Governance and control in distributed ledgers: Understanding the challenges facing blockchain technology in financial services

Dr Markos Zachariadis\*

Information Systems & Management Group, Warwick Business School,

The University of Warwick, Coventry, United Kingdom, CV4 7AL.

Dr Garrick Hileman

Centre for Macroeconomics, Department of Economics, London School of Economics,

Houghton Street, London, United Kingdom, WC2A 2AE

Dr Susan V. Scott

Information Systems & Innovation Group, Department of Management, London School of Economics,

Houghton Street, London, United Kingdom, WC2A 2AE.

## **Abstract**

As blockchain platforms are becoming increasingly noticeable in financial services and beyond, questions arise regarding their suitability to compete with or replace existing payment systems and marketplaces and redesign the financial infrastructures of the future. Prominent amongst these concerns are issues around governance and control in distributed ledgers: How are distributed ledger technologies governed? Can blockchains address complex administration problems? What key issues of note for practitioners and academics have emerged thus far? In this paper we aim to review the existing governance practices of established or popular blockchain and decentralized autonomous organization (DAO) systems with a view to understanding how they hold up in times of crises. What questions are raised when they are compromised or faced consensus challenges in coordinating action especially around control and accountability? We use a translational process, generating focal insights about present concerns from the reference point of completed academic studies and extensive practitioner consultation. Rather than adopting a declarative approach attempting to provide all the answers, we draw insights from the IT platform governance literature to offer a critical perspective for asking the right questions around key governance issues in financial infrastructure such as decision rights, control mechanisms, and incentives.

*Keywords:* Financial infrastructures, blockchain, distributed ledger technology, distributed autonomous organization, payment systems, governance, Ethereum, Bitcoin, cryptocurrencies.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

“We are stuck with technology when
what we really want is just stuff that works”

― Douglas Adams,

Author of *The Ultimate Hitchhiker's Guide to the Galaxy*

1. **Introduction**

 Blockchain technology has been portrayed as the “next-generation Internet” (Shermin, 2017), a new “foundational technology” (Iansiti & Lakhani 2017) with the potential to reshape financial transactions, influence how people interact in economic life, and even change society. Analysts foresee it transforming a wide-ranging set of processes from finance to manufacturing, healthcare, government and beyond[[1]](#footnote-1). It is routinely described as a disruptive, “game-changing” innovation with some claiming that its long-term influence may prove to be even more significant than the World Wide Web or the Internet (MacIver, 2016; Tapscott & Tapscott, 2016). Indeed, a recent *Harvard Business Review* article claims that “blockchain will do to banks and law firms what the Internet did to media” (Ito et al., 2017).

 Despite this broad base of interest and recognition, many applications of blockchain technology have attracted concern. Whether it is distributed autonomous organisations (DAOs) that sit on top of blockchain infrastructures or initial coin offerings (ICOs) that utilize existing digital tokens to raise capital, many Bitcoin-like digital currencies have been characterised as “Ponzi schemes” or at best “solutions in search of a problem”[[2]](#footnote-2). Some critics have cautioned that if we embrace such a technological shift it will attract criminal activity, if not paving the way for anarchy then at least fuelling the rise of a particular form of authoritarianism (Werbach, 2018). While opinions about blockchain’s efficacy and legitimacy vary dramatically, even the firmest supporters of the ‘blockchain revolution’ have conceded that the biggest single challenge for the growth of distributed ledgers is and will be governance: “Any controversy that you read about [blockchain] today is going to revolve around these governance issues.”[[3]](#footnote-3) Unlike existing foundational technologies like the Internet which is governed by well-established international organizations and consortia (for example the IETF[[4]](#footnote-4), Internet Governance Forum[[5]](#footnote-5), W3C[[6]](#footnote-6), ICANN[[7]](#footnote-7), Internet Society, etc.), current blockchain platforms and cryptocurrency communities are deemed to be chaotic at best with little or no structure to achieve consensus, coordinate action, and resolve differences (Kirkland & Tapscott, 2016). Understandably, this could jeopardize the widespread adoption of the technology and future blockchain applications but most importantly it poses significant risks to users as well as growing concern for regulators, especially in financial services where any threat to the stability and trust in the fiscal environment are of paramount importance.

 In this paper, we highlight the characteristics of blockchain-inspired, distributed ledger technologies and examine their efficacy as part of the financial services infrastructure. Our approach is to generate focal insights about present governance concerns from the reference point of completed academic studies and extensive practitioner consultation. We employ a translational process to guide us toward relevant questions about the present and future of governance practices in financial services. To guide our thinking, we borrow from the literature on IT platform governance (Wareham et al, 2014; Weill & Ross, 2004; Weill, 2004; Tiwana, 2013; Tiwanaet al, 2010; etc.) and use it as a lens to examine key governance features such as decision rights, control mechanisms, and incentives structures in digital infrastructures. As the conversation around blockchain evolves and moves beyond Bitcoin, practitioners and policymakers have started considering not just the fundamental properties of blockchain technology, but also the complexities of the institutional, legal and socio-economic premises of the environment being created. We illustrate our discussion using critical situations where existing blockchains have been challenged and experienced crises that put their governance models to the test. We use these ‘moments of interest’ to assess issues of trust, risk, and efficiency that lie at the heart of robust functioning financial systems. This enables us to present a succinct discussion of capabilities and conditions of governance that provides insights into mission-making or -breaking challenges.

 The structure of our paper is as follows: we begin by grounding our ideas within the existing literature on information infrastructures, digital platforms and IT governance. We then provide an accessible description of blockchains and digital ledger technologies before reviewing the promise they hold as a foundational technology for financial services. In so doing, we draw out specific concerns about governance surrounding blockchain and its applications. Finally, we use a number of examples where ‘things went wrong’ in order to explore how issues of governance emerged and the manner in which particular challenges were addressed. This allows us to identify the limitations of existing governance arrangements among existing distributed ledger systems, DAOs, and ICOs. We close by revisiting the notion of blockchain governance in light of both the illustrations and literature we discuss. Our conclusion summarises the implications of our discussion for future developments in infrastructural technologies and identifies critical areas for future research including blockchain scalability, openness, standards, liability, transparency, and security.

1. **The challenge of governance**

Governance is a topic that spans all institutional contexts across the history of society and economic thought. The question of how best to structure and steer organizational processes has been a perennial one faced by sovereign powers, local economies, corporations, public bodies and even religious institutions. This is because the capacity to resolve disputes and create consensus when actors have different incentives and interests is central to responsible organizational work processes. Business administration and management scholars define corporate governance as the mechanisms that address “managerial accountability, board structure, and shareholder rights” in multi-member organizations that are seeking collective action (Cheffins, 2013; p.46). Through these mechanisms business organizations “oversee, execute, and maintain a complex series of interacting agreements between the organization’s different stakeholders” (Reyes et al., 2017; p.14).

In economics the problem of efficient governance has been approached from the viewpoint of transaction costs and how these can affect the production of goods and services in firms (Coase, 1937; Williamson, 1975; 1979). Transaction cost theory aims to expose the optimal governance of contractual relations and economic coordination – hierarchical organizations or markets – in the face of uncertainty and opportunistic behaviour from the various actors. Most of the relational contracting or market mechanisms require some form of trust, or “established character”, between the transacting parties which is not always present. A hierarchy provides protection against opportunism, especially when the payoff of one’s investment largely depends on transaction-specific assets and high frequency of dealings (Williamson, 1979). Hierarchical modes of governance are usually regarded as most effective when there is “contractual incompleteness” due to the transacting parties’ inability to write complete contracts that cover all unforeseen contingencies and rule enforcing issues (Williamson, 1985; Hart & Moore, 1990; Davidson et al, 2018). In this context, information plays a crucial role. Information asymmetries between counterparties will generally increase the probability of adverse selection and moral hazard thus incurring further transaction costs as both sides will need to introduce further policies and complex contracting to battle uncertainty (Akerlof, 1970). The greater the uncertainties (and higher the transaction costs), the more this disadvantages the *marketplace* as a model for effective governance and coordination of economic activity (i.e. bilateral trading) where people transact on a peer-to-peer basis.

The above theoretical position on transaction costs justifies to a certain degree the emergence of a vertically-integrated organizational form that concentrates (or centralizes) economic production and confines it within the boundaries of the firm (Coase, 1937). Such organizational forms have dominated the international business landscape since the industrial revolution. Over the last few decades practitioners have experimented with flatter and less centralised modes of organizing that support flexible work practices offering more autonomy to different parts of the firm in order to encourage the development of innovative products and services (Shermin, 2017).

Management scholars have identified a number of approaches to governing economic activity that vary from “project-based” (Sydow et al., 2004) to “temporary” (Bakker, 2010) and even “disposable” (March, 1995) organizations. This marks a move away from classic, vertically integrated models of hierarchically governed firms toward more configurable organizational forms capable of coordinating production through “orchestration” (Nambisan & Sawhney, 2017). Alongside the rise of more diverse organizational forms, a demand for different governance arrangements capable of supporting more distributed work practices has emerged. The challenge is to keep pace with emergent and reconfiguring innovations while establishing contractual faith and trust between counterparties. As we will discuss in the next sub-section, while Internet-based digital platforms have managed to navigate the construction of trusted governance mechanisms, this still represents a key challenge for the current generation of blockchain technologies in financial services.

***2.1 Governing IT infrastructures and digital platforms***

The efficiency gains and opportunities produced by widespread digitization of transactions led to new organizational forms, motivating the design of next generation of governance processes. For example, while the Internet facilitated organizational innovation (Shermin, 2017, p.501), trust between counterparties transacting over its TCP/IP network infrastructure was not initially assured. In this space, “powerful intermediaries” (Edelman, 2014) emerged offering ways to govern the relationships between buyers and sellers, lenders and borrowers, etc. and ensure the coordination and integrity of economic transactions by imposing rules and exercising control over the relevant operations.

The Internet became a new foundational technology enabling the rise of digital platforms such as Google, Amazon, Facebook, Airbnb, and UBER. Digital platforms do not usually sell goods and services directly to consumers but act as ‘matchmakers’ mitigating trust relations in economic exchanges. Essentially, they function as two-sided marketplaces that facilitate the relationship between users who want to purchase (or rent) a good and actors able to fulfill that demand by selling or lending that good through the platform (Rochet & Tirole, 2006). Their success relies on their capacity to “sell reductions in transaction costs” (Munger, 2015) by minimizing opportunistic behavior through careful curation and governance (Benzell et al., 2017), thus making the platform attractive to users who eventually increase their net utility.

The popularity and influence of such platforms, and of the ecosystem around them, means that the rules they impose and their approach to governance plays a significant role in the way economic actors transact and the way economic activity is realized. Information systems and management scholars have studied the governance of such IT infrastructures and digital platforms extensively and have made efforts to systematically highlight the key dimensions of their structural forms. In prior literature, IT governance is defined as the “set of mechanisms” ensuring delivery of IT capabilities for the organization (Loh & Venkatraman, 1992; Henderson & Venkatraman, 1993). In a study of how top-performing firms govern IT, Weill (2004, p.4) provides detailed insight into frameworks of “decision rights and accountabilities to encourage desirable behavior in the use of IT”. He underlines a number of important characteristics of IT governance which he maintains is: “…about systematically determining who makes each type of decision (a decision right), who has input to a decision (an input right), and how these people (or groups) are held accountable for their role”. More recently, Tiwana et al. (2010), have stressed the need to move away from framing IT as a function within the organization (i.e. a discrete department or capability) and instead emphasizes the significance of new forms of governance in “platform-based software ecosystems” (p.675).

Building on the basic premise that governance is “who makes what decisions about a platform”, Tiwana et al (2010) claim that the biggest challenge in governing a digital platform is the “delicate balance of *control*” by the owner (p.676). This point is also emphasized by Wareham et al., (2014) who note the criticality of ensuring the integrity of the platform while simultaneously enabling autonomy among independent module developers in order to encourage innovation. The trade-offs that this entails influence the evolutionary dynamics of ecosystems and modules associated with the platform as it attempts to optimize its capabilities for further innovation. All of this sums up to a different set of demands and pressures upon governance especially when compared to centralized, hierarchical and highly integrated organizations with pipeline business models as the basis for their value chains. Digital platform governance needs mechanisms and policies that meet the needs of a modular and layered architecture (Constantinides et al. 2018; Parker & Van Alstyne, 2017; Rochet & Tirole, 2003). Such an approach to governance must steer a set of distinct issues relating to capacity, performance and utility that are critical to the continued development of multiple inter-related and inter-operable information systems comprising the digital platform.

In the literature, there are three different aspects of digital platform governance design relevant to our discussion in this paper (Tiwana, 2013; Tiwana et al., 2010; Wareham et al., 2014; Constantinides et al., 2018). First, the allocation and partitioning of decision rights addresses the “who has the authority and responsibility to do what” on the platform. These decision rights can range from: defining the functionality that the system and its modules should have (i.e. strategic decision making); how these will be executed (i.e. implementation decision-making); and the design of interfaces or APIs determining interoperability (i.e. control over inter-organizational boundaries). How these decision-making rights are divided up between the platform owners[[8]](#footnote-8) and module developers or users will reflect the level of decentralization the platform aims to achieve through its governance (Baldwin and Woodard, 2009).

Information infrastructures (IIs) scholars have argued that hierarchical and more centralized, “top-down” governance approaches are not usually effective due to the IIs dynamic complexity, varying needs of multiple stakeholders, and a tendency for the development of IIs to ‘drift’ (Hanseth & Lyytinen, 2004; Sahay et al., 2009). Instead, a “bottom-up” design is regarded as better able to facilitate the IIs performance and scalability. Prior research further suggests that information infrastructures are “sociotechnically interdependent on the heterogeneity of interests and resources of a distributed user base” (Constantinides & Barrett, 2015; p.3). This effectively means that the actor’s different ideological goals and interpretations will influence their decisions and collective action as well as the means through which they will seek to ensure the platforms future development and scalability.

The second aspect of governance relating to digital platforms involves the control mechanisms (informal or formal) that platform owners will implement in order to ensure the “good behaviour” of module developers and users. This includes guidance on the organizational and management processes that they are expected to follow, enforcing rules, holding participants accountable, and employing metrics, etc. (Constantinides et al., 2018). Control can also be exercised in the opposite direction with platform participants scrutinizing owner’s actions and questioning the decisions that have been made. In decentralised and open settings, where there is no authoritarian regime to make decisions, control mechanisms tend to be more informal “coordination” procedures that foster common values and shared beliefs (Tiwana et al., 2010).

The third aspect of governance that we highlight are the incentive structures put in place to “influence the strategic behavior of stakeholders and the monetary profits of the platform” (Constantinides et al., 2018; p.4). Providing incentives for producers and consumers is crucial to maintain the interests of the platform participants who contribute to its value. Depending on the ownership structure and the partitioning of the decision rights on the platform, it can sometimes be challenging to align interests and ensure that all stakeholders maintain their competitive position; e.g. platform owners enjoy higher platform profits while at the same time producers and users benefit from increased value in the ecosystem (Boudreau & Hagiu, 2009). This review of the digital platform literature is a useful starting point for our examination of blockchain governance, providing a set of familiar features that enable us to highlight the most important similarities and differences among these distinctive emerging technologies.

1. **Blockchains and Distributed Ledger Technologies**

In this section, we begin by describing the characteristics of blockchain technologies in order to better understand their potential as a new foundational technology, transforming how we organize economic activity in the future. In so doing, we distinguish blockchain from the general classification of distributed (or shared) ledgers. We then focus on a particular sub-set of blockchain technologies currently being used to transfer value and provide financial services. Our aim is to explore how closely these instantiations of blockchain exemplify the principle of distributed governance described above. More particularly, we examine the strengths and limitations of the different governance arrangements underlying the current generation of financial services blockchain.

***3.1 A problem of definition***

Defining what a blockchain is (and is not), and how blockchains differ from other types of distributed databases, is a subject of considerable confusion and debate (Hileman & Rauchs, 2017). Narayanan and Clark (2017) state that “the term blockchain has no standard technical definition but is a loose umbrella term used by various parties to refer to systems that bear varying levels of resemblance to Bitcoin and its ledger”.[[9]](#footnote-9) Most (if not all) of the components of what is generally defined today as a blockchain existed many years prior to Bitcoin.[[10]](#footnote-10) However, it was Satoshi Nakamoto’s invention of a novel peer-to-peer electronic cash system, which he first publicly described in a paper published on 31 October, 2008 and then put into operation on 3 January, 2009, that popularized blockchain technology (Nakamoto, 2008).[[11]](#footnote-11)

Understanding the fundamental differences between the various blockchain technologies is a necessary condition in order to lay the groundwork needed to understand the conditions and rules that govern digital ledger technology platforms and lead to the design of successful applications (Saito & Yamada, 2016). In essence, a blockchain is a distributed database system managed by a peer-to-peer network of computing devices that provides a shared, yet accurate record (Werbach, 2018). The governing principles and parameters of the various blockchains that have been developed since Bitcoin can differ, but all blockchains feature a similar data structure and distributed architecture. In all blockchain systems, new transactions and other information to be added to the database are bundled into ‘blocks’ by network participants. After a new block is deemed valid by the network it is appended (‘chained’) in sequential order to the previously validated block. As new transactions occur this process is repeated. The blockchain is maintained and replicated across a distributed set of nodes that abide by set of rules (a consensus mechanism) to process *bona fide* transactions and maintain the integrity of the database. Various incentives exist for nodes[[12]](#footnote-12) to contribute resources to the network, such as rewards in the form of newly issued tokens (coins) and transaction fees. Blockchains employ various forms of cryptography (e.g. public/private key infrastructure, hash functions, etc.) to secure the database and its users from attacks and other malicious behaviour, such as ‘double spending’ tokens.

Where debate over the definition of a blockchain tends to emerge is in the area of blockchain principles. Murck (2017) claims there are five key principles underlying the definition of a blockchain: irreversibility of records (also sometimes referred to as “immutability”), transparency, peer-to-peer transmission, distributed architecture, and computational logic. Under examination, some of these principles raise questions. For example, if events recorded on a blockchain are reversed, (as occurred during the July 2016 Ethereum hard-fork which we discuss below), would a blockchain platform no longer be considered a blockchain? For some scholars who follow this debate, immutability is not an essential feature of a blockchain given the ever-present potential for chain reorganizations and the fundamental probabilistic nature of blockchains (Saito & Yamada, 2016).

More recently, the term ‘distributed ledger technology’ (DLT) has come to be used to describe a broader class of ‘blockchain inspired’ technology. One example of this might be the distributed ledger system called “Corda”[[13]](#footnote-13) which has been developed by “R3”, a blockchain financial services consortium. Some of these distributed ledgers, while resembling the Bitcoin blockchain, can differ in several important respects, such as data access restrictions, limits on which parties can validate transactions, and other features (Hileman & Rauchs, 2017). These particular types of distributed ledgers sometimes go by the name of ‘permissioned’ ledgers due to their restrictions on network participation. According to Gendal-Brown (2017), permissioned ledgers are similar to ‘public’ or ‘permissionless’ blockchains because they are both “systems that enable parties who don’t fully trust each other to form and maintain consensus about the existence, status and evolution of a set of shared facts”. This quality of distributed ledgers underscores a key difference between them and other types of distributed databases (and why an institution might want to employ one or the other).



**Figure 1 – Distributed databases, distributed ledgers, and blockchains.**

*Note*: Figure 1 shows the different groupings of distributed technologies that broadly belong to the blockchain-inspired universe. Blockchains occupy the narrow space of technologies that use a data structure comprised of a chain of linked blocks. Distributed ledgers are broader in nature and assume the presence of malicious nodes. Finally, distributed databases are more inclusive of all types of distributed systems even when they are governed by a single operator.

Like a distributed database, distributed ledgers employ multiple CPUs dispersed across different physical locations to provide data redundancy and network resiliency. In terms of governance, a distributed database arguably has more in common with centralized databases than with distributed ledgers; control over the distributed database is often in the hands of single operator. Distributed databases are not designed for the prospect that a node may potentially have different motivations, priorities, and code of conduct than other nodes within the same database. In short, a distributed ledger may not be the best solution in a trusted setting where perfect alignment exists across the goals and incentives of different database nodes and stakeholders. However, for the many other types of networks and relationships where the possibility of an adversarial relationship could develop (e.g., customer-business, government-citizen, and marketplaces such as securities trading) a distributed ledger may provide a number of advantages over more traditional centralized database governance structures.

Iansiti & Lakhani (2017) draw a comparison with TCP/IP and its historical step-change from circuit switching. Using smart contracts as their illustrative example, they maintain that blockchain innovations could transform the regulation and maintenance of administrative control saying that in a distributed digital ledger*:*

“…contracts are embedded in digital code and stored in transparent, shared databases, where they are protected from deletion, tampering, and revision. In this world every agreement, every process, every task, and every payment would have a digital record and signature that could be identified, validated, stored, and shared. Intermediaries like lawyers, brokers, and bankers might no longer be necessary. Individuals, organizations, machines, and algorithms would freely transact and interact with one another with little friction. This is the immense potential of blockchain” (p. 120).

The resiliency of blockchain technology has received particular focus; Bitcoin, which is believed to be the world’s most powerful ever computing network, has effectively suffered zero downtime since it first became operational in January 2009. The Bitcoin network, which currently operates across nearly ten thousand nodes that are running in close to one hundred different countries[[14]](#footnote-14), is also now broadcasting transaction data from satellites in Earth’s orbit[[15]](#footnote-15). The massive replication and redundancy enabled by distributed ledger technology, managed by parties that may not know or trust each other, could make an important contribution to design of critical infrastructure systems, such as energy and payments.

A further defining characteristic of distributed ledger phenomena is whether they represent a public or private initiative. In the minds of many, blockchain is closely associated and it has become synonymous with cryptocurrencies such as Bitcoin. But it is important to recognize that distributed ledger computing may have other non-currency applications and eventually help us address a broad range of multi-stakeholder challenges. Within financial services, there are areas in which DLT innovation could make a critical difference; for example, clearing and settlement of securities, cross-border payments, financial inclusion, etc. While these areas provide a significant opportunity for development and innovation, it is hard for some to envision how these could depend on public blockchain networks that are accessible to all with no or little screening. As a result, it is private blockchain innovations that are attracting the most interest in the traditional financial sector at the current time and are considered most probable for early adoption. This interest is taking the form of in-house experiments by incumbents, formation of alliances, investment in venture capital, emergence of large consortiums as well as small entrepreneurial start-ups (Hileman & Rauchs, 2017). In this paper, we have chosen to compare and contrast our knowledge of existing digital platforms with the specific governance arrangements exemplifying blockchain.

***3.2 Distributed governance***

 Blockchain is undoubtedly technologically complex but all distributed ledgers share a basic premise which shapes their day-to-day operation and governance: they offer a decentralised infrastructure to maintain the ‘single version of truth’ recording all changes made on the blockchain database since its formation. Their distributed governance is realised without the need for a central authority as all nodes in the peer-to-peer (P2P) network share the same full copy of the database (a “shared ledger”) and thus no administrator needs to hold a “master version” (hence avoiding a ‘single point of failure’ in the network). Distributed ledgers are thus characterised as “organizationally decentralised” since many network participants share a database but “logically centralised” because there is a single shared ledger[[16]](#footnote-16). The decentralized peer-to-peer architecture works in a similar way to other popular P2P software programs like Gnutella, Kazaa, and BitTorrent where users can participate by downloading software and installing it on their computers in order to participate. The practical implications for governance are that blockchain infrastructures, like Bitcoin, have no official organization or physical and legal entity “in charge” that operates the network and is responsible for its performance or failures (Walch, 2015). This marks a major difference with privately-owned technological infrastructures or shareholder-owned digital platforms such as Facebook and Amazon.

 But what about the kind of informal organizational governance that typifies online open-source communities? If we look more closely at Bitcoin, the largest public blockchain platform and cyptocurrency to date, we find some similarities with open-source: both have been founded and maintained by diverse community members exhibiting multiple identities, varying in stakeholder interests. ‘Bitcoin-ers’ range from general technical participants (software developers who maintain or ‘debug’ code), to miners who run the code required to form blockchain, to the ‘users’ who, through their digital wallets, purchase, store and transfer value in the form of Bitcoin. However, unlike open-source communities where roles and responsibilities are assigned to expert technical participants, in Bitcoin these groups of software developers are “just an amorphous, ever-shifting cluster of people who come and go […] as they please” (Walch, 2015; p.35). This presents challenges in terms of governance because if action is urgently required (e.g. crisis threatens the continuity of the system or a repair is needed), Bitcoin’s stakeholders can only rely on voluntary contributions. Perhaps more importantly, Bitcoin developers can’t be held accountable or responsible for any of the code they produce or for the solutions they suggest and implement.

 Unlike digital platforms where responsibility is held by accountable individuals and groups that can be traced back through an organizational chart, Bitcoin governance protocol is purely passive and cumulative. In other words, if significant changes are needed that will affect the rules of the system (e.g. dealing with standard IT infrastructure issues such as scalability and performance, etc.) no single participant or group of developers have the formal legitimacy to act on behalf of the broader community. There is no commonly acceptable election point or form of input through which users can provide feedback on the codebase changes. Even the timeframe in which action must be taken is not specified. Instead, progress on issues can only be made when there is sufficient buy-in from other members and an absolute majority of users decide to install software updates to replace older versions. Consequently, decision-making can be time-consuming and inefficient.

 The difficulty of enacting governance processes in the Bitcoin community has led to periodic crises in collective action and control. For example, as discussed in the section on digital platform governance, scalability is a major issue for IT infrastructures and blockchain is no exception. Inability to resolve the trade-off between encouraging diverse participation base (able to mine small blocks) and the need to scale up (potentially fewer participants mining larger blocks) fuelled what became known as the “block size debate”. Dissatisfaction has resulted in multiple “hard forks” since the launch of Bitcoin’s operation in 2009 (Metz, 2015). So-called ‘forks’ in the blockchain system happen when newer versions of the codebase are issued and widely adopted but are incompatible with prior releases. Depending on how many users and miners install the new software release, the system can end up with two different blockchains which can create confusion among participants and pose serious risk for token value. Whilst there have been attempts to reform voting on the Bitcoin blockchain[[17]](#footnote-17), it is widely acknowledged that further effort is needed in this area.

 Moving to the Ethereum public blockchain system, the second largest according to its market capitalization or value of coins in distribution, we find it is also based on an open-source protocol. Its most active developers influence the direction of the technology through the Ethereum Improvement Proposals (EIPs). It is perhaps closer to some open-source models because it has a ‘benevolent dictator’, Vitalik Buterin. Having authored the white paper (2013) defining the concept of Ethereum, Buterin became its founder and creator. He holds significant influence over the community and remains the single top contributor of EIPs making him a defining figure in Ethereum’s development[[18]](#footnote-18). In the past, Buterin has admitted weaknesses in the governance of the Ethereum platform, particularly the process for reaching consensus and facilitating collective action: “voice or exit? Do you make your opinion known through a voting process or complain on online channels like Reddit, or going to a town-hall meeting, or you just pack up your bag and go somewhere else?”[[19]](#footnote-19)

The enduring paradox of blockchain is that although it is one of the most distributed foundational technologies ever developed, its governance is often comprised of simple majority voting mechanisms that are potentially vulnerable to lobbyists (for example investors) and/or the influence of particularly active contributors. This means that ironically “their governance structures have a seemingly inherent degree of centralization” (Azouvi et al. 2018; p.2). The governance of Internet-based commercial digital platforms is also centralised but arguably they display quite different forms of accountability and control mechanisms.

Blockchain’s openness is thus both its strength and its vulnerability with decision-rights ‘up for grabs’, available to anyone who can put in the time to make improvement proposals and write code. To counter this, both Bitcoin and Ethereum communities have created Foundations to encourage participation from a broad base of developers in a bid to enlarge the community of contributors and make voting mechanisms less prone to ‘capture’ by lobbyists. Indeed, a recent initiative from Ethereum designed to make decision-making more systematic, proposes experimenting with different voting mechanisms that will make its governance structure more effective[[20]](#footnote-20). The realisation that existing voting rights can produce a polarizing majority-driven tipping point is counter-intuitive and against public perception that the governance of permissionless(or public)ledgers is not only decentralized but directed by a form of negotiated politically-assured consensus. Consensus does lie at the core of blockchain governance but as we will go on to discuss in the next sub-section, the way it functions is defined by agreed coding norms and practices rather than democratic process.

***3.3 “One code to rule them all”***

 Arguably the most technically complex part of a blockchain, with the most defining influence on its governance, is the mechanism that creates consensus between nodes and decides (or controls) which copy of the transactional database needs to be distributed amongst the members of the network. This is what makes participants trust the system and ensures the integrity of the transactions in the entire ledger. While there are many consensus mechanisms depending on the blockchain or DLT in use, the most widely adopted is the ‘proof-of-work’ consensus (also known as the Nakamoto consensus after Bitcoin’s founder) which is used by many public blockchains, including Bitcoin and Ethereum.

 According to the software code, the verification of transactions takes place by certain actors (miners) who compete by dedicating costly computing power in order to solve a mathematical problem involving cryptographic hashes on the network. When the problem is solved, the block containing payment instructions from users is ‘chained’ to the previous blocks by broadcasting the block across the entire network and thus the transactions are executed (or more accurately, are permanently part of the distributed ledger).

 The second way in which code is implicated in blockchain governance is in the operation of the infrastructure where technical code exercises control and rules the behaviour of network participants as well as defining the incentives on the platform to ensure continuity (Lehdonvirta & Robleh, 2016). The incentive for the miners is that their efforts are rewarded with new bitcoins (or ether, the native cryptocurrency on the Ethereum blockchain) issued to them. Making the process resource-intensive and time-consuming makes it more difficult for an attack to occur that will compromise the integrity of the ledger.[[21]](#footnote-21) Depending on the blockchain platform and ‘proof-of-work’ protocol, the algorithmic code decides on the difficulty of the cryptographic problem in order to moderate the frequency with which blocks are being created and validated. This is mostly to regulate the pace with which coins are being created and to keep incentivising miners.

 The code-driven consensus mechanism characterizing blockchain is equivalent to the settlement phase of a payment system because the tamper resistant nature of distributed ledgers gives finality to transactions. This is the main reason why blockchain technology is generally deemed to be an important contender for the payment infrastructures of the future effectively enabling the financial services sector to overcome bottlenecks in existing payment networks. It creates a new form of trust minimization and allows the efficient communication of value between counterparties that do not fully trust one another and would normally have to pay for independent intermediation in order to ensure the fair and safe completion of a transaction. However, while many blockchain platforms are often transparent, they are (pseudo-) anonymous networks and do not provide any “know-your-customer” (KYC) functionality which traditional payment systems are currently required to provide.

***3.4 Smart contracts and the emergence of DAOs***

 While Bitcoin and Ethereum are both open-source, public distributed ledgers utilizing “proof-of-work” consensus mechanisms, they were built for different purposes. Bitcoin focused more on basic (crypto-)fund transfers utilizing the technology and technical code to achieve a more seamless and secure transfer of tokens without central authorities[[22]](#footnote-22). On the other hand, Ethereum’s philosophy was to build “an alternative protocol for building decentralized applications”[[23]](#footnote-23). The key to this is its Turing-complete scripting language that allows software developers to produce distributed applications (or DApps) like they would for any other computer system – only this time these would run on the Ethereum distributed consensus network. Distributed applications are largely based on smart contracts, first described by cryptocurrency pioneer Nick Szabo in 1994, that “enable complex relationships to be layered into, or on top of, the underlying DLT protocol” (Reyes et al., 2017; p.11).[[24]](#footnote-24) These are in principle “self-executing digital contracts” based on a computer algorithm or protocol that structure relationships between counterparties in a self-enforcing way (Davidson et al., 2018).

 The potential of smart contracts has been widely applauded and are actively being explored by many organizations in various industries as a way to take further advantage of blockchain technology. Due to their popularity, Ethereum (which was launched in July 2015) has become one of the most promising platforms in the blockchain realm engaging a large part of the blockchain and finance communities and reaching a “market capitalization” of $1 billion within a year. One of the most ambitious decentralised applications made possible by smart (digital) contracts is the founding of ‘distributed autonomous organizations’ (DAO), that purely encoded and executed on the blockchain can replace traditional organizational functions (e.g. raise capital, voting, pay salaries, dividents, etc.). While this can have implications in many domains of social and political life, at the business and organizational levels it can impact the way economic production is organized.

 By revisiting our previous analysis around the problem of efficient governance in organizations, it is clear that blockchain technology and smart contracts can challenge the “economic efficiency of hierarchies (which exploits incomplete contracts) and relational contracting over markets (which requires trust between parties)” (Davidson et al., 2018; p.9) by minimizing opportunism. This however, can only be made possible if we assume that one can develop and code complete contracts in a world where firms function on the basis of incomplete contracts. In addition, encoding all contractual agreements and organizational relationships on the blockchain can create significant risks. For example, if governance and trust purely depend on the code base, then – by definition – finding a loophole in the code and (e.g. siphoning off funds, or bypassing agreements) would make it a legitimate action and allowable ‘within code’.

 To illustrate this, in the next section we briefly describe two incidents, or what we regard as ‘moments of interest’, which provide us with an opportunity to examine the similarities and differences between an existing part of the core financial services infrastructure and blockchain innovation and how their governance structure influenced the outcome of each of these instances.

1. **Governance crises in the blockchain economy**

***4.1 The DAO hack: challenging blockchain foundations***

Launched in April 2016, one of the most well-known smart contract “applications” built on Ethereum was “The DAO” – a distributed autonomous organization that was developed to act as a virtual venture capital fund, executing contracts in order to finance various projects and gain profits in return.[[25]](#footnote-25) The DAO gained attention and attracted investments of more than $160 million worth of ether (ETH).

In June 2016, a DAO token holder exploited a technical vulnerability in The DAO and siphoned 3.6 million ETH (approximately $60 million at that time) into a separate account. Following the exploit, the Ethereum community, with the support of its founder, Vitalik Buterin, decided to “unwind the theft” via a “hard fork” that would allow people to reclaim their ether funds. The proposed hard fork was heavily debated in the community. According to many, this was the “right thing to do” in order to maintain the *trust* of developers and investors, but it led to the controversial creation of a parallel Ethereum platform – a.k.a. Ethereum Classic – within which the siphoned funds still exist and are controlled by the attacker[[26]](#footnote-26).

 Although the incident was largely resolved as most miners adopted the ‘corrective’ software, the DAO incident has served as a provocation with the financial services blockchain community, raising concerns about the reliability of distributed ledger technology, the success of distributed autonomous organizations, and the governance of the entire system. Prior to the exploit, the mantra “code is law” was frequently evoked by key proponents of The DAO and assumed to lie at the core of the ideals underpinning it. Technically, The DAO ‘hack’ exploited a vulnerability but worked within the principle of “code is law” and the ‘flexibility’ that the software allowed. Despite this a different approach was taken to its resolution, ‘the hard fork’[[27]](#footnote-27), forcing people to come to terms with the implications of the hack for the good standing of this blockchain platform in the broader context of the financial sector. Many claimed that in trying to undo the damage done by the hack, some fundamental principles of the Ethereum platform were violated. What is the standing of immutability of transactions and tamper-resistance after the DAO hack?

 While smart contracts such as The DAO are a “next layer beyond the blockchain itself” (Werbach, 2018, p.25), they do raise questions regarding the governance procedures around testing, approving or certifying smart contracts on blockchain platforms (Birch & Parulava, 2018). Tiwana (2013) argue that some control mechanisms need to be in place in order to ensure housekeeping and a certain quality and security of applications (e.g. DApps) that have been externally developed and run on platforms such as Ethereum. In the blockchain universe this may be even more important as the network conducts value or rights to assets.

***4.2 “Fat-finger” moments and bugs***

 While cryptographic tamper resistance is an important feature of blockchain-based systems that makes them more trustworthy, it also leads to issues that software itself cannot disentangle. While guarding against sophisticated security attacks are usually the top priority, there are numerous occasions in the history of finance where ‘fat-finger’ typo incidents and basic computer mistakes cost investors many millions of dollars. In May 2017, a Canadian digital currency exchange (QuadrigaCX) reported that a computer error in a smart contract (when a contract failed to execute an upgrade) led to losses of $14.7 million as “a significant sum of ether [67,317.25 ETH] was effectively […] trapped”[[28]](#footnote-28) and thus no longer accessible. While the exchange offered a solution to recover the ether (similar to the DAO case above) no actions were taken by the Ethereum community and QuadrigaCX absorbed the cost of the incident ensuring no client balances were affected.

 In a similar situation, Parity – an Ethereum client company and one of the organizations that contributes significantly to the Ethereum blockchain codebase – revealed in November 2017 that in an attempt to fix a bug and repair a vulnerability in the system, a GitHub user (Devops1999) accidentally “killed” the “single-owned” wallet smart contract he had created in the process and froze around $300 million worth of ether (more than 500,000 ETH).[[29]](#footnote-29) While the freeze was a case of “bad luck” and “poor code” rather than malicious activity, it resulted in a much bigger loss than the DAO hack and immediately sparked a debate amongst the Ethereum community about whether to initiate another fork to retrieve the funds[[30]](#footnote-30). Shortly after, Parity proposed ways to deal not only with the current incident but also with all future cases where “the revival of suicided contracts”[[31]](#footnote-31) would need to be addressed. While acknowledging that hard forks are contentious and a definitive change to how participants previously expected the network to behave, they have tried to argue that these changes would be a functional enhancement to the platform. Their closing statement in the letter sums up the challenges the Ethereum community has had in order to agree on fundamental decisions and reflects upon the lack of a proper governance structure: “This next discussion will be an important test of how contention can be turned into consensus”.

In our final section, we discuss the challenges that the cases above pose to the governance of blockchain platforms and current financial infrastructures. We subsequently conclude by exploring the implications of the incidents described above for building the financial infrastructure of the future.

1. **Discussion and conclusions**

The purpose of this paper has been to provide a point of entry for practitioners and early stage scholars to gain a better understanding of the issues surrounding blockchain technology. Using the prior literature on information infrastructures and digital platforms we examined the issues that digitally-enabled organizational innovations pose for governance. We focused on the particular challenge posed by distributed governance: the balance of integrity and autonomy; decision-rights; control mechanisms; and incentive structures. It was notable that while the management literature emphasises the need for approaches capable of agile orchestration of resources across time and space, a surprising degree of centralization characterizes the governance of digital platforms. This motivates us to look more closely at the distributed nature of blockchain. Having described the difference between distributed databases, distributed ledgers and blockchains, we use illustrative examples of ‘when things go wrong’ to explore the critical issues of trust and governance that characterise use of blockchain technology for financial services.

While acknowledging the potential of distributed ledger technologies, we also believe that many questions are yet to be answered regarding DLTs ability to deal with some of the fundamental issues of concern such as scalability, openness, standards, liability, transparency, and security. The position that we take in this paper is that these critical issues will need to be continually addressed in order for blockchain to achieve widespread adoption in financial services. In Table 1 below, we summarise these issues and pose related further research questions.

**Table 1 – A summary of critical issues and the further research questions that they pose**

|  |  |  |
| --- | --- | --- |
| **Critical issues** | **Public blockchain platforms** | **Further research questions** |
| **Scalability** | Limited relative scalability in terms of transaction capacity.‘Permissionless’ ledgers have struggled to address scalability issues due to lack of consensus and governance structures. This may be due to varied interests and incentives of the different actors in their ecosystem but also due to lack of resources to meaningfully take part in the dialogue through proposals.“Infinite” scalability in terms of architecture and operational capability, albeit limited by its transactional protocol. | - How is scalability affecting the effectiveness of blockchain technologies in finance?- Can these issues be dealt with through better governance and control of blockchain infrastructures?- Who should be making these decisions and what would be the role of financial regulatory bodies?- Which governance framework would be more effective in encouraging consensus? |
| **Openness** | Public blockchains such as Ethereum and Bitcoin are inherently open.Anyone is able to access their networks by installing a wallet and purchase digital tokens from public exchanges (or other means). They are also open-source and accessible to anyone who was interested in participating in the development process.Issues around use of public blockchains for illicit activity. | - Does the inherent openness of public blockchains make them unfit to function as payment infrastructures?- How can KYC processes be utilised in this context?- What could be the role of financial institutions such as banks in the blockchain economy?- Can a digital identity framework be established to give legitimacy to transactions? |
| **Interoperability and standards** | Dependent upon voluntary Internet standards groups and proprietary standards initiatives.Coordination and collaboration required.Several consortia can lead to multiple standards and protocols.Further investment and tools for interoperability are required. | - How can the blockchain community bypass issues around the lack of interoperability between blockchain platforms?- What would be the role of standards in this process and who should develop these? |
| **Liability and resilience**  | Distinctive underlying technology with zero downtime relying on sophisticated consensus mechanism.Value never leaves.Issues of dark web use and ‘tainted coins’.Compensating record can be added (if permissions mechanisms allow).Dispute resolution options exist but resolution can be slow or effectively impossible. Operational risks are reduced and high levels of capital efficiency are achievable but other kinds of complexity enter the system. | - How can the resilience of blockchain platforms be leveraged to make financial transactions more efficient?- Is immutability a desirable property, and how can this be reversed in case of a fraudulent transaction (e.g. due to illegitimate access)?- How can platforms ensure consensus (and therefore continuous operation) when there is decreasing alignment of incentives? |
| **Transparency and privacy** | Ethereum and Bitcoin are pseudo-anonymous which means that real identities are not required to use either system (users are represented by particular alphanumerical addresses).The blockchain is publicly open and hence all transactions are visible which makes it easy to audit. However, there are many challenging cases where privacy is of major concern. | - How can transparency be leveraged when transactions are meant to be private?-Can a privacy balance be struck with blockchains? |
| **Security** | Response/coordination are voluntary and based on capacity from a community of users. Violating the principle of immutability opens the door to entirely new risks.Reputation and credibility. | - How should code “bugs” identified by security researchers be responsibly disclosed to public blockchain communities, particularly ones with billions of financial value at risk due to irresponsible bug disclosure[[32]](#footnote-32) |

In principle, public blockchain platforms such as Ethereum (or Bitcoin) and financial information infrastructures like the SWIFT network are offering some similar capabilities e.g. SWIFT describes itself as a “messaging platform […] facilitating global and local financial flows”[[33]](#footnote-33), while Ethereum claims that it is a “shared global infrastructure that can move value”.[[34]](#footnote-34) However, their approach in dealing with the core issues mentioned above is fundamentally different (Scott & Zachariadis, 2012, 2014). Perhaps the most fundamental difference is that SWIFT is a private, proprietary network infrastructure allowing access only to users who are fully identified and verified as legal entities in the finance sector and beyond. On the other hand, Ethereum is a distributed public blockchain network accessible to anyone who cares to download its digital wallet in order to trade and store ether (ETH). In doing so, users are not obliged to identify themselves in any way and can only be traced through their alphanumeric address, thus being pseudo-anonymous. In the case of SWIFT, trust derives from being an acknowledged member of a private, centralized network which is considered as secure and resilient, whereas, in the case of Ethereum or Bitcoin, trust is created by relying on the blockchain protocol which prevents any double-spending of the digital tokens and guarantees that the distributed ledger will not be amended in the future, thus not allowing to reverse any of the transactions on record (a.k.a. trust minimized network).

In line with their autonomous and decentralised operation, public blockchain platforms such as Ethereum are also governed on a distributed basis which can often create issues due to the “lack of a central legal entity with formal responsibility over the system” (Lehdonvirta & Robleh, 2016). The risks from such a governance scheme can be further exacerbated during times of crisis and as the developers of the system try to agree on software code alterations to deal with the issue. As it became apparent from the DAO incident, while the Ethereum blockchain platform is considered very secure due to the use of cryptographic elements and the fact that there is arguably no central point of failure, this does not always apply to the smart contracts that run on the platform. Smart contract code is “only as good as the people who write them” and “if a mistake in the code gets exploited, there is no efficient way in which an attack or exploitation can be stopped” (Blockgeeks, 2017) other than violating the platform’s principle of immutability and rewriting the underlying code by obtaining a network consensus. Describing the DAO incident, Leising (2017) writes that “it played out in front of anyone who cared to watch and couldn’t be stopped.” This kind of inflexibility deriving from the Ethereum governance structure and the “ruling via technical code” principle (Lehdonvirta & Robleh, 2016), puts a strain on the system that potentially impacts the security of the infrastructure. Our conclusion is that the in-principle efficiencies that could be achieved in processing smart contracts have yet to be realised in a way that would give regulated bodies in financial services the confidence to adopt DLT wholesale across their business.

Blockchain is currently defined as a “foundational technology” (Iansiti & Lakhani 2017). For the present, in more established financial services, blockchain innovations are more likely to be a complementary technology or an additional ‘rail’ upon which data and value travels across different parts of the financial system. The suggestion that it will completely replace the current core payment systems or bypass certain kinds of financial intermediaries are premature. If this does happen, there is a complex array of interdependencies of all kinds to be addressed including issues around governance which can have a decisive effect on all aspects of value transfer systems such as the ones we discussed above. Although distributed ledger technology may not wholly replace payment systems or messaging systems used by banks in the short run, payment systems “will connect to the blockchain, augmenting existing business networks and provide increased discoverability and trust” (Finextra, 2016 p.4).

A final observation is that our financial infrastructures are entangled in critical political dynamics, and this suggests the importance and need for boundary-crossing research. For example, the regulator mandated imposition of sanctions against Iran highlighted the possibility of cutting off a nation state from the world’s core financial telecommunication and payment messaging platform. Furthermore, recent calls for regulators to impose similar access restrictions on other countries, (Russia, Myanmar, and others) suggest that financial systems can and are being used politically. During the Iranian sanctions, the level of financial activity between Iran and China increased exponentially as alternate sources of relief and/or investment were sought and found. This suggests that developments altering both access and terms of use for financial services will prove potentially critical to political order. Future research is urgently needed to raise public awareness and broader understanding of these geopolitical risks which are intensifying in our digital economy.

**Acknowledgements**

We would like to thank participants at the inaugural *Research Impact and Contributions to Knowledge (RICK) Workshop* at Cambridge Digital Innovation at Hughes Hall and CJBS, University of Cambridge (June 2017) for their constructive feedback. We would also like to thank our anonymous reviewer(s) for their comments and suggestions in developing this paper further. Our appreciation to the RICK Section Editor, Prof. Michael Barrett of Cambridge Judge Business School, University of Cambridge and *Information & Organization* Editor-in-Chief, Prof. Elizabeth Davidson of Information Technology Management, University of Hawaii at Mãnoa for their continued support and encouragement to see this paper through. Finally, a major thanks to all our industry contacts and practitioners who challenged our thinking and made this paper more relevant to practice.

**References**

Akerlof, George A. (1970). The Market for 'Lemons': Quality Uncertainty and the Market Mechanism. *Quarterly* *Journal of Economics* 84 (3): 488–500.

Azouvi, S., Maller, M., and Meiklejohn, S. (2018). Egalitarian Society or Benevolent Dictatorship: The State of Cryptocurrency Governance. *University College London Working Paper*.

Bakker, R. M. (2010). Taking stock of temporary organizational forms: A systematic review and research agenda. *International Journal of Management Reviews*, 12(4), 466-486.

Baldwin, C., and Woodard, J. 2009. The Architecture of Platforms: A Unified View. in: Platforms, Markets and Innovation, A. Gawer (ed.), Edward Elgar, Cheltenham, UK, 19-44.

Benzell SG, Lagarda G, Van Alstyne M. 2017. The Impact of APIs on Firm Performance. Working Paper February.

Birch, D. and Parulava, S. (2018) Ambient Accountability: Shared Ledger Technology and Radical Transparency for Next Generation Digital Financial Services. (chapter 17, pp. 375-387). In *Handbook of Blockchain, Digital Finance, and Inclusion, Volume 1.* Edited by Chuen, David Lee Kuo and Deng, Robert. Elsevier.

Boudreau K., Hagiu A. (2009) Platform rules: Multi-sided platforms as regulators. Gawer A, ed. *Platforms, Markets and Innovation* (Edward Elgar, Cheltenham, UK), 163–191.
Cheffins, Brian R. (2013) The History of Corporate Governance, in The Oxford Handbook of Corporate Governance; Mike Wright et al. eds., Oxford University Press.

Coase, R.H. (1937) "The Nature of the Firm." *Economica* 4(16): 386­405.

Constantinides, P. and Barrett, M. (2015) Information Infrastructure Development and Governance as Collective Action. *Information Systems Research* Vol. 26, No. 1, pp. 40–56.

Davidson, S., De Filippi, P. and Potts, J. (2018). Blockchains and the economic institutions of capitalism. *Journal of Institutional Economics,* Volume 14, Issue 4, pp. 639-658.

Edelman, Benjamin (2014) Mastering the Intermediaries. Harvard Business Review, Issue (June).

Finextra White Paper (produced in association with IBM). Banking on Blockchain: Charting the Progress of distributed ledger technology in financial services. January 2016.

Gawer, A. 2009. Platforms, Markets and Innovation. Edward Elgar, Cheltenham, UK.

Gendal-Brown, R. (2017) On Distributed Databases and Distributed Ledgers. <https://gendal.me/2016/11/08/on-distributed-databases-and-distributed-ledgers/>.

Hanseth, O. and Lyytinen, K. (2004). "Theorizing about the Design of Information Infrastructures: Design Kernel Theories and Principles," Case Western Reserve University, USA . *Sprouts: Working Papers on Information Systems*, 4(12).

Hart, O., Moore, J. (1990). "Property Rights and the Nature of the Firm". *Journal of Political Economy* 98: 1119–58.

Henderson, J.C and N. Venkatraman (1993) “Strategic alignment: Leveraging information technology for transforming organizations”, *IBM Systems Journal* (32)1, pp. 472-485.

Hileman, G. and Rauchs, M. (2017) Global Blockchain Benchmarking Study (2017). Available at SSRN:

[https://ssrn.com/abstract=3040224](https://ssrn.com/abstract%3D3040224).

Iansiti, M., & Lakhani, K. R. (2017). The Truth about Blockchain. *Harvard Business Review*, *95*(1), 119-127.

Ito, J., Narula, N., and Ali, R. (2017) The Blockchain Will Do to the Financial System What the Internet Did to Media. *Harvard Business Review*, 8th March.

Kaniadakis, A. and Constantinides, P. (2014) Innovating Financial Information Infrastructures: The Transition of Legacy Assets to the Securitization Market. *Journal of the Association for Information Systems* Vol. 15, Special Issue, pp. 244-262.

Lehdonvirta, V. and Robleh, A. (2016) "Governance and Regulation" In: Distributed Ledger Technology: Beyond Blockchain. London: UK Government Office for Science.

Leising, M. (2017) “The Ether Thief” <https://www.bloomberg.com/features/2017-the-ether-thief/>.

Loh, L. and N. Venkatraman (1992) “Diffusion of Information Technology Outsourcing: Influence Sources and the Kodak Effect, *Information Systems Research* 3(4), pp. 334-359.

MacIver, Kenny (2016) “From the internet of information to the internet of value” <http://www.i-cio.com/big-thinkers/don-tapscott/item/from-the-internet-of-information-to-the-internet-of-value>.

March, J.G. (1995). The future, disposable organizations and the rigidities of imagination. *Organization*, 2, pp. 427–440.

Metz, C. (2015) The bitcoin schism shows the genius of open source. Wired, August 19.
McKinsey (2015) Toward an internet of value: An interview with Chris Larsen, CEO of Ripple Labs. *McKinsey on Payments*, 8(21) pp.19-22.

Munger M. 2015. Coase and the ‘Sharing Economy,’ (chapter 9, pp. 187-208). In Forever Contemporary: The Economics of Ronald Coase. Edited by Cento Veljanovski. London: Institute for Economic Affairs.

Murck, P. (2017). Who Owns the Blockchain. *Harvard Business Review*. April 19.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. <https://bitcoin.org/bitcoin.pdf>.

Nambisan, S. and Sawhney, M. (2017). Orchestration Processes in Network-Centric Innovation: Evidence From the Field. *Academy of Management Perspectives* Vol. 25, No. 3.

Parker GG and Van Alstyne MW (2017). Innovation, openness, and platform control. *Management Science* Vol. 64, No. 7.

Reyes, CL, Geslevich-Packing, N, and Edwards, BP. (2017) Distributed Governance. *William & Mary Law Review Online*. Vol 59:001.
Rochet JC, Tirole J (2003) Platform competition in two-sided market. *Journal of European Economic Association* 1(4):990–1029.
Rochet JC, Tirole J. (2006). Two‐sided markets: a progress report. *The RAND Journal of Economics* 37(3): 645-667.

Sahay S, Monteiro E, Aanestad M (2009) Configurable politics and asymmetric integration: Health e-infrastructures in India. *Journal of the Association of Information Systems* 10(5):399–414.

Saito, Kenji; Yamada, Hiroyuki (2016). What's So Different about Blockchain? Blockchain is a Probabilistic State Machine. Published in: 2016 IEEE 36th International Conference on Distributed Computing Systems Workshops (ICDCSW), June.
Scott, S.V. and Zachariadis, M. (2012) Origins and development of SWIFT, 1973–2009. *Business History*, 54 (3). pp. 462-482.
Scott, S.V. and Zachariadis, M. (2014) *The Society for Worldwide Interbank Financial Telecommunication (SWIFT): Cooperative Governance for Network Innovation, Standards, and Community*. London: Routledge.

Shermin, V. (2017) Disrupting Governance with Blockchains and Smart Contracts. *Strategic Change* (26:5), pp 499-509.
Skinner, C. (2016) ValueWeb: How fintech firms are using mobile and blockchain technologies to create the Internet of Value. Marshall Cavendish Business: Singapore.
Sydow, J., Lindkvist, L. and DeFillippi, R. (2004). Project- based organizations, embeddedness and repositories of knowledge: editorial. Organization Studies, 25, pp. 1475– 1489.

Tiwana A (2013) *Platform Ecosystems*: *Aligning Architecture, Governance, and Strategy* (Morgan Kaufmann, San Francisco).
Tiwana A, Konsynski B, Bush AA (2010) Research commentary— Platform evolution: Coevolution of platform architecture, gov- ernance, and environmental dynamics. *Inform. Systems Res.* 21(4):675–687.

Walch, A. (2015). The bitcoin blockchain as financial market infrastructure: A consideration of operational risk. *New York University Journal of Legislation & Public Policy* Vol. 18, Issue 4.
Werbach, Kevin (2018) Trust, But Verify: Why the Blockchain Needs the Law. *Berkeley Technology Law Journal*, forthcoming.
Wareham J, Fox PB, Giner JLC (2014) Technology ecosystem governance. Organ. Sci. 25(4):1195–1215.
Weill, P. (2004). Don’t just lead, govern: How top-performing firms govern IT. MIS Quarterly Executive, 3(1), 1-17.
Weill, P. and Ross, J. (2004) *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*, Harvard Business School Press, Boston.
Williamson, O. (1975) Markets and Hierarchies, Free Press.
Williamson, O. (1979) “Transaction-Cost Economics: The Governance of Contractual Relations." *Journal of Law and Economics* 22 (October): 233-261.

Zachariadis, M. and Ozcan, P. (2017) The API Economy and Digital Transformation in Financial Services: The Case of Open Banking. *SWIFT Institute Working Paper* No. 2016-001. Available at SSRN: [https://ssrn.com/abstract=2975199](https://ssrn.com/abstract%3D2975199).

1. \* Corresponding author. Email: markos.zachariadis@wbs.ac.uk

 See for example Walport, M. "Distributed Ledger Technology: Beyond Blockchain." *UK Government Office for Science* (2016) and Tapscott, Don, and Alex Tapscott. *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. Penguinm (2016). [↑](#footnote-ref-1)
2. For example, see: “Bitcoin and Blockchain seem more like solutions looking for a problem” (<https://qz.com/844507/bitcoin-and-blockchain-seem-more-and-more-like-solutions-looking-for-a-problem/>), “Is Blockchain looking for a problem to solve?” (<https://www.temenos.com/en/market-insight/2016/is-blockchain-looking-for-a-problem-to-solve/>), and “Blockchain: a solution looking for a problem” (<http://www.risk.net/cutting-edge/views/2472176/blockchain-solution-looking-problem>). [↑](#footnote-ref-2)
3. Extract from an interview conducted by Rik Kirkland, the senior managing editor of McKinsey Publishing with Don Tapscott, CEO of the Tapscott and co-author of the *Blockchain Revolution*. [↑](#footnote-ref-3)
4. The Internet Engineering Task Force (IETF) is an open international community of network engineers, telecommunication operators, technology vendors and researchers who study the evolving internet architecture and are concerned with the smooth operation with the internet. IETF operates more than 100 active Working Groups which do technical work and produce various recommendations, standards specifications (a.k.a. Internet Standards), and ongoing improvements of existing protocols depending on their area of focus (e.g., routing, transport, security, etc.). The community uses formal email lists and online tools as well as meetings and events to coordinate action and achieve its objectives. The task force plays an instrumental role in achieving consensus and maintains the unofficial motto: “We believe in rough consensus and running code” (<https://www.ietf.org/how/runningcode/>). In their *IETF Working Group Guidelines and Procedures* (RFC 2418, 1998; <https://tools.ietf.org/html/rfc2418>) they outline how the “rough consensus” process works in action as part of the Working Groups activities: “consensus does not require that all participants agree […] 51% of the working group does not qualify as "rough consensus" and 99% is better than rough. It is up to the Chair to determine if rough consensus has been reached”. [↑](#footnote-ref-4)
5. The Internet Governance Forum (IGF) was established by the United Nations and formally launched in 2006 when the first meeting was also convened. It’s a “forum for multi-stakeholder dialogue on public policy issues related to key elements of Internet governance issues, such as the Internet's sustainability, robustness, security, stability and development.” (<https://www.intgovforum.org/multilingual/content/about-igf-faqs>). [↑](#footnote-ref-5)
6. The World Wide Web Consortium (W3C) is an international community founded by directed by Sir Tim Berners-Lee with the mission to “lead the World Wide Web to its full potential by developing protocols and guidelines that ensure the long-term growth of the Web” (<https://www.w3.org/>). As of June 2018, W3C has 476 members, mainly international organisations from all industries but also universities, national authorities, etc. [↑](#footnote-ref-6)
7. The Internet Corporation for Assigned Names and Numbers (ICANN) is a not-for-profit, private-public partnership corporation responsible for the delegation of Top-Level Domain names and Internet Protocol (IP) address space allocation (<https://www.icann.org/>). [↑](#footnote-ref-7)
8. Platforms can be either proprietary (single firm owning the entire infrastructure) or have shared ownership amongst several actors each having a different stake. This can influence platform evolution significantly, however, in some contexts the *openness* of the platform, e.g. how open is its architecture or whether it is open-source or not, may be more important properties (Tiwana et al., 2010; Gawer, 2009). [↑](#footnote-ref-8)
9. https://queue.acm.org/detail.cfm?id=3136559 [↑](#footnote-ref-9)
10. https://queue.acm.org/detail.cfm?id=3136559 [↑](#footnote-ref-10)
11. The term ‘blockchain’ does not appear in Nakamoto’s 2008 paper (Nakamoto instead refers to a “proof-of-work chain”, or uses other terms), and it is unclear who originally coined the term. [↑](#footnote-ref-11)
12. In some consensus mechanisms the verification of transactions is done by “miners” who compete between them to solve a cryptographic puzzle by committing costly resources (such as computing power) to the network. [↑](#footnote-ref-12)
13. https://www.r3.com/about/ [↑](#footnote-ref-13)
14. <https://bitnodes.21.co> accessed on 21 Sept. 2017 - 9,487 and 93 countries. [↑](#footnote-ref-14)
15. https://blockstream.com/2017/08/15/announcing-blockstream-satellite.html [↑](#footnote-ref-15)
16. Wenger, A. (2014) “Bitcoin: Clarifying the Foundational Innovation of the Blockchain, Continuations”, accessed at http://continuations.com/post/105272022635/bitcoin- clarifying-the-foundational-innovation-of. [↑](#footnote-ref-16)
17. For more details on the newer developments around the Bitcoin voluntary signalling mechanism called BIP 9 and more recent blockchain platform initiatives that deal with the issue of on-chain governance, see Werbach (2018). [↑](#footnote-ref-17)
18. Alyssa Hertig, “Major Blockchains Are Pretty Much Still Centralized”, accessed: <https://www.coindesk.com/major-blockchains-pretty-much-still-centralized-research-finds/>. [↑](#footnote-ref-18)
19. Talk by Vitalik Buterin on “Governance for Public Blockchains and DAOs” at Silicon Valley Ethereum Meetup, 2016. [↑](#footnote-ref-19)
20. Rachel Rose O’Leary, “Experimental Voting Effort Aims to Break Ethereum Governance Gridlock”, accessed: <https://www.coindesk.com/experimental-voting-effort-aims-break-ethereum-governance-gridlock/>. [↑](#footnote-ref-20)
21. Only an attacker who possesses a sufficient share of the total computing power of the whole network can compromise the ledger and replace or add to the blockchain fraudulent blocks. This attack is known as a “51-percent attack” as controlling greater than 50% of the computing network power ensures a successful attack can be performed, although it is still possible to perform a successful attack with less than 50% of the network’s computing power. [↑](#footnote-ref-21)
22. In his position paper, Nakamoto (2008) highlights quite intensely his objections towards the established financial institutions and the need to create a *trusted* decentralized environment that will disintermediate banks and allow people to transact on a peer-to-peer basis. [↑](#footnote-ref-22)
23. Ethereum White Paper: “A Next-Generation Smart Contract and Decentralized Application Platform”, accessed here: <https://github.com/ethereum/wiki/wiki/White-Paper#philosophy>. [↑](#footnote-ref-23)
24. http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html [↑](#footnote-ref-24)
25. DAO projects would be voted on before they were funded, with voting share based on each individual’s respective capital contribution share to The DAO. [↑](#footnote-ref-25)
26. As the DAO attacker is legitimately recognized by the Ethereum Classic community, and the ETC value has significantly climbed since the hard fork, the funds the attacker controls (3.6 million ETC) worth approximately $67.4 million. This varies according to the exchange rate for ETC in the various digital currency exchanges. The figure mentioned here is based on the ETC rate on June 2017, which was $18.71. [↑](#footnote-ref-26)
27. In the context of a blockchain platform, a “hard fork” is described as a radical change to the protocol/source code, or an “update of the software” that results into a separate branch from the original blockchain (essentially a new blockchain infrastructure) that is both backward and forward incompatible to the original. Following such split, the dominant infrastructure is considered the version of the code that is being used by the majority of users. [↑](#footnote-ref-27)
28. For a technical explanation and more details see QuadrigaCX’s announcement: <https://www.reddit.com/r/ethereum/comments/6ettq5/statement_on_quadrigacx_ether_contract_error/>. [↑](#footnote-ref-28)
29. <https://www.theguardian.com/technology/2017/nov/08/cryptocurrency-300m-dollars-stolen-bug-ether>. [↑](#footnote-ref-29)
30. See <https://www.ethnews.com/parity-proposes-hard-fork-to-unfreeze-funds> for a more detailed discussion. [↑](#footnote-ref-30)
31. See Parity Technologies statement here: <https://paritytech.io/on-classes-of-stuck-ether-and-potential-solutions/>. [↑](#footnote-ref-31)
32. See Narula, N. keynote lecture at Financial Cryptography and Data Security 2019, https://fc19.ifca.ai/program.html [↑](#footnote-ref-32)
33. <https://www.swift.com/about-us/discover-swift> [↑](#footnote-ref-33)
34. <https://www.ethereum.org/> [↑](#footnote-ref-34)