POWER AND BITCOINS: A CRITICAL REALISM PERSPECTIVE

Research full-length paper
Track N°00

Zamani, Efpraxia D., Information School, University of Sheffield, UK, e.zamani@sheffield.ac.uk

Abstract

In this study, through the lens of critical realism to power, we take a close look into the power dynamics behind the Bitcoin protocol in relation to its Cypherpunk philosophical underpinnings. We focus on some of its main components that can be seen as constraining structures, and we discuss how these structures generate constraining mechanisms that restrict users' power to act, further reinforcing other entities'' power over them. In doing so, we illustrate that the Bitcoin Protocol, as it is used today, is in tension with the principles on which it was developed. In addition, we show that power, instead of being decentralised and distributed to the many, it has merely shifted from traditional actors to what can be seen as newcomers or atypical regulators. In line with the paradigm of critical realism, we note that the identified mechanisms and structures we discuss in this paper, are those that we were able to observe through our subjective lens; others may exist but may require different contextual conditions to be activated and observed.

Keywords: Bitcoin, Power, decentralisation, critical realism

1 Introduction

The Bitcoin and the Blockchain technology have been attracting the interest of many researchers and practitioners alike on a global scale, primarily because they promise to solve many issues surrounding transparency, trust, decentralisation and traceability. About then years after Nakamoto's original paper (Nakamoto, 2008a) on the Bitcoin protocol, the literature exhibits a strong focus on proposing innovative use cases (e.g., Creer et al., 2016; Kypriotaki et al., 2015), investigating the desirability and feasibility of regulation around it (e.g., Schaupp and Festa, 2018; Vidan and Lehdonvirta, 2018), as well as technical matters concerning security, privacy and risk (e.g., Puthal et al., 2018; Zamani et al., 2018).

However, a less investigated aspect of the Bitcoin and the Blockchain is that which pertains to their underlying philosophy and their links to the Cypherpunk Manifesto (Swartz, 2018; Vidan and Lehdonvirta, 2018). The Manifesto recognised as law only what can be illustrated through maths and enforced by code, and focuses on the anonymity of the involved parties (Narayanan, 2013). Indeed, when the Bitcoin protocol was first introduced, what seemed to spark the interest of users was the potential to move from trusting a single regulatory body or state, to trusting anonymous, unknown and therefore untrusted peers by leveraging the power of maths and cryptography (Vidan and Lehdonvirta, 2018). At the same time, what seemed equally promising was the potential to shift the power balance from sovereign states and financial institutions to users and citizens thanks to the technology's decentralised nature (Corradi and Höfner, 2018).

In effect, this was an effort to move from the centralisation of power for authorising and validating payments to the decentralisation of the process, where some thousands of peers could all have an equal saying in doing so. In other words, what the Bitcoin protocol suggested was that power could effectively be distributed across the many rather than being concentrated in the hands of the few. Along these lines, fairly recently, a small number of studies begun looking into these attributes of these two technologies, and in relation to the promised potential to shift the power balance (Swartz, 2018; Vidan and Lehdonvirta, 2018).

In this paper, we focus our attention on the philosophical underpinnings of the technology, and analyse some of its major features in relation to them. Our aim is to showcase that, first, the technology as used today is in contrast to these underpinnings, and that second, the trajectory of the Bitcoin and that of the Blockchain suggest that power has not been distributed but instead shifted from traditional actors (such as states) to newcomers and less typical regulatory bodies.

The paper is structured as follows. We start off by presenting a short overview of the philosophical underpinnings of the Bitcoin and the Blockchain. We then introduce our theoretical approach to the concept of power. This is followed by a discussion around the tension between the technology's philosophical underpinnings and how it is used today, unpacking the constraining structures and the constraining mechanisms, so as to showcase how the Bitcoin protocol is a system of power.

2 On the Philosophical Origins of the Bitcoin

Researchers (e.g., Swartz, 2018; Zamani and Babatsikos, 2017) suggest that the idea behind the Bitcoin protocol can be found in Chaum's 1983 proposal for a fully anonymous payment system, that leveraged cryptographic protocols to secure the anonymity and the privacy of stakeholders in electronic transactions (Chaum, 1983). The need for privacy is a focal point in Hughes' Cypherpunk's Manifesto, as well, which can only be achieved through anonymity (Hughes, 1993):

> *"Privacy is necessary for an open society in the electronic age. […] privacy in an open society requires anonymous transaction systems. […] An anonymous system empowers individuals to reveal their identity when desired and only when desired; this is the essence of privacy."*

Against this background, many of the features and functions in the Bitcoin protocol are firmly aligned with each of the themes raised within the Cypherpunk's Manifesto. For example, the Manifesto underlines that "each party to a transaction [should] have knowledge only of that which is directly necessary for that transaction" (Hughes, 1993). This, in principle, is satisfied by the use of public key cryptography, where each user possesses their own pair of keys for initiating and settling transactions, thus confirming the authenticity of the transaction. Further, Hughes stresses the importance of an open and transparent system that is distributed and maintained by the many: "[w]e publish our code so that our fellow Cypherpunks may practice and play with it. Our code is free for all to use, worldwide. […] We know that software can't be destroyed and that a widely dispersed system can't be shut down." (Hughes, 1993). Indeed, the Bitcoin protocol in essence builds on the concept of a peer-to-peer network, where all users are connected to each other over the internet for the purpose of minting new coins, transacting with one another and validating transactions. The protocol itself, i.e., the code, is publicly available and open to all, for investigation, auditing etc., in the principles of open source code, where anybody can access it, identify flaws, or further build their own applications on top of it.

The most critical theme however that emerges out of the Cypherpunk's Manifesto is that of the distrust regarding the role of governments and corporations: "[w]e cannot 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). In other words, this underlines that the intentions and actions of such institutions are not and should not be considered as benevolent, but rather that citizens should actively seek out their autonomy, self-reliance and self-control in order to resist institutionalized authority (Coleman and Golub, 2008). Along these lines, and with regards to the Bitcoin, its objective was to create a network and an infrastructure that can be trusted, without necessarily trusting the peers themselves, but rather the technology and the cryptographical means used (Vidan and Lehdonvirta, 2018), thus removing the need for card issuers, central banks, states and escrow services (Westphal, 2015), which are often addressed as corrupt by many of the core developers of the Bitcoin (De Filippi and Loveluck, 2016).

Because the Bitcoin protocol places a great emphasis on privacy and anonymity, and reducing the power of institutionalized authorities, it is often considered as the technological manifestation of the 'libertarian dream' (De Filippi, 2014). However, the protocol in itself is politically agnostic, in the sense that it can be easily seen through the lens of the libertarian Right wing, that exhibits general mistrust and is negatively inclined toward state control, as well as through the lens of the pacifist Left wing, challenging the oligopoly and disrupting the status quo (Coleman and Golub, 2008; De Filippi and Loveluck, 2016). True to this agnosticism, Cypherpunks may be radical libertarians, anarcho-capitalists, or socialists, which is also reflected in a recent survey on the political leanings of Bitcoin adopters, where the majority identify themselves as Liberals (CoinDesk, 2018).

3 Theoretical Background

3.1 Power and Technology: the Foucauldian Approach

Traditionally, within the Information Systems domain, the Foucauldian approach to power has been quite influential. For example, its influence can be seen clearly in Zuboff's work (Zuboff, 1988), where information systems are discussed as machines with the power to automate and informate, and which can be used for discipline, monitoring and surveillance (Doolin, 2004). According to Foucault, power is relational, and it exists only when exercised (Foucault, 1979). In other words, it entails the capacity to act, it suggests resistance (Willcocks, 2004) and exists in and stems from within social relationships (Doolin, 2004). As such, it lives within the knowledge, practices and technologies that impact on others and their capacity to act (Hindess, 1996). However, due to social relationships and practices, power becomes internalised, and its impact can be observed not only when directly exercised, but also when experienced through its apparatuses (Doolin, 2004).

Foucault's work has received several criticisms, with some of them having been addressed by Foucault himself in his later writings. In what follows we discuss those that pertain to this study and our own conceptualisation of power, later presented.

As discussed by Willcocks, the Foucauldian approach to power presents certain difficulties in applying it (Willcocks, 2004). He notes that if indeed power is ever present, then "all social and cultural phenomena become reducible to power relations" (Willcocks, 2004, p. 262), where agency is either understated or dismissed (Best, 1994). Willcocks also draws from Reed (1998) to note that the poor attention to agency further underestimates the relationship between agency and structure. As a result, it is impossible to investigate into and assess the differences between social actions and structural constraints, and therefore such an approach does not allow researchers understand how material and social constructions are either supported or constrained by agents, and in the case of information systems, technology. Further, in Foucauldian terms, power is treated in a somewhat flat manner, without attention to the hierarchical nature of institutions, the state etc., while explicitly rejecting the notion of underlying structures, and generative mechanisms that impact on the exercise of power and the potential outcomes (Sayer, 2012).

This later point with regards to agents' and technologies' constraining or supportive role is of increased importance for the field of ICTs. Technologies should be seen as interacting with the individual, as part of a process, whereby both the technology and the individual get redefined as a result of their interaction and exposure to each other. In this context, the technology itself merely mediates the will and actions of the individual (Latour, 1994) and social relations (Leclercq-Vandelannoitte, 2011), based on how this technology has been designed by others, supporting certain actions and restricting others. As such, technologies can be seen, not simply as means to control and monitor but rather as objects that, on the one hand, adhere to certain societal and organisational norms while on the other hand, empower, being the tools and providing the space and opportunities to act (Bloomfield and Coombs, 1992).

3.2 A Critical Realism Perspective of Power

Our own conceptualisation of power is understood through the lens of critical realism (Palermo, 2007; Sayer, 2012), which addresses the criticisms on the Foucauldian approach, especially with regards to the constraining structures and mechanisms, and causality. Power can be considered as the ability to do or not do something (power to act). Within the context of interpersonal relationships, power translates into the ability to influence others' actions as well (power over somebody). Power, more explicitly, can be described as the decision-making set that allows an agent to adopt a potential set of actions (Palermo, 2007). Such an agent can be an individual, a financial institution, a state, or any other type of entity. Therefore, power over somebody entails that an agent can have and exercise power over somebody only when there is a dependency relationship, i.e., when the an individual is dependent on whatever actions another individual chooses to adopt from their decision-making set. Practically speaking, this may entail influence on another individual's goals and actions, or influence and impact on their own decision-making set (Palermo, 2007, 2014). As a result, power to act and power over somebody are inescapably interwoven, because power over somebody essentially depends on the distribution of power to act within a given system, such as society (Sayer, 2012).

To date, there are different approaches to power, ranging from its non-existence within a capitalistic system, to existing solely within a bounded system (e.g., a firm), and even being ubiquitous. Such approaches depend largely on one's understanding with regards to the existence or absence of interpersonal relationships, which in capitalism and perfectly competitive markets are seen as non-existent, and therefore power to act is unrestricted (Palermo, 2014). This stems from the idea that one cannot exercise their authority over others in order to dictate a certain action, as individuals may opt to disengage from the relationship and therefore resist the exercised authority (Vatiero, 2010). However, the modern society is characterised by asymmetries (Gershenson, 2015) and power is typically unevenly distributed (Palermo, 2007). As a result, these asymmetries give way to power over others within interpersonal relationships. The important point then becomes what is the extent and the intensity of power, i.e., how many individuals' decision making and actions can potentially be restricted as a result of a single agent (extent) and would be the potential impacts and consequences should this agent decides to exercise their power over others (intensity).

The above description of power and power relations is in line with the critical realism approach (Mingers and Standing, 2017; Sayer, 2012). Critical realism has been recently attracting the interest within the IS literature, particularly thanks to its potential to provide mechanism-based causal explanations for phenomena. Critical realism puts forth the idea that the world exits independently from our own knowledge of it and that we are able to observe only a fraction of it. This suggests in turn that structures and entities exist independently and can be understood solely through our own subjective lens that has been ingrained with our sociocultural perceptions (Mingers, 2004). In other words, critical realism differentiates between the real, the actual and the empirical domains of a phenomenon (see Figure 1 for the stratification of the domains). The real denotes the causal generative mechanisms that make things happen, and can be ideas and structures, among other things, which may or may not be observable by us (Mingers and Standing, 2017). Whether these generative mechanisms get activated depends on the contextual factors of the phenomenon, and therefore they may or may not lead to changes. Drawing from prior knowledge, experience and other observations, the researcher is then able to appreciate the causal explanations behind the investigated phenomenon (Volkoff and Strong, 2013). The actual domain denotes the temporary generated events that result from the generative mechanisms and finally the empirical domain is the subset of the events that we as researchers are able to observe (Mingers and Standing, 2017). In brief, the actual domain contains the events that can potentially occur but the empirical domain contains those that both occur and are observed (Mingers et al., 2013), and therefore one can argue that critical realism combines positivism and interpretivism.

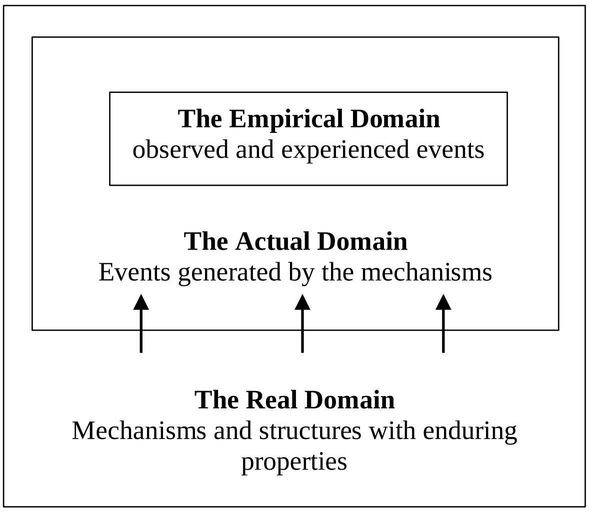

Figure 1. Domains of the real, the actual and the empirical, adapted from Mingers (2004).

One of the most critical elements of critical realism is that of generative mechanisms, which is missing from the Foucauldian approach. Therefore, the ontology of critical realism can help overcome these shortcomings (Sayer, 2012). These mechanisms can be investigated through retroductive reasoning, whereby the researcher looks into an observed event and attempts to theorise around them and their causal explanation (Mingers, 2004). It is quite possible that there is a number of generative mechanisms that can potentially explain an outcome, but the researcher needs to focus only on those that are directly relevant to the investigated phenomenon (Henfridsson and Bygstad, 2013) and the underlying contextual conditions (Henfridsson and Bygstad, 2013).

Along these lines, within the context of an investigation into power, an important aspect is whether power is activated, which depends on the existence of absence of dependencies and relations among actors. In turn, when power is activated, one needs to assess to what extent the subject is susceptible to the exercised power (Sayer, 2012). As a result, it is necessary to acknowledge that there is no deterministic effect between the exercise of power and whatever outcomes may or may not occur. Instead, what exactly is the outcome depends on the contextual conditions (Henfridsson and Bygstad, 2013).

More specifically, the power to act (individual decision-making sets) and their interdependencies create a larger decision-making system, where the relationship between agents can be shaped in many different ways. One agent may proceed with a set of actions that simply are unavailable to other agents. In addition, one agent may have imposed constraints on them on what action they can actually pursue, while the same constraints may not exist for other agents, as a result of others' power over them. In other words, within a single decision-making system, there may be numerous constraints, asymmetrically distributed across agents.

In this paper, our aim is to illustrate the structures and mechanisms that govern the power distribution in the Bitcoin protocol. We posit that such an asymmetric distribution of constraints do exist within the Bitcoin protocol as a result of the technology as designed and used. In what follows we discuss such non-observable entities that exist in the domain of the real, and specifically constraining structures, constraining mechanisms and the system of power in relation to the Bitcoin protocol. In doing so, we showcase that the technology as used is misaligned with its philosophical underpinnings.

4 Bitcoin as a System of Power

It is beyond the scope of this study to provide a detailed description of the Bitcoin protocol in its entirety. However, we will discuss in this section those features and functions of the protocol, which, through the lens of critical realism, act as the mechanisms and structures in the real domain that transform the Bitcoin protocol into an observed system of power.

4.1 Constraining Structures

While the Foucauldian approach to power rejects the concept of causality with regards to power, Sayer stresses "the importance of structures in the generation of power" (Sayer, 2012, p. 180) in order to understand power itself. This importance stems from the fact that the power of an entity exists "in virtue of the structure of [that entity]" (Sayer, 2012, p. 181) and is dependent upon exogenous structures, especially enduring ones that interact with endogenous structures.

In the case of the Bitcoin protocol, there are two major components that relate to the purposes of our study; *proof of work and block selection*[1]. The Proof of Work (PoW) is the consensus algorithm for the confirmation of transactions and for the minting process of new bitcoins (Reid and Harrigan, 2013). The process requires that each peer of the network vote with their computing power, by solving proof of work instances and thus creating the appropriate blocks in the chain. The Bitcoin protocol uses more specifically the Hashcash system. Based on this system, the miners need to complete a proof of work that covers all the transactions in the block (Bitcoin Wiki, 2019). The protocol further introduces the concept of difficulty, which dictates the amount of work required for the identification of a new block. Therefore, this process becomes computationally expensive, in terms of skills, time and the financial resources required to set up and run the necessary infrastructure (Gervais et al., 2016), which often includes advanced GP-GPU and ASICs, specifically developed for bitcoin mining. In the early years, mining could take place through the graphics card mounted on the computer (GPU), which could take up the computations necessary for solving the puzzles and the transaction blocks. However, following the huge hype that began surrounding the Bitcoin, as many users jumped on the mining bandwagon, the prices of graphic cards exploded, making the acquiring of a good graphic card quite expensive. In addition, as the mining process increases in difficulty every so many years, in order to maintain the steady supply of bitcoins, the typical graphics cards can no longer support any mining – at least not in any way that makes financial sense for the individual. As a result, another approach has surfaced, that of using ASIC (Application Specific Integrated Circuits) mining. ASICs are designed solely for the purpose of mining bitcoins at full speed, while consuming as little power as possible. Of course, they are expensive and still require a lot of time to mine coins.

As a result, based on the overall constraints imposed by the PoW, there is a high threat with regards to the centralisation of mining power to few miners only and mining pools (Bitcoin Wiki, 2019), that have access to additional resources than the average user, which in turn transforms this into an oligopoly (Arnosti and Weinberg, 2018). This undermines the central tenet of the cypherpunk movement and that

[1] Other important components, such as the Blockchain, private key cryptography and wallets, are not referred here as they are less relevant to the constraining structures of the protocol.

of the Bitcoin protocol, where the aim is meant to decentralise power and redistribute it from the few to the many, since it is not the many that have access to such skills and resources.

Next, Block selection refers to the process through which miners compete against each other in order to receive the reward for mining the next block, and therefore add a new block in the blockchain. Essentially, miners attempt to identify and broadcast their proof of work for a given block before all other miners in the network, as only the first one who does so is able to receive the block reward. The requirement for the identification of the block is again computational power, as the miner is required to solve a cryptographic puzzle before all others (Eyal and Sirer, 2018), but further includes a random component (the solution is based on a nonce). For this reason, the process has often been described as random. However, while computational power and speed may not be the sole factors, the actual probability for a miner to get selected is still proportional to their share of the employed computational resources in the network ("The 3 or 4 fastest nodes' dominance would only be proportional to their share of the total CPU proof-of-worker. Anyone's chance of finding a solution at any time is proportional to their CPU proof-of-worker." (Nakamoto, 2008b)), which allows for a trial and error approach in solving the code (Maurer et al., 2013). Because there are great incentives, the competition among miners to be the first to broadcast their proof of work is great. Therefore, to win this competition, a miner needs to dedicate increased computational power. In other words, the computational power, or lack thereof, further challenges the underpinnings of the Bitcoin protocol, by constraining and significantly decreasing the chances of a miner with less computational power being rewarded.

Another point that relates to the constraining structures of the Bitcoin protocol has to do directly with the operation expenses. The process of mining consumes significant electrical power, both for the operation itself of the equipment, as well as for its cooling (Taylor, 2017). Understandably and depending on the exact geographical location of the miner, this translates into actual financial costs. For regions such as Europe for example, it is very much expensive to mine, while for other regions, such as China and Iceland, the costs are significantly lower, as a result of a combination of reasons, ranging from the actual climate conditions to the regulatory environment. Obviously, the incentive here would be that the received reward outweighs the costs spend for the mining. In other words, the reward must worth more than the electrical power spent to make financial sense for the user.

It therefore follows that the code itself, while initially considered as a way to distribute power, due to the computational requirements that ever increase by design, results today in power becoming concentrated to the few (Vidan and Lehdonvirta, 2018). Through the lens of critical realism to power, one can argue that the structures discussed above belong in the domain of the real as they have enduring properties and impacts. Further, we note that the decision-making set of miners, especially those that individually mine bitcoins, is significantly restricted. It is not simply that the minimum requirements for mining are today excessively high. The competition itself emerging as a result of the technology as designed suggests that certain miners with increased computational power are better positioned to take advantage of the technology by mining bitcoins and thus receive rewards (power to act), while others with less computational power are unable to do so and can solely participate in the verification process, which is not resource intensive.

4.2 Constraining Mechanisms

The Bitcoin protocol today is about 10 years old and throughout this time updates and revisions to the code have been the subject of intense discussions among Bitcoin developers and enthusiasts. Generally, such changes in the code need to be agreed upon by a majority of miners who vote for the incorporation of said changes. For the purposes of the discussion around Bitcoin and power however, we can consider that the constraining structures previously discussed have remained stable over time, with minor changes. In such cases, where the constraining structures remain fairly stable over time, what need to be addressed are the constraining mechanisms that regulate and further propagate them (Palermo, 2007; Wrenn, 2017).

Mechanisms, constraining mechanisms in this study, are meant to impact on one's actions and have a causal force (Nicholson et al., 2013) that explains the observed events in the empirical domain. In this sense, we posit that the asymmetric power distribution discussed earlier, stemming from the constraining structures, is the result of the constraining mechanisms residing externally from the protocol. Such mechanisms include, among others, external actors with an interest in the Bitcoin protocol, including the state, financial institutions, central banks, large Bitcoin exchanges, technologists and large mining pools, who manage to control in effect the production and the valuation of the Bitcoin and enhance or impair the technology's status. These mechanisms get activated depending on their relationships with other entities, such as the end users, the Bitcoin structural elements and so on and so forth. The effect of these mechanisms is subject to the strength, vulnerabilities and relative positioning of the entities with which they relate, which can reinforce or block the power exercised (Sayer, 2012). These mechanisms are discussed in the following sections in relation to the philosophical underpinnings of the protocol.

4.2.1 The mechanism of identification and verification: back to deanonymisation

The preservation of anonymity has been since the beginning the central idea behind the peer-to-peer electronic cash system proposed by Nakamoto. In addition, the inability to preserve anonymity within a perceived as corrupt state-driven payment system is what dictated for Cypherpunks the necessity to incorporate strong cryptographic techniques in their code and place their trust only in their code: "Cypherpunks deplore regulations on cryptography, for encryption is fundamentally a private act. The act of encryption, in fact, removes information from the public realm. Even laws against cryptography reach only so far as a nation's border and the arm of its violence" (Hughes, 1993).

In the original paper published by Nakamoto, there is no indication that online or brick and mortar cryptocurrency exchanges would be necessary or even desired. Rather, when the electronic cash system was launched, the idea was that Bitcoin users would be minting new coins themselves, which they would store locally on their personal devices. Through their devices, users would be able to transact directly with each other and without going through a financial institution of some kind (Nakamoto, 2008a). However, for a number of reasons, including convenience, self-efficacy, and usability, such cryptocurrency exchanges emerged as early as 2010 (Sedgwick, 2018).

With the advent of such cryptocurrency exchanges, Bitcoin users begun acquiring bitcoins from them, trading fiat money for cryptocurrencies and using the exchanges' wallets and transacting with others through them. Because of underlying risk concerns in transacting with unknown others and thanks to the convenience offered in locating buyers and sellers, many users, who hold their funds in hardware (offline) or hot (online) wallets, transfer their funds, even momentarily, to their online exchange accounts to complete transactions. However, to access such services, the increased majority of these exchanges require that users identify and verify themselves by providing their personal details, including name, address, nationality and a copy of a government ID (e.g., national ID, driving licence, passport), in an effort to satisfy Know Your Customer (KYC) requirements. While these are not broadcasted on the blockchain when a transaction occurs, it is possible to trace back the transaction itself and then link it to the sender and the recipient of the transaction. Vidan and Lehdonvirta (2018) refer to these exchanges as 'gatekeepers' who break the protocol's promise of anonymity. Others have shown that there is a discrepancy between potential and actual anonymity because it is possible, with enough resources, to link addresses of the same user together and in time identify large entities and their interactions (Meiklejohn et al., 2016). In addition, Jeff Garzik, a member of the Bitcoin core development team has noted that with today's statistical analysis and network analysis techniques, it is possible to identify Bitcoin users (Maurer et al., 2013).

We call this the mechanism of identification and verification. The above discussion reveals that while the technology has been developed as an attempt to preserve the anonymity of participants, externally from it, there is a still the need for the identification and verification of the transacting parties. Positioning this within the context of critical realism, the mechanism of identification and verification gets activated when there is a requirement to align with long established regulatory frameworks (KYC, in the case of cryptocurrency online exchanges), as well as to track fraudulent and illicit activities (which the state and society have an interest to deter and interrupt). As a result, what occurs is that external to the technology measures are still in place, and the verification of the trustworthiness of users and the legality of the transactions is still mandatory; the difference is that the verifying authority has shifted from the state to these exchanges. What is important for our discussion on power is that these exchanges, while part of the Bitcoin peer-to-peer network enjoy greater leverage than individual users, and can exercise their power over others by choosing to include or exclude individuals on the basis of the laters' perceived trustworthiness.

One could argue that users could choose not use these exchanges and transact directly with each other. Along these lines, it needs to be noted that there are several exchanges that do not require any authentication, and others that allow for offline transactions. In such cases however users exchange the preservation of their anonymity for higher fees and commissions, and normally less easy to use interfaces. In addition, in the case of direct transactions, the transacting parties will further need to trust each other, as the technology cannot ensure that e.g., the seller will fulfil the transaction by delivering the product or service paid for. These elements put together constrain significantly Bitcoin users' power to act.

4.2.2 The mechanism of cost effectiveness: back to centralisation

Early Bitcoin adopters had the opportunity to mine bitcoins with significantly decreased difficulty and fewer technological requirements. Therefore, they were able to acquire bitcoins through mining with considerably lower costs. Currently, because of the increased starting costs and operational costs, together with the increased competition for identifying the next block to mine and the decrease in the reward, the overall costs of mining individually outweigh potential profits (Taylor, 2017). It is therefore highly unusual to be an individual miner, and what is observed is that Bitcoin miners tend to join large mining pools. Through such mining pools, individual users join their efforts with other miners and pool their computational resources, and therefore hashing power. In turn, this brings them, as a group, in a better position to defeat their competition in mining and identifying the next block, and therefore receive the mining reward (Maurer et al., 2013). The reward itself is directed to the mining pool rather to any individual miner within that pool, but each of them receive a fraction of the reward according to their contribution and the rewarding scheme adopted by the pool (Dziembowski, 2015).

Figure 2 show the market share of the most popular Bitcoin mining pools. Based on these data, we see that today exist some very large mining pools, such as BTC.com, AntPool and SlushPool. These large pools are followed by several smaller ones, along the dimensions of hashing power and number of blocks identified. In 2016, a study has found that 75% of the hashing power resided in China and Chinese mining pools (De Filippi and Loveluck, 2016). In other words, not only the computational power today is concentrated into few mining pools but these pools, for a number of reasons, are mostly concentrated in a single country (Peck, 2017; Tuwiner, 2019). CoinMetrics have investigated the concentration of hashing power and the mining pools into greater detail, and have identified some additional interesting patterns (Figure 3): a) large mining pools may come and go, but there are some that seem quite persistent over time such as F2Pool and Slushpool, thus being more attractive to prospective miners as a result of their longevity, and b) it is difficult to assess real world power concentration just by looking into the power distribution across pools, because some, such as Antpool and BTC.com are owned by the same company, Bitmain (Coinmetrics, 2019). In other words, Bitmain owns the largest and second largest mining pools today, enjoying a significant leverage over the mining process.

The concentration of hashing power to a few large mining pools is a concern for many Bitcoin researchers with regards the security of its Blockchain. When more than 50% of the network's hashing power is concentrated by a single entity, then this entity is able to control the Blockchain through a number of ways: e.g., the entity is able to prevent the confirmations of transactions, thus leading to transactions being rejected, and they are able to reverse transactions even if these have been completed. Most importantly, in such an event, double spending of coins could be possible, which was one of the major problems that the Bitcoin has managed to solve for digital cash systems (Nakamoto, 2008a). Therefore, the concentration of power by few mining pools is not only a very obvious threat for the decentralised nature of the Bitcoin, but also creates a risk for the security of the Blockchain and the Bitcoin payment system in general (Conti et al., 2018; Eyal and Sirer, 2018).

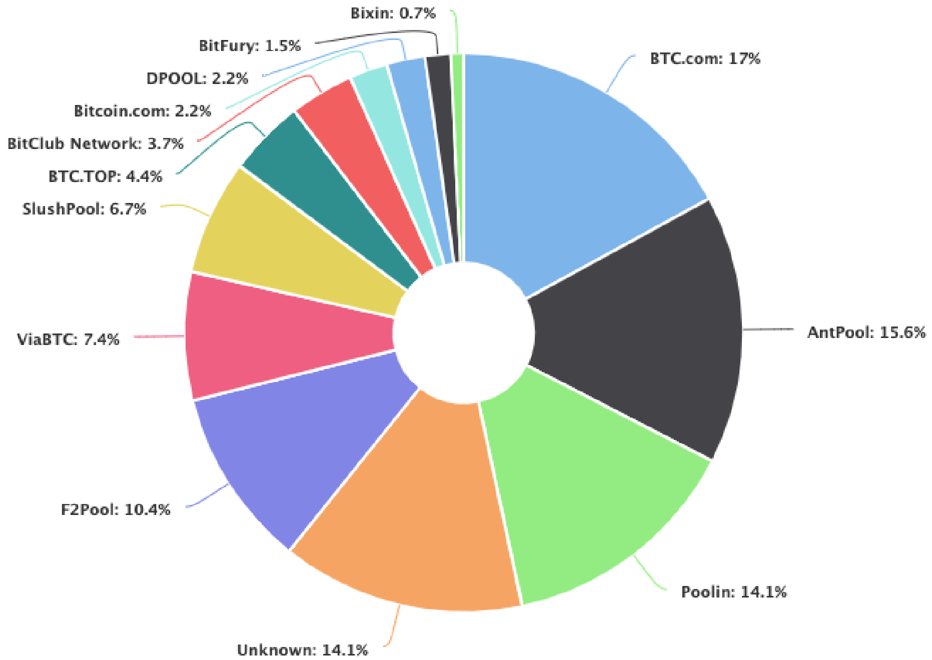

Figure 2. *Bitcoin hashrate distribution in May 10, 2019. 'Unknown' means that Blockchain.info was unable to determine the origin. Source: https://www.blockchain.com/explorer (accessed on 10/05/2019).*

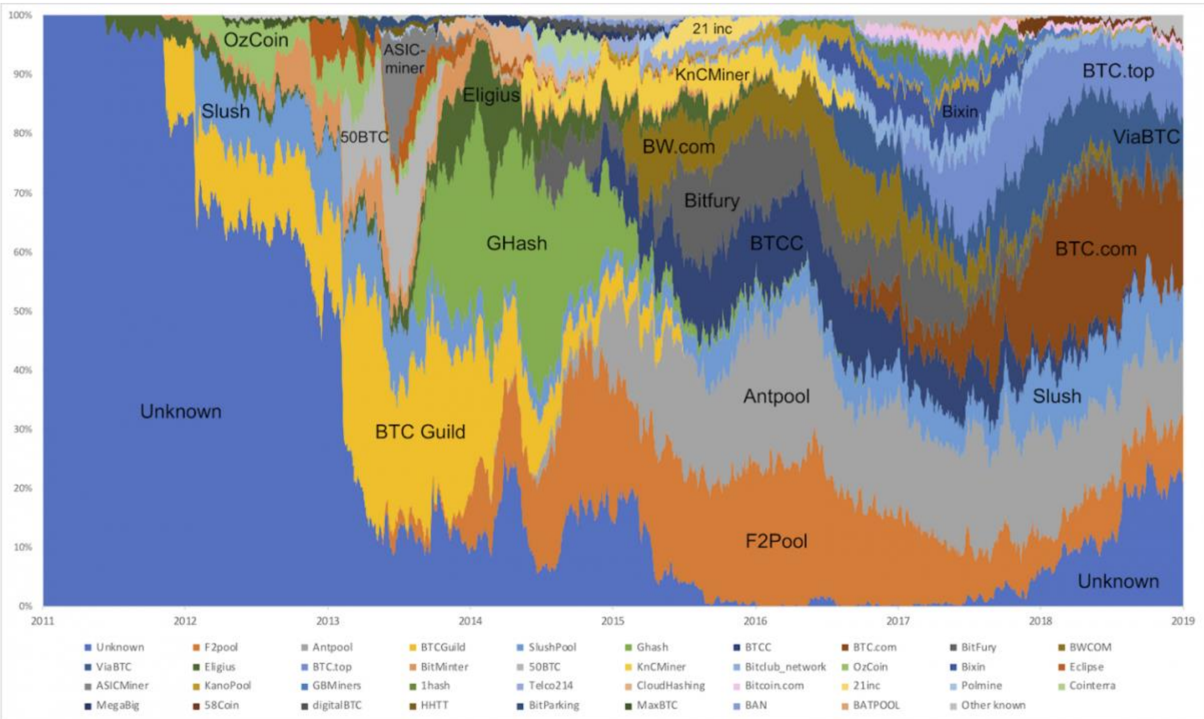

Figure 3. *Distribution of hashing power among mining pools (until January 7, 2019). Source: (Coinmetrics, 2019).*

We call this the mechanism of cost effectiveness. Based on the discussion above, we have shown that as a result of increasing costs and decreasing rewards, the miners do not have many options in order to receive financial gains and incentives towards keep on mining. Today, the only visible way for making profits and operating a financially viable mining operation is that of joining a mining pool, which progressively leads to the establishment of large groups of users, i.e., large mining pools, all working together in an effort to mine the next block. In other words, this mechanism gets activated when the ratio of financial gains to operational costs decreases overall, quite possibly converging to zero (Derks et al., 2018), and when operational costs exceed financial gains, which functions as a cut-off point after which mining is a cost for the miner. For simple users, the large mining pools exert power over them as the pool or the combination of pools are able to control confirmations, and transactions. For individual miners, the impact is similar with mining pools reducing the formers' opportunities to mine and receive rewards, as the later leverages greater hashing power.

A subsequent discussion of power through the lens of critical realism would then be on the decision making of miners for joining a mining pool, in order to appreciate the extent of their power to act to join a certain pool and the extent and the intensity of the power of the mining pools over miners. Typically, there are two main factors that play into one's decision making. The first has to do with the scheme the pool operates for paying out the reward and the fee it deducts. The second has to do with the size of the pool, i.e., how many peers comprise the pool, which is an indication of its hashing power (bitcoin wiki, 2011). Intuitively, we argue that prospective miners would be more inclined to join a pool with an established history such as Slush Pool, or a pool that has a low fee and a large pay out reward. There are different approaches to the fees. Some pools, such as Slush Pool require a 2% fee but share all transaction fees with its miners, whereas Ant Pool does not charge any fees, but does not share transaction fees. Next, the mining reward is computed based on the contribution of the miner toward the identification of a block, in other words, it is based on the hardware the miner owns and uses for mining. Therefore a single miner may wish to trade stability for increased pay outs, or vice versa. In all cases, miners willing to join a pool enjoy greater power to act and decide which pool to join, as they can even change pools.

4.2.3 What is it good for? The mechanism of perceptions

Within the context of examining the Bitcoin protocol as a system of power, we have shown so far that power to act and power over somebody exists as a result of endogenous, enduring structures and specifically as a result of some of its core components. We have further addressed how two major constraining mechanisms emerge as a result of these constraining structures, restricting miners' and users' power to act. Another constraining mechanism however stems from exogenous structures, such as the state, financial institutions, central banks, and technologists, who leverage their power over their audience and the public and inescapably influence the laters' perceptions.

When the Bitcoin protocol was first introduced, it was seen as a solution for preserving the anonymity in transactions, for the problem of power centralisation in the hands of the few, and as a way to overcome issues that stem from inflation and deflation. Yet, today, the Bitcoin is mostly discussed in relation to two main things as a result of its affordances. The first has to with fraudulent activities and illicit trading (e.g., Burge, 2015), and the second with its potential to provide huge returns for investors (but also losses) (Gerlach et al., 2018).

The Bitcoin protocol has been the subject of several discussions so far in relation to illicit trading, fraudulent activities and generally activities that appear to be against the status quo. One of the first events that have brought the Bitcoin into the general public's attention is presumably the establishment of Silk Road, an online marketplace for the trade of illicit goods, and its subsequent shutdown (Maurer et al., 2013). Silk Road users were transacting with each other using bitcoins in an effort to remain anonymous. However, since the traded goods were actually illicit (guns, drugs etc.), Silk Road naturally attracted the interest of law enforcement, who then were successful in not only shutting down the market but also tracking and identifying sellers and buyers (Meiklejohn et al., 2016). In addition, bitcoins have been widely used for donating to causes that may seem as threatening the establishment, such as WikiLeaks' operations, Julian Assange's, Edward Snowden's and Ross Ulbricht's defence funds, with the cryptocurrency being seen as "a censorship-resistant digital currency" (Maurer et al., 2013, p. 266). While such events supported the popularity of the Bitcoin to grow, they have also facilitated governmental agencies, regulators and financial actors to link, in the public's mind, the technology to fraudulent activities.

Next, the Bitcoin is often discussed in the media in relation to its price, the price's volatility, its use as an investment as well as its potential to disrupt different industries. Thus far, it seems there is an increased majority that agrees in that the Bitcoin does not perform well as a medium of exchange due to its price volatility (Maurer et al., 2013). Others approach it as an instrument to speculate on its price and therefore gain and maximise their profits in the process (De Filippi and Loveluck, 2016). However, investing in Bitcoin can be a very risky endeavour and not always profitable. For many, the Bitcoin has no intrinsic value and therefore, its price may be justified or explained by speculative behaviour that often leads to price bubbles (Cheah and Fry, 2015; Shahzad et al., 2019). In addition, financial institutions seem less ready to invest in Bitcoin (although the same cannot be said for the Blockchain (Du et al., 2019)) due to concerns regarding the regulatory environment, taxing and accounting (Shahzad et al., 2019), which therefore indicates that more established players put less trust in the technology. Finally, a number of studies have linked Bitcoin's price to speculation by investors, who seek to make great profits in less time with lower investment costs (Baur et al., 2018; de la Horra et al., 2019). However, this may lead to adverse effects with investors being exposed to the usual market risks (Koutmos, 2019), especially if one ascribes to the notion that the Bitcoin has no intrinsic value.

While the above discussion can be telling with regards the influence of such players on any market, for us it is useful for considering their impact, not on the price of the Bitcoin, but instead on the public's opinion regarding the technology. Because of the complexity of the technology, and because it still hasn't been widely adopted, novice users are less ready to place their trust in the Bitcoin (Alshamsi and Andras, 2019), and more likely to be influenced by media hype, which admittedly focuses on the more dystopian side of the Bitcoin (Cameron and Trinh, 2017). We call this the mechanism of influencing perceptions, that drives the increased majority of novice users to think of the Bitcoin as something without value, that cannot be used as an electronic payment system, and something to steer away from since the vernacular typically links it to less positive stories. In line with the critical realism's view of power, it is reasonable to suggest that the influence of exogenous structures, such as financial institutions, central banks, media and technologists, exerts a disproportionate power over potential users and the wider public. In the short term, this restricts the public from using the Bitcoin as a payment system, because it is still not widely accepted by merchants, banks and the state as 'money', or medium of exchange, especially because of their perceptions regarding its risky nature. In the long term,

4.3 System of Power: the interaction of structures and mechanisms

The constraining structures and the constraining mechanisms provide the underlying principles for systems of power (Palermo, 2007). In the case of the Bitcoin, the constraining structures of Proof of Work and Block Selection, and the constraining mechanisms of identification and verification, cost effectiveness, and perceptions make the Protocol a system of power. Against this background, power to act and power over somebody continuously interact and reinforce each other.

With regards to the mechanism of cost effectiveness, we see that under the pressure of receiving the mining reward, miners compete against each other in order to be the first to solve the cryptographic puzzle (constraining structure of Proof of Work) as well as for identifying the next block (Block Selection). In this race, due to the increasing costs and the increasing difficulty, the mechanism of cost effectiveness gets activated, where miners work collaboratively, in effect against other mining pools, in order to create economies of scale and take advantage of the consolidated computing power.

Next, as far as the mechanism of identification and verification is concerned, we note that the Proof of Work, as a function in itself, does not require any more information than what is included in a transaction. Transactions themselves are executed and verified using public key cryptography, where ownership of any fraction of bitcoin is proved by signing the broadcasted transaction with the paired private key (Biryukov and Pustogarov, 2015). In addition, cryptocurrency exchanges do not provide their services for free, but instead apply a fee to a every transaction that goes through them. These two points combined activate the mechanism of identification and verification because of two reasons. First, despite that the Bitcoin is pseudonymous rather than purely anonymous, it is still difficult to link one's real world identity to the Bitcoin wallet. Second, cryptocurrency exchanges and Bitcoin users can have significant profits as a result of their trading activities, but due to pseudonymity, taxation becomes increasingly difficult. However, the state, central banks and other financial institutions have a stake on taxation and general regulation: for the state and central banks, taxation of bitcoins is a source of income; for financial institutions, cryptocurrency exchanges may well seem as brokers, offering an alternative trading system to their own with fewer restrictions for participants (Shapiro, 2018) and therefore seem more attractive for trading and investments. In both cases, the constraining structure activates the mechanism of identification and verification.

In relation to this, the mechanism of perceptions further reinforces the mechanism of identification and verification. The hype that surrounds the Bitcoin, the volatility of its price that can lead equally to great profits and great losses, as well as the lack of regulation and its affordance to be used in illicit activities, further feed into the mechanism of identification and verification, by means of questioning its legitimacy (DeVries, 2016). This requires that Bitcoin users trading through exchanges identify themselves so that their activities can be traced and verified. In many cases, this is also desired by the users themselves, as it is still difficult for several of them to trust unknown transacting parties that operate at the margins of regulation (Zamani and Babatsikos, 2017). However, what we note here is that the mechanisms themselves get activated as a result of the constraining structures, but further interact with each other, reinforcing each other.

5 Conclusions

In this study, we have focused our attention on the underlying constraining structures and constraining mechanisms that transform the Bitcoin protocol into a system of power. As raised by other researchers, technologies are rarely used and employed as originally designed or even imagined (Orlikowski and Baroudi, 1991), and our study offers further confirmation. However, we also show that the main components of a technology, in this case of the Bitcoin protocol, can act as constraints with regards to restricting users' power to act in a manner that is in line with the Bitcoin's philosophical underpinnings.

We have further shown that some constraining mechanisms, that exist independently from these structures and the protocol, possess and exercise their power over users and miners, reinforcing each other and further restricting users' and miners' power to act. In doing so, we have shown that while the Bitcoin protocol was developed and launched with the aim to decentralise power and distribute it to individual users and citizens, due to such mechanisms, power has instead shifted from more traditional actors, such as the state, to newcomers, such as cryptocurrency exchanges. Focusing specifically on the mechanism of identification and verification, we see that such actors have taken up the role of controllers or 'gatekeepers' (Vidan and Lehdonvirta, 2018), previously exercised by the state and central banks. However, their role as a controller and this mechanism are further reinforced by other mechanisms, such as the one of perceptions, where exchanges, while exercising their power over users, are required to do so but the enduring power of the state.

We have built our study drawing from critical realism. It is therefore necessary to note that, while the identified mechanisms and structures exist independently within the domain of the real, we can only observe a fraction of this domain. In other words, we expect that there will be additional structures and mechanisms that our study has not revealed nor addressed, due to our own subjective lens (Mingers, 2004) and because different contextual conditions may be required to activate them and bring them into the fore. Further, we have based our study solely on phenomena that presently both occur and are observable (actual domain). However, Mingers and Standing (2017) note that other phenomena, temporary in nature, may be generated by the identified generative mechanisms (actual domain) without being observable. In continuing with a similar analysis in the future, it would useful to cast a wider net across the cryptocurrency landscape, the legal and regulatory environment as well the market, in order to identify a larger set of tendencies, consequences and associations among the components of the Bitcoin system and between them and the different financial and social relationships of the involved actors.

References

Alshamsi, A. and Andras, Prof.P. (2019), “User perception of Bitcoin usability and security across novice users”, *International Journal of Human-Computer Studies*, Vol. 126, pp. 94–110.

Arnosti, N. and Weinberg, M.S. (2018), “Bitcoin: A natural oligopoly”, *10th Innovations in Theoretical Computer Science Conference (ITCS 2019)*, presented at the 10th Innovations in Theoretical Computer Science Conference (ITCS 2019), Cambridge, Massachusetts, available at:https://doi.org/10.4230/LIPIcs.ITCS.2019.5.

Baur, D.G., Hong, K. and Lee, A.D. (2018), “Bitcoin: Medium of exchange or speculative assets?”, *Journal of International Financial Markets, Institutions and Money*, Vol. 54, pp. 177–189.

Best, S. (1994), “Foucault, postmodernism and social theory”, in Dickens, D.R. and Fontana, A. (Eds.), *Postmodernism and Social Inquiry*, Routledge, London, New York, pp. 25–52.

Biryukov, A. and Pustogarov, I. (2015), “Proof-of-Work as Anonymous Micropayment: Rewarding a Tor Relay”, in Böhme, R. and Okamoto, T. (Eds.), *Financial Cryptography and Data Security*, Springer Berlin Heidelberg, pp. 445–455.

bitcoin wiki. (2011), “Mining pool reward FAQ”, *Bitcoin Wiki*, available at: https://en.bitcoin.it/wiki/Mining_pool_reward_FAQ (accessed 14 August 2018).

Bitcoin Wiki. (2019), “Hashcash - Bitcoin Wiki”, 30 April, available at: https://en.bitcoin.it/wiki/Hashcash (accessed 9 May 2019).

Bloomfield, B.P. and Coombs, R. (1992), “Information Technology, Control and Power: The Centralisation and Decentralisation Debate revisited”, *Journal of Management Studies*, Vol. 29 No. 4, pp. 459–459.

Burge, M.E. (2015), “Apple Pay, Bitcoin, and Consumers: The ABCs of Future Public Payments Law”, *Hastings Law Journal. Texas A&M University School of Law Legal Studies*, Vol. 67, pp. 1493–1550.

Cameron, A. (Lucy) and Trinh, K. (2017), “Four factors driving the price of Bitcoin”, *The Conversation*, available at: http://theconversation.com/four-factors-driving-the-price-of-bitcoin-87244 (accessed 16 May 2019).

Chaum, D. (1983), “Blind Signatures for Untraceable Payments”, in Chaum, D., Rivest, R.L. and Sherman, A.T. (Eds.), *Advances in Cryptology*, Springer US, Boston, MA, pp. 199–203.

Cheah, E.-T. and Fry, J. (2015), “Speculative bubbles in Bitcoin markets? An empirical investigation into the fundamental value of Bitcoin”, *Economics Letters*, Vol. 130, pp. 32–36.

CoinDesk. (2018), *State of Blockchain Q2 2018*, CoinDesk, available at: https://www.coindesk.com/research/state-of-blockchain-q2-2018 (accessed 5 January 2019).

Coinmetrics. (2019), “Granular mining pool mapping with Bitcoin’s coinbase outputs”, *CoinMetrics*, 7 January, available at: https://coinmetrics.io/mining-pool-mapping/ (accessed 16 May 2019).

Coleman, E.G. and Golub, A. (2008), “Hacker practice: Moral genres and the cultural articulation of liberalism”, *Anthropological Theory*, Vol. 8 No. 3, pp. 255–277.

Conti, M., E, S.K., Lal, C. and Ruj, S. (2018), “A Survey on Security and Privacy Issues of Bitcoin”, *IEEE Communications Surveys & Tutorials*, Vol. forthcoming, pp. 1–39.

Corradi, F. and Höfner, P. (2018), “The disenchantment of Bitcoin: unveiling the myth of a digital currency”, *International Review of Sociology*, Vol. 28 No. 1, pp. 193–207.

Creer, D., Crook, R., Hornsby, M., Gonzalez, N.A., Simpson, M., Weisfeld, N., Wyeth, B., et al. (2016), *Proving Ethereum for the Clearing Use Case*, Royal Bank of Scotland, available at: https://emerald-platform.gitlab.io/static/emeraldTechnicalPaper.pdf (accessed 13 April 2017).

De Filippi, P. (2014), "Bitcoin: a regulatory nightmare to a libertarian dream", *Internet Policy Review*, Vol. 3 No. 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*, Vol. 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*, Vol. 28 No. 3, pp. 321–338.

DeVries, P.D. (2016), "An Analysis of Cryptocurrency, Bitcoin, and the Future", Vol. 1 No. 2, p. 10.

Doolin, B. (2004), "Power and resistance in the implementation of a medical management information system", *Information Systems Journal*, Vol. 14 No. 4, pp. 343–362.

Du, W. (Derek), Pan, S.L., Leidner, D.E. and Ying, W. (2019), "Affordances, experimentation and actualization of FinTech: A blockchain implementation study", *The Journal of Strategic Information Systems*, Vol. 28 No. 1, pp. 50–65.

Dziembowski, S. (2015), "Introduction to Cryptocurrencies", ACM Press, pp. 1700–1701.

Eyal, I. and Sirer, E.G. (2018), "Majority is not enough: bitcoin mining is vulnerable", *Communications of the ACM*, Vol. 61 No. 7, pp. 95–102.

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

Gerlach, J.-C., Demos, G. and Sornette, D. (2018), *Dissection of Bitcoin's Multiscale Bubble History*, Swiss Finance Institute Research Paper No. 18-30, Rochester, NY, available at: https://papers.ssrn.com/abstract=3164246 (accessed 14 August 2018).

Gershenson, C. (2015), "Protecting Markets from Society: Non-Pecuniary Claims in American Corporate Democracy", *Politics & Society*, Vol. 43 No. 1, pp. 33–60.

Gervais, A., Karame, G.O., Wüst, K., Glykantzis, V., Ritzdorf, H. and Capkun, S. (2016), "On the Security and Performance of Proof of Work Blockchains", *2016 ACM SIGSAC Conference on Computer and Communications Security - CCS'16*, presented at the 2016 ACM SIGSAC Conference on Computer and Communications Security - CCS'16, ACM Press, Vienna, Austria, pp. 3–16.

Henfridsson, O. and Bygstad, B. (2013), "The Generative Mechanisms of Digital Infrastructure Evolution", *MIS Quarterly*, Vol. 37 No. 3, pp. 907–931.

Hindess, B. (1996), *Discourses of Power: From Hobbes to Foucault*, Blackwell Publishing, Oxford.

de la Horra, L.P., de la Fuente, G. and Perote, J. (2019), "The drivers of Bitcoin demand: A short and long-run analysis", *International Review of Financial Analysis*, Vol. 62, pp. 21–34.

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

Koutmos, D. (2019), "Market risk and Bitcoin returns", *Annals of Operations Research*, available at:https://doi.org/10.1007/s10479-019-03255-6.

Kypriotaki, K.N., Zamani, E.D. and Giaglis, G.M. (2015), "From Bitcoin to decentralized autonomous corporations: extending the application scope of decentralized peer-to-

peer networks and blockchains", *18th International Conference on Enterprise Information Systems (ICEIS 2015)*.
Latour, B. (1994), "On Technical Mediation", *Common Knowledge*, Vol. 3 No. 2, pp. 29–64.
Leclercq-Vandelannoitte, A. (2011), "Organizations as Discursive Constructions: A Foucauldian Approach", *Organization Studies*, Vol. 32 No. 9, pp. 1247–1271.
Maurer, B., Nelms, T.C. and Swartz, L. (2013), "'When perhaps the real problem is money itself!': the practical materiality of Bitcoin", *Social Semiotics*, Vol. 23 No. 2, pp. 261–277.
Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G.M. and Savage, S. (2016), "A fistful of Bitcoins: characterizing payments among men with no names", *Communications of the ACM*, Vol. 59 No. 4, pp. 86–93.
Mingers, J. (2004), "Real-izing information systems: critical realism as an underpinning philosophy for information systems", *Information and Organization*, Vol. 14 No. 2, pp. 87–103.
Mingers, J., Mutch, A. and Willcocks, L. (2013), "Critical Realism in Information Systems Research", *MIS Quarterly*, Vol. 37 No. 3, pp. 795–802.
Mingers, J. and Standing, C. (2017), "Why things happen – Developing the critical realist view of causal mechanisms", *Information and Organization*, Vol. 27 No. 3, pp. 171–189.
Nakamoto, S. (2008a), "Bitcoin: A peer-to-peer electronic cash system", *Nakamoto Institute*, available at: http://nakamotoinstitute.org/bitcoin/.
Nakamoto, S. (2008b), "Cryptography Mailing List. Bitcoin P2P e-cash paper", *Nakamoto Institute*, available at: https://satoshi.nakamotoinstitute.org/emails/cryptography/13/ (accessed 10 May 2019).
Narayanan, A. (2013), "What Happened to the Crypto Dream?, Part 1", *IEEE Security & Privacy*, Vol. 11 No. 2, pp. 75–76.
Nicholson, J., Tsagdis, D. and Brennan, R. (2013), "The structuration of relational space: Implications for firm and regional competitiveness", *Industrial Marketing Management*, Vol. 42 No. 3, pp. 372–381.
Orlikowski, W. and Baroudi, J.J. (1991), "Studying Information Technology in Organizations: Research Approaches and Assumptions", *Information Systems Research*, Vol. 2 No. 1, pp. 1–28.
Palermo, G. (2007), "The ontology of economic power in capitalism: mainstream economics and Marx", *Cambridge Journal of Economics*, Vol. 31 No. 4, pp. 539–561.
Palermo, G. (2014), "The economic debate on power: a Marxist critique", *Journal of Economic Methodology*, Vol. 21 No. 2, pp. 175–192.
Peck, M.E. (2017), "Why the Biggest Bitcoin Mines Are in China", *IEEE Spectrum*, 4 October, available at: https://spectrum.ieee.org/computing/networks/why-the-biggest-bitcoin-mines-are-in-china (accessed 11 June 2018).
Puthal, D., Malik, N., Mohanty, S.P., Kougianos, E. and Yang, C. (2018), "The Blockchain as a Decentralized Security Framework [Future Directions]", *IEEE Consumer Electronics Magazine*, Vol. 7 No. 2, pp. 18–21.
Reed, M. (1998), "Organizational analysis as discourse analysis: A critique", in Grant, D., Keenoy, T. and Oswick, C. (Eds.), *Discourse and Organization*, Sage, London.
Reid, F. and Harrigan, M. (2013), "An Analysis of Anonymity in the Bitcoin System", in Altshuler, Y., Elovici, Y., Cremers, A.B., Aharony, N. and Pentland, A. (Eds.), *Security and Privacy in Social Networks*, Springer New York, New York, NY, pp. 197–223.

Sayer, A. (2012), “Power, causality and normativity: a critical realist critique of Foucault”, *Journal of Political Power,* Vol. 5 No. 2, pp. 179–194.
Schaupp, L.C. and Festa, M. (2018), “Cryptocurrency adoption and the road to regulation”, *Dg.o ’18 Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age*, presented at the dg.o ’18 Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age, ACM Press, pp. 1–9.
Sedgwick, K. (2018), “Bitcoin History Part 6: The First Bitcoin Exchange”, *Bitcoin.Com*, 25 December, available at: https://news.bitcoin.com/bitcoin-history-part-6-the-first-bitcoin-exchange/ (accessed 10 May 2019).
Shahzad, S.J.H., Bouri, E., Roubaud, D., Kristoufek, L. and Lucey, B. (2019), “Is Bitcoin a better safe-haven investment than gold and commodities?”, *International Review of Financial Analysis,* available at:https://doi.org/10.1016/j.irfa.2019.01.002.
Shapiro, D.C. (2018), “Taxation and Regulation in Decentralized Exchanges”, *Journal of Taxation of Investments*, Vol. 36 No. 1, pp. 3–13.
Swartz, L. (2018), “What was Bitcoin, what will it be? The techno-economic imaginaries of a new money technology”, *Cultural Studies*, Vol. 32 No. 4, pp. 623–650.
Taylor, M.B. (2017), “The Evolution of Bitcoin Hardware”, *Computer,* Vol. 50 No. 9, pp. 58–66.
Tuwiner, J. (2019), “Bitcoin Mining Pools”, 29 January, 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*, Vol. 6 No. 3, pp. 689–707.
Vidan, G. and Lehdonvirta, V. (2018), “Mine the gap: Bitcoin and the maintenance of trustlessness”, *New Media & Society,* p. 146144481878622.
Volkoff, O. and Strong, D.M. (2013), “Critical Realism and Affordances: Theorizing IT-Associated Organizational Change Processes”, *MIS Quarterly,* Vol. 37 No. 3, pp. 819–834.
Westphal, A. (2015), “Blockchain”, *International Capital Market Association*, 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, E., He, Y. and Phillips, M. (2018), “On the Security Risks of the Blockchain”, *Journal of Computer Information Systems*, pp. 1–12.
Zamani, E.D. and Babatsikos, I. (2017), “The Use Of Bitcoins In Light Of The Financial Crisis: The Case Of Greece”, *Mediterranean Conference on Information Systems (MCIS),* presented at the Mediterranean Conference on Information Systems (MCIS), Genoa, Italy, p. 13.
Zuboff, S. (1988), *In the Age of Smart Machines*, Basic Books.