Chapter 2
Blockchain Governance: De Facto (x)or Designed?

Darra Hofman, Quinn DuPont, Angela Walch, and Ivan Beschastnikh

2.1 Introduction: De Facto Governance in Blockchains

> [B]lockchain technology is being lauded as transformative for every human practice that uses recordkeeping (so, all of them). [. . .] if blockchain technology ends up enabling our most fundamental social infrastructures, then the governance processes for creating, maintaining, and altering the technology deserve careful scrutiny, as they will affect the resilience of the technology, as well as any infrastructure that comes to rely on it. (Walch 2019a, p. 59)

Examining the governance of blockchain technologies is critical but challenging. As Quinn DuPont (2019, p. 197) writes, "Governance is the buzzword in blockchains today [. . .] However, governance is notoriously difficult to define

(x)or, also known as "exclusive or" is a logical operation that outputs "true" only when inputs differ (one is true, the other is false); (x)or emphasizes mutual exclusiveness in the sense of "A or B, but not A and B." In the case at hand, there will be governance of the blockchain—if not designed, then de facto.

D. Hofman (✉)
School of Information, University of British Columbia, Vancouver, BC, Canada
e-mail: dhofman@mail.ubc.ca

Q. DuPont
School of Business, University College Dublin, Dublin, Ireland
e-mail: quinn.dupont@ucd.ie

A. Walch
School of Law, St. Mary's University, San Antonio, TX, USA

University College London, London, UK
e-mail: awalch@stmarytx.edu

I. Beschastnikh
Department of Computer Science, University of British Columbia, Vancouver, BC, Canada
e-mail: bestchai@cs.ubc.ca

V. L. Lemieux, C. Feng (eds.), *Building Decentralized Trust*,
https://doi.org/10.1007/978-3-030-54414-0_2

let alone operationalize. A definition for governance might be: stewardship, a mechanism that sets institutional rules and incentives, or the strategic exercise of power".

Governance, as traditionally understood, initially received little attention in the world of blockchain, at least outside of the technical dimensions of blockchain systems and their incentives. This occurred, in part, because of quintessential beliefs about blockchain technologies, at least in the public, permissionless form that has most captured the public imagination, such as Bitcoin and Ethereum. For example, an exclusive focus on the protocols bred a belief that blockchains are apolitical—"beyond the scope of governments, politics, and central banks" (De Filippi and Loveluck 2016, p. 1)—and that "algorithms are more trustworthy and authoritative than existing institutions," (Lustig and Nardi 2015, p. 747), a technocratic approach that "tries to solve issues of social coordination and economic exchange by relying, only and exclusively, on technological means" (De Filippi and Loveluck 2016, p. 1).

In other cases, such as "The Decentralized Autonomous Organization" (DAO), there was deliberate experimentation, an attempt to "create a social and political world quite unlike anything we have seen before" (DuPont 2018, p. 157). In most cases, however, early discussion about blockchain governance focused primarily on the technical aspects of the systems.

2.2 The Case for a Grounded Theory of Blockchain Governance

Given this context, there is relatively little literature on the prescriptive governance of blockchain platforms.[1] Consider, for example, the questions grounding Beck et al.'s blockchain governance framework: it becomes clear that very basic questions of governance ("How are decisions made?") remain open in the blockchain space (2018). However, while Beck et al.'s agenda is helpful, it is grounded in and informed by a theoretical framework of IT governance, which understands governance through decision rights, accountability, and incentives, and relies on agency theory.

Beck et al.'s work is certainly not the only lens through which to understand blockchain governance. De Filippi and Loveluck draw upon internet governance, by which they understand the internet as "a complex and heterogenous socio-technical construct [that] combines many different types of arrangement—involving social norms, legal rule and procedures, market practices and technological solutions—which, taken together, constitute its overall governance and power structures" (2016, p. 24). Walch (2019a) examines "decentralization" and the governance of blockchains through the lens of fiduciary law and the legal scholarship thereof,

[1] Some examples of work that discuss blockchain governance prescriptively include DuPont (2019) and Hofman et al. (2019).

while Hofman et al. (2019) discuss blockchain systems and the European Union's General Data Protection Regulation through the lens of information governance, informed largely by the lens of archival science. Not one of these approaches speaks to the totality of governance; each author takes a different approach to serve a different purpose.

Even though this literature attempts to situate blockchain governance within broader, mostly disciplinary, governance frameworks, the majority of existing literature on blockchain governance is descriptive and atheoretical, having largely arisen out of real-world crises of governance. The DAO hack of 2016 led to extensive analysis of governance challenges, in part because DAOs—decentralized autonomous organizations—are experiments in an entirely novel form of human governance (DuPont 2019; Walch 2019a). Seemingly prosaic or purely technical matters, however, have also led to crises of governance. De Filippi and Loveluck, in their examination of Bitcoin XT and the subsequent controversy over block size, note that "[t]o many outside observers, the contentious issue may seem surprisingly specific [. . ., but it] eventually led to a full-blown conflict which has been described as a 'civil war' within the Bitcoin community" (2016, p. 11). Ultimately, these crises have encouraged communities to find resolution not through code, but through social negotiation, or, in the case of "hard forks," the creation of new communities.

What has become clear from these crises is that while blockchains may permit experimentation with new forms of governance, they are not beyond or outside governance. After all, "[governance in] its purest form [. . .] describes the structures and decision-making processes that allow a state, organization or group of people to conduct affairs" (Bruce-Lockhart 2016). Even if it were possible[2] to set up a completely autonomous system of algorithmic authority in which all governance and management were executed on-chain, the structures and decision-making processes themselves would have to be agreed upon, created, and instantiated. Furthermore, this seemingly "autonomous" organization would still have to interact with the broader world. As De Filippi and Loveluck observe, "one cannot get rid of politics through technology alone, because the governance of a technology is—itself—inherently tied to a wide range of power dynamics" (2016, p. 16). For this reason, it may make more sense to adopt a grounded approach to development of governance theory for blockchains, rather than attempting to apply existing theories of governance to these novel contexts. Such a theory would take into consideration the social, institutional, and political contexts of blockchains, where these contexts are considered an essential part of understanding blockchain governance.

[2]It's not.

2.3 Situating Blockchain Governance in Existing Power Structures

> Decentralization inherently affects political structures by removing a control point [. . .] as Bitcoin evolves—and in the eventuality that it gets more broadly adopted—it will [. . .] encounter a variety of social and political challenges—as the technology will continue to impinge upon existing social and governmental institutions, ushering in an increasingly divergent mix of political positions. (De Filippi and Loveluck 2016, p. 15)

Blockchain protocols take their action within the existing world of material constraints, institutions, cultures and norms, and above all, existing sovereign governance systems. Decisions about the governance of any given blockchain system will impact and be impacted upon by these existing power structures: actions taken by participants within blockchain systems that violate nation state laws will be subject to state-based consequences. On the other hand, participants within blockchain systems continue to avail themselves of remedies offered by state actors (e.g., bankruptcy, fraud claims).

A substantial amount of rhetoric around blockchain technologies focuses on "decentralization" and "trustlessness." By enabling decentralized transactions and decision making and reducing or even eliminating the need to depend on humans, blockchains—or so the argument goes—will revolutionize how people interact, conduct business, and even govern themselves. Indeed, De Filippi and Loveluck describe the "implicit political project" of Bitcoin as "getting rid of politics by relying on technology" (2016, p. 22). In reality, however, blockchain technologies are complex sociotechnical systems, or as we argue in this volume, socio-informational-technical systems. "Decentralization" and "trustlessness" are both fraught terms that capture technical and social discourses and their interrelationships—a *promotion* of a kind of reality as much as a *description* of it.

As Walch explains:

> the term 'decentralized' is generally being used to describe how power operates in blockchain systems—suggesting that power exercised by people in these systems is diffuse rather than concentrated. This is critically important, as our understanding of how power is exercised within these systems will shape conclusions about how responsibility, accountability, and risk should work for them (2019b, p. 40)

Walch traces two major uses of "decentralization" in the discourse surrounding blockchain technologies, which are often conflated with one another: decentralization as a description of the network architecture which supports the blockchain, and decentralization as a description of "how power or agency works within permissionless blockchain systems" (2019b, p. 42). De Filippi and Loveluck similarly distinguish "between two distinct coordination mechanisms: governance *by* the infrastructure (achieved via the Bitcoin protocol) and governance *of* the infrastructure (managed by the community of developers and other stakeholders) (2016, p. 1). Even in Beck et al.'s study of Swarm City—a case study in which the interviewed developers have an explicit, ideologically-driven goal of making their code "increasingly decentralized and autonomous once it is implemented"—the developers

nonetheless admit that "in order to make the tools, we initially need a really hierarchical governance," which they term a necessary "benevolent dictatorship" (2018, p. 1029). Technical decentralization can belie substantial centralization in how a system is actually designed and run, with tremendous decision-making power invested into the social structures surrounding the design, implementation, and operation of the system.

"Trustlessness" fares little better. Despite the fact that many of their participants used Bitcoin as "an act of resistance against institutions they felt had failed them" (Lustig and Nardi 2015, p. 762), Lustig and Nardi uncovered significant ways that participants relied on human judgement and trust. For example, they found that many of the individuals they interviewed spent 2–3 h per day trying to get informed about Bitcoin in order to learn "who to trust, how to protect their bitcoins from theft or fraud, and what community interventions were necessary to help Bitcoin itself run smoothly" (Lustig and Nardi 2015, p. 762). Similarly, DuPont found that, when The DAO's vision for novel governance broke down, people turned to "traditional models of sociality—using existing strong ties to negotiate and influence, argue and disagree" (2018, p. 2). Ultimately, De Filippi and Loveluck argue that, "although the *trustlessness* of the [Bitcoin] network seeks to obviate the need for a central control point, in practice, as soon as a technology is deployed, new issues emerge from unanticipated uses of technology—which ultimately require the setting up of social institutions in order to protect or regulate the technology" (2016, p. 25). Even "trustless" technologies, then, are connected to, protected and/or regulated by, and impact on social institutions of various degrees of trustworthiness.

"Decentralization" and "trustlessness," then, are not sufficient to exempt blockchains from governance, both internally (within the code) and externally (beyond the code). What that governance will look like, how blockchain governance will differ from other infrastructures, and how it will emerge, remains unknown. As Beck et al. note, "how exactly governance will change in the emerging blockchain economy is still little understood. Nevertheless, the promise of the blockchain economy is dependent on the implementation of effective governance mechanisms, which are, in turn, dependent on a thorough understanding of the phenomenon" (2018, p. 1029). Their study on IT governance, identifies a number of open questions for governance in what they term the "blockchain economy" (see Fig. 2.1).

2.4 Blockchain Governance Analysis Framework

> [G]overnance is [. . .] strategic and visionary. Governance involves the assessment of multiple options, limitations, and opportunities (DuPont 2019, p. 23)

Given the great variety of blockchain technologies, the myriad purposes to which those blockchains might be put, and the limitations of existing theoretical perspectives on blockchain governance, we take a step back and pose the following question as a guide: what ought to be a *theory* of blockchain governance, specifically, one that

Dimension	Research questions
Decision rights	• How are decisions made in the blockchain economy? • How are decision management rights and decision control rights allocated? • How is disagreement about decision-making resolved in the blockchain economy? • What is the role of ownership in the blockchain economy?
Accountability	• How is accountability determined in the blockchain economy? • How is identity engrained in the blockchain economy? • How is transaction enforcement embedded in the blockchain economy? • How are disputed transactions resolved in the blockchain economy? • How is trust affected by the blockchain economy? • What is the role of institutions in the blockchain economy?
Incentives	• How is consensus incentivized in the blockchain economy? • How does incentive alignment work in the blockchain economy? • How is system use incentivized in the blockchain economy? • How is system development and maintenance incentivized in the blockchain economy? • How do business models shape the blockchain economy?

Fig. 2.1 Research agenda for governance in the blockchain economy (Beck et al. 2018, p. 1029)

is endogenous to the socio-political, economic, cultural, informational and technical realities that define crypto? This is not a question of "what is or ought to be governance" but rather, what would or should a meaningful theory of crypto governance be, where "meaningful" means a theory that is analytically descriptive and prescriptive. Our framework is meant to enable descriptive or prescriptive analyses of blockchain platforms, acknowledging that, "there is no one right approach to [blockchain] governance [. . .] there are risks and opportunities for each" (DuPont 2019, p. 198).

Our framework, shown in Fig. 2.2, tries to capture the embeddedness of blockchain solutions in the broader world, noting that this is based on our review and understanding of the existing blockchain literature rather than a much needed rigorous grounded-theoretic analysis of blockchain governance.

We took the water cycle as an exemplar, where blockchain governance is a small part of much broader, more complex systems. Similar to the water cycle, blockchain governance exists within, is determined by, and ultimately determines the broader world in which it is embedded. The reciprocity in the framework—the "world" in our water cycle—captures the fact that blockchain systems do not exist separately from the broader world. "Even in a world with widespread use of blockchains, governments still retain their four regulatory levers—*laws, code, market forces, and social norms*—which could be used to either directly or indirectly regulate this new technology" (De Filippi and Wright 2018, p. 208). We add a much-needed fifth category—the environment—because environmental factors have a direct impact on our social and institutional systems broadly, and on all blockchain systems specifically.

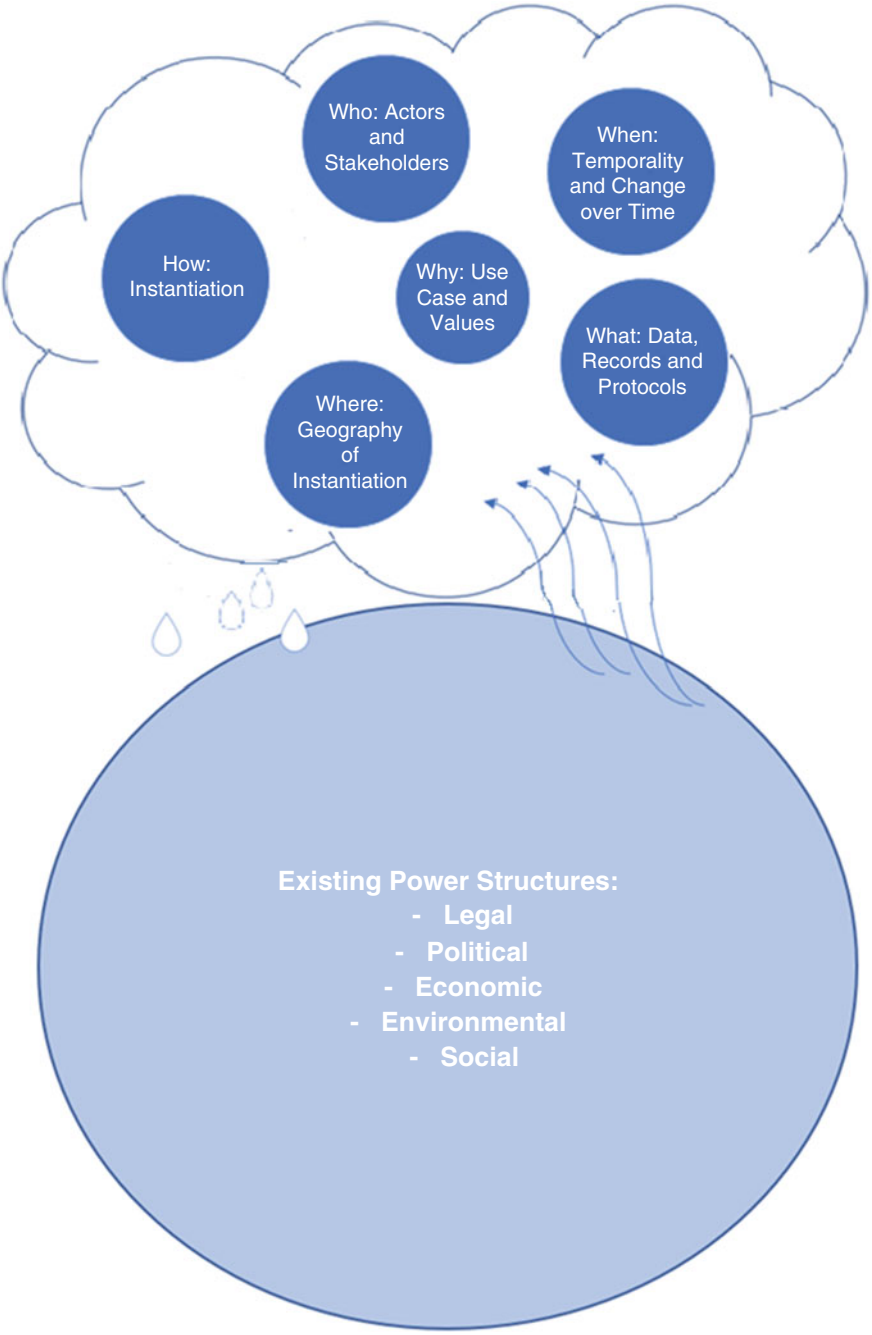

Fig. 2.2 Governance analysis framework

This framework is meant to serve as a high-level analytic tool; given the enormous variability in blockchain systems (including incommensurabilities such as values and norms), we propose an inclusive, question-led approach, which enables the examination of governance for any system without a priori prescribing technical goals or socio-economic realities.

2.4.1 Within the Cloud: Internal Governance

The "cloud" in our model represents governance modalities of the blockchain system itself. Governance of the blockchain system interacts with existing power structures in complex ways that co-determine each system's modalities. We imagine a homeostatic relationship between internal and external governance mechanisms. At the centre of the cloud—the origin of governance theory—is the question "why?" Governance choices flow from these exogenous values.

2.4.1.1 Why: Values and Use Cases

The initial question in our analysis framework is "why?" Establishing the "why" of the system—defining the use case, eliciting requirements and the values behind the design of the solution, and engaging in value-sensitive design—helps to ensure that governance decisions about the design/implementation of the system, and the resolution of conflicts once the system is deployed, support the ultimate purpose of the system. Analysis of purposes, goals, and values allows for the identification of conflicts between proposed use cases and implementation decisions.

Some questions to be asked at this phase include:

- What problem(s) should this system solve? What are the use-cases that the system intends to support, and the use-cases that it is not designed for?
- Why is a blockchain the chosen solution (or part of the solution)?
- What are the goals of this system? What social and technical guarantees does the system provide? (These may be security and privacy guarantees in the context of a specific threat model, or usability requirements that the software aims to provide.)
- What values are important in this system?

2.4.1.2 Who: Actors and Stakeholders

The next step is to identify actors and stakeholders and to identify their interests, rights, and obligations.

Some questions to ask at this stage include:

- Who are the actors and stakeholders (or better yet, "actants")? Identifying actors is often a practical challenge, especially when systems are designed to be privacy-preserving or purposefully obfuscate the actors. Some of the direct actors in a public blockchain system include developers, record producers, nodes, and the designers or creators of the system. As these systems integrate further into socio-economic infrastructures, this list and its complexity grows to include end users, public policy makers, and the broader ecosystem engaging with or building on the blockchain system.
- How are the actors in the system identified and how are their identities regulated? Public and private cryptographic keys, email addresses, names, and many other approaches may be used to identify and regulate participants. These design choices will constrain if and how actors may prove their identity, change or create new identities, leave the system, maintain anonymity, and so on.
- What expectations do we have of them? What actions will or might they take? How will these actions impact others?
- Will some actors act on behalf of others? On what (moral, legal?) ground do they implement the will of others? (Which others?)
- How is discretion exercised when conflict arises? When is consent, permission, and authority needed, granted, or assumed?
- What norms or other frameworks constrain the behavior of actors?
- What types of actions are forbidden, encouraged, or tolerated?
- What norms or other frameworks constrain the designers or creators of the systems?

Research and development norms and values deserve special mention here. In his study of research and development norms in the field, DuPont (2020) found that software developers are largely aware of formal guidelines but made little use of such guidelines: Perhaps most worrisome, DuPont found that researchers and developers have significant unacknowledged conflicts of interest, use risky research methods, and lack safe mechanisms for disclosure reporting. DuPont (2020) concluded that because these systems typically involve valuable tokens (for game-theoretical security models and decentralized funding structures), they comprise a new kind of per se value technology, with research and development governance challenges that rival bio- and nanotechnology.

Norms determine governance behaviours. For example, with developers, there may be norms determining that a developer will not try to thwart the system or that contributing to an open source software project is a virtuous act of contributing to the common good. Similarly, there may be norms around reputation—if a developer is seen to be trying to harm the system or seen to be incompetent, such behaviours will damage their reputation and future earnings. As such, these potential consequences may constrain governance options. The public nature of the software code also constrains a developer's behavior to some extent. Since code is subject to public scrutiny, bad/incompetent actions by developers will be revealed (assuming the veracity of "Linus's Law" that "given enough eyeballs, all bugs are shallow" (Raymond 1999)). Transparency of the code here is an "architectural" constraint

on developer behaviour. However, people may not be able to read code, and typically in practice, relatively few people actually review code even when it is open source. Also, sophisticated developers may be able to hide actions in platform or contract code (even when surreptitious code injection is for the acknowledged benefit of the system, as has happened in the past, this capability introduces governance questions). The social aspects of blockchain governance, then, can be as complex and nuanced as the technical aspects.

2.4.1.3 When: Temporality and Change Over Time

As noted *supra*, blockchain solutions change—both in function and through their relationship to broader structures of power. This iterative relationship is why we chose a homeostatic model of governance for this framework. Thus, in determining the governance of the blockchain, questions of temporality and change over time—the system's lifecycle—must be asked, such as:

- How will governance address actors' changing relationships to the system over time? Are all developers fungible? Must the system be able to differentiate between different classes of records producers and users, and in what ways?
- What known future changes will the system have to be able to respond to? For example, if there are legal or regulatory changes, how will the system and its actors—including "autonomous" components—respond? Likewise, how will other risk factors be addressed, including those that lie unknown in the future and that may present existential or systematic risk?
- Could future events bring about consequences where the platform ought to be destroyed? Lifecycle management affects all system components, including assets no longer under control.

2.4.1.4 What: Data, Records, and Protocols

Blockchains serve to store and/or help protect the integrity of data and/or records. In order to understand and/or establish the governance of a particular blockchain solution, it is necessary to understand what that system stores and how it provides the intended functionality. The technical realization of a blockchain will simultaneously impose demands and constraints on the governance structure. For example, if the data is arbitrary and is stored without revealing the origin of the data, then governance must concern itself with issues like copyright infringement and whether or not to establish structures that would impose constraints on the data allowed into the system.

Questions to ask at this stage include:

- What data and/or records must the system store? (What are the legal or regulatory obligations?)

- What data and/or records must not be stored in the system? (For purposes of privacy, financial risk management, or corporate policy.)
- Are there data and/or records that require special consideration? For example, are there data and/or records containing personally identifiable information that requires special treatment under law?
- Are there data and/or records that must not be kept indefinitely?

2.4.1.5 Where: Geography of Instantiation

While blockchain solutions are largely treated as borderless in the popular imagination, state actors continue to exercise territorial (and extraterritorial) jurisdiction, even in cyberspace. As just two examples, the great firewall of China determines what internet content is accessible to people who access the internet from Chinese territory (Griffiths 2019), and ISPs in the USA distinguish between internet traffic between end-points that are both in the USA versus traffic where one of the end-points is outside of the USA (Gallagher and Moltke 2018; Goldberg 2017).

Furthermore, depending on the use case, being able to demonstrate compliance with laws and regulations may be necessary. And, beyond law and regulation, there are economic, political, social, and environmental constraints that are specific to their geography; e.g., a Proof of Work consensus mechanism might be prohibitively expensive in an area with high electricity costs (or, alternatively, in a very hot area where significant cooling would be required).

Some questions to ask about where a solution is instantiated:

- Are there any reasons why this solution must be instantiated in a particular location? For example, data localization laws might require data to be held in a particular legal jurisdiction (which limits both the "where" and the "how" of the instantiation).
- Are there any reasons why this solution should *not* be instantiated in a particular location?
- Are there location-based strengths/weaknesses that encourage adoption of a private blockchain instead of the broadly-distributed public blockchains?
- Is there a differentiation in access or power granted to actors in the system based on their geographical locale? For example, diversity of location (of nodes, users, etc.) may be encouraged and even required in systems that aim to avoid becoming too geographically centralized.

2.4.1.6 How: Instantiation

Finally, after establishing all of the above, governance must address executable code (the technical layer). Data and records are instantiated, but so are implicit, social properties that affect communities of developers, records producers, and users.

Some questions to ask about the instantiation of the solution include:

- What kind of blockchain solution best meets the governance needs of the system? Public, private, permissioned, permissionless?
- What technical features increase governance capacity?
- What consensus mechanism best meets the needs of both the use case and the actors?
- How will buy-in of the necessary communities be made clear?

2.5 Conclusion

> When it comes to freedom and autonomy, the assumption that the rule of code is superior to the rule of law is a delicate one—and one that has yet to be tested. (De Filippi and Wright 2018, p. 207)

Given the extensive role that blockchain technologies—and new blockchain-enabled forms of organization and interactions, such as DAOs—could play in society, we must consider governance of, by, and through blockchains to ensure that we identify areas of risk and in turn understand how conflict and crisis can be handled. By adopting a meta-theoretical model of homeostatic interaction, anchored in the values of a given set of actors, our framework proposes opportunities for innovation in governance. With their incentive and prohibition mechanisms, decentralized architectures, and ontologies of per se value, blockchain systems provide opportunities for social experimentation (DuPont 2019). "Governance" might indeed be difficult to define and operationalize, but trying to do so, through a grounded and contextual approach, is a necessary step to ensure that blockchain solutions can meet their potential.

References

Beck, R., Müller-Bloch, C., & King, J. L. (2018). Governance in the blockchain economy: A framework and research agenda. *Journal of the Association for Information Systems, 19*(10), 1. https://aisel.aisnet.org/jais/vol19/iss10/1

Bruce-Lockhart, A. (2016). What do we mean by 'governance'? *World Economic Forum.* https://www.weforum.org/agenda/2016/02/what-is-governance-and-why-does-it-matter/

De Filippi, P., & Loveluck, B. (2016). The invisible politics of Bitcoin: Governance crisis of a decentralized infrastructure. *Internet Policy Review*, *5*(3). https://doi.org/10.14763/2016.3.427.

De Filippi, P., & Wright, A. (2018). *Blockchain and the law: The rule of code*. Cambridge, MA: Harvard University Press.

DuPont, Q. (2018). Experiments in algorithmic governance: A history and ethnography of "The DAO," a failed decentralized autonomous organization. In M. Campbell-Verduyn (Ed.), *Bitcoin and beyond* (pp. 157–177). New York: Routledge.

DuPont, Q. (2019). *Cryptocurrencies and blockchains*. Cambridge: Polity Press.

DuPont, Q. (2020). Guiding principles for ethical cryptocurrency, blockchain, and DLT research. *Cryptoeconomic Systems Journal*.

Gallagher, R., & Moltke, H. (2018). The wiretap rooms: The NSA's hidden spy hubs in eight U.S. cities. *The Intercept*. https://theintercept.com/2018/06/25/att-internet-nsa-spy-hubs/

Goldberg, S. (2017). Surveillance without borders: The "traffic shaping" loophole and why it matters. *The Century Foundation*. https://tcf.org/content/report/surveillance-without-borders-the-traffic-shaping-loophole-and-why-it-matters/

Griffiths, J. (2019). *The great firewall of China: How to build and control an alternative version of the internet*. London: Zed Books.

Hofman, D., Lemieux, V. L., Joo, A., & Batista, D. (2019). The margin between the edge of the world and infinite possibility. *Records Management Journal, 29*(1/2), 240–257. https://doi.org/10.1108/RMJ-12-2018-0045.

Lustig, C., & Nardi, B. (2015). Algorithmic authority: The case of Bitcoin. In *2015 48th Hawaii International Conference on System Sciences (HICSS)*, HI (pp. 743–752). Los Alamitos, CA: IEEE. https://doi.org/10.1109/HICSS.2015.95

Raymond, E. S. (1999). *The cathedral and the bazaar: Musings on Linux and open source by an accidental revolutionary* (Vol. 12, pp. 23–49). Cambridge, MA: O'Reilly.

Walch, A. (2019a). In code(rs) we trust: Software developers as fiduciaries in public blockchains. In I. Lianos, P. Hacker, G. Dimitripolous, & S. Eich (Eds.), *Regulating blockchain: Techno-social and legal challenges* (pp. 58–81). Oxford: Oxford University Press.

Walch, A. (2019b). Deconstructing 'decentralization': Exploring the core claim of crypto systems. In C. Brummer (Ed.), *Cryptoassets: Legal, regulatory, and monetary perspectives* (pp. 39–68). New York: Oxford University Press.