implementation. *Communications of the ACM* 26(6): 430–444.

Mattke J, Maier C, Reis L, et al. (2020) Bitcoin investment: a mixed methods study of investment motivations. *European Journal of Information Systems*: 1–25. DOI: 10.1080/0960085X.2020.1787109.

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. DOI: 10.1080/10350330.2013.777594.

Medaglia R, Eaton B, Hedman J, et al. (2021) Mechanisms of power inscription into IT governance: Lessons from two national digital identity systems. *Information Systems Journal*: isj.12325. DOI: 10.1111/isj.12325.

Meiklejohn S, Pomarole M, Jordan G, et al. (2016) A fistful of Bitcoins: characterizing payments among men with no names. *Communications of the ACM* 59(4): 86–93.

Mingers J (2004) Real-izing information systems: critical realism as an underpinning philosophy for information systems. *Information and Organization* 14(2): 87–103. DOI: 10.1016/j.infoandorg.2003.06.001.

Mingers J and Standing C (2017) Why things happen – Developing the critical realist view of causal mechanisms. *Information and Organization* 27(3): 171–189. DOI: 10.1016/j.infoandorg.2017.07.001.

Mingers J, Mutch A and Willcocks L (2013) Critical Realism in Information Systems Research. *MIS Quarterly* 37(3): 795–802.

MIT media lab (2021) 51% Attacks. Available at: https://dci.mit.edu/51-attacks (accessed 11 March 2021).

Nakamoto S (2008a) Bitcoin: A peer-to-peer electronic cash system. *Nakamoto Institute*. Available at: http://nakamotoinstitute.org/bitcoin/.

Nakamoto S (2008b) Bitcoin P2P e-cash paper. mail-archive.com. Available at: https://www.mail-archive.com/cryptography@metzdowd.com/msg09971.html (accessed 6 March 2021).

Nakamoto S (2008c) Cryptography Mailing List. Bitcoin P2P e-cash paper. Available at: https://satoshi.nakamotoinstitute.org/emails/cryptography/13/ (accessed 10 May 2019).

Narayanan A, Bonneau J, Felten E, et al. (2016) *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press.

Nicholson J, Tsagdis D and Brennan R (2013) The structuration of relational space: Implications for firm and regional competitiveness. *Industrial Marketing Management* 42(3): 372–381. DOI: 10.1016/j.indmarman.2013.02.013.

Orlikowski W and Baroudi JJ (1991) Studying Information Technology in Organizations: Research Approaches and Assumptions. *Information Systems Research* 2(1): 1–28.

Orlikowski W and Scott SV (2008) Sociomateriality: Challenging the Separation of Technology, Work and Organization. *The Academy of Management Annals* 2(1): 433–474.

Palermo G (2007) The ontology of economic power in capitalism: mainstream economics and Marx. *Cambridge Journal of Economics* 31(4): 539–561. DOI: 10.1093/cje/bel036.

Palermo G (2014) The economic debate on power: a Marxist critique. *Journal of Economic Methodology* 21(2): 175–192. DOI: 10.1080/1350178X.2014.907440.

Parkin J (2019) The senatorial governance of Bitcoin: making (de)centralized money. *Economy and Society* 48(4): 463–487. DOI: 10.1080/03085147.2019.1678262.

Peck ME (2017) Why the Biggest Bitcoin Mines Are in China. Available at: https://spectrum.ieee.org/computing/networks/why-the-biggest-bitcoin-mines-are-in-china (accessed 11 June 2018).

Philippas D, Rjiba H, Guesmi K, et al. (2019) Media attention and Bitcoin prices. *Finance Research Letters* 30: 37–43. DOI: 10.1016/j.frl.2019.03.031.

Qin R, Yuan Y and Wang F-Y (2018) Research on the Selection Strategies of Blockchain Mining Pools. *IEEE Transactions on Computational Social Systems* 5(3): 748–757. DOI: 10.1109/TCSS.2018.2861423.

Reid F and Harrigan M (2013) An Analysis of Anonymity in the Bitcoin System. In: Altshuler Y, Elovici Y, Cremers AB, et al. (eds) *Security and Privacy in Social Networks*. New York, NY: Springer New York, pp. 197–223. DOI: 10.1007/978-1-4614-4139-7_10.

Rowlands B and Kautz K (2021) Power relations inscribed in the enactment of systems development methods. *Information Systems Journal*: isj.12322. DOI: 10.1111/isj.12322.

Sayer A (2012) Power, causality and normativity: a critical realist critique of Foucault. *Journal of Political Power* 5(2): 179–194. DOI: 10.1080/2158379X.2012.698898.

Stoll C, Klaaßen L and Gallersdörfer U (2019) The Carbon Footprint of Bitcoin. *Joule* 3(7): 1647–1661. DOI: 10.1016/j.joule.2019.05.012.

Swartz L (2018) What was Bitcoin, what will it be? The techno-economic imaginaries of a new money technology. *Cultural Studies* 32(4): 623–650. DOI: 10.1080/09502386.2017.1416420.

Taylor MB (2017) The Evolution of Bitcoin Hardware. *Computer* 50(9): 58–66. DOI: 10.1109/MC.2017.3571056.

Teng Y (2021) Towards trustworthy blockchains: normative reflections on blockchain-enabled virtual institutions. *Ethics and Information Technology*. DOI: 10.1007/s10676-021-09581-3.

Tool MR and Samuels WJ (1989) *The Economy As a System of Power*. Transaction Publishers.

Tuwiner J (2019) Bitcoin Mining Pools. Available at: https://www.buybitcoinworldwide.com/mining/pools/ (accessed 16 May 2019).

Vatiero M (2010) The Ordoliberal Notion of Market Power: An Institutionalist Reassessment. *European Competition Journal* 6(3): 689–707. DOI: 10.5235/ecj.v6n3.689.

Vidan G and Lehdonvirta V (2018) Mine the gap: Bitcoin and the maintenance of trustlessness. *New Media & Society*: 146144481878622. DOI: 10.1177/1461444818786220.

Volkoff O and Strong DM (2013) Critical Realism and Affordances: Theorizing IT-Associated Organizational Change Processes. *MIS Quarterly* 37(3): 819–834. DOI: 10.25300/MISQ/2013/37.3.07.

Wedel JR (2017) From Power Elites to Influence Elites: Resetting Elite Studies for the 21st Century. *Theory, Culture & Society* 34(5–6). SAGE Publications Ltd: 153–178. DOI: 10.1177/0263276417715311.

West SM (2021) Survival of the cryptic: Tracing technological imaginaries across ideologies, infrastructures, and community practices. *New Media & Society*: 146144482098301. DOI: 10.1177/1461444820983017.

Westphal A (2015) Blockchain. Available at: http://www.icmagroup.org/Regulatory-Policy-and-Market-Practice/market-infrastructure/fintech/distributed-ledger-technology-dlt/ (accessed 2 February 2017).

Willcocks L (2004) Foucault, Power/Knowledge and Information Systems: Reconstructing the Present. In: Mingers J and Wilcocks L (eds) *Social Theory and Philosophy for Information Systems*. John Wiley & Sons Ltd, pp. 238–298.

Wrenn M (2017) Heterodox economics and theories of interactive agency. In: Jo T-H, Chester L, and D'Ippoliti C (eds) *The Routledge Handbook of Heterodox Economics*. Routledge. Available at: https://www.routledge.com/The-Routledge-Handbook-of-Heterodox-Economics-Theorizing-Analyzing-and/Jo-Chester-DIppoliti/p/book/9781138899940 (accessed 9 May 2019).

Zamani ED and Giaglis GM (2018) With a little help from the miners: distributed ledger technology and market disintermediation. *Industrial Management & Data Systems* 118(3): 637–652. DOI: 10.1108/IMDS-05-2017-0231.

Zamani ED, He Y and Phillips M (2020) On the Security Risks of the Blockchain. *Journal of Computer Information Systems*: 1–12. DOI: 10.1080/08874417.2018.1538709.

Zook MA and Blankenship J (2018) New spaces of disruption? The failures of Bitcoin and the rhetorical power of algorithmic governance. *Geoforum* 96: 248–255. DOI: 10.1016/j.geoforum.2018.08.023.