JOURNAL OF MANAGEMENT INFORMATION SYSTEMS
2020, VOL. 37, NO. 2, 316–348
https://doi.org/10.1080/07421222.2020.1759974

Routledge
Taylor & Francis Group

Decision Problems in Blockchain Governance: Old Wine in New Bottles or Walking in Someone Else's Shoes?

Rafael Ziolkowski [a], Gianluca Miscione [b], and Gerhard Schwabe [a]

[a]University of Zurich, Zurich, Switzerland; [b]University College Dublin, Dublin, Ireland

ABSTRACT

Blockchain comes with the promise of being a disruptive technology with the potential for novel ways of interaction in a wide range of applications. Following broader application, scholarly interest in the technology is growing, though an extensive analysis of blockchain applications from a governance perspective is lacking to date. This research pays special attention to the governance of blockchain systems and illustrates decision problems in 14 blockchain systems from four application domains. Based on academic literature, semi-structured interviews with representatives from those organizations, and content analysis of grey literature, common problems in blockchain governance have been singled out and contextualized. Studying their enactment revealed their relevance to major organizational theories in what we labelled "Patrolling the borders," "External Legitimation," "Reduction of Discretionality," and "Temporal Management." The identification of these problems enriches the scarce body of knowledge on the governance of blockchain systems, resulting in a better understanding of how blockchain governance links to existing concepts and how it is enacted in practice.

KEYWORDS

Blockchain governance; decision-making in blockchain systems; blockchain; distributed governance

Introduction

In recent years, blockchain technology has emerged from being an enabler of cryptocurrencies to become a novel architecture to transact, maintain, and share data in a decentralized manner. All over the globe, organizations of all sorts form consortia to explore the merits of this technology [53]. These merits vary from product innovation or optimization of inter-organizational business processes by replacing third-party authentication with an algorithmic one that blockchain technology natively provides. After years of research in this field, it became clear that blockchain systems are at the same time a new instantiations of known research problems — hence "old wine in new bottles" in the title — and also present some novel dynamics, which require to be understood — hence "walking in someone else's shoes" — to revise our theoretical views. Indeed, three of the six decision problems we identified clearly relate to existing IS research problems. The other three are blockchain specific.

Despite all the enthusiasm, how those efforts are governed — also beyond who is formally in charge — remains an open question. The history of research on open as well as inter-organizational collaboration is long [17, 18]; despite being fundamentally different, collaboration in both settings has not always been fruitful, often for common reasons like mistrust, or vested interests [29, 46]. Our research sees governance through the narrow

CONTACT Rafael Ziolkowski ziolkowski@ifi.uzh.ch University of Zurich, Binzmuehlestrasse 14, CH-8050 Zurich, Switzerland

lens of decision problems and their corresponding solutions, thus shedding light on how blockchain systems are governed in open and inter-organizational settings. Then, theoretical implications of those findings are discussed.

Little is known about decision problems in the blockchain domain and how solutions can be found and enforced in blockchain systems [111]. There is a plethora of domain-specific governance frameworks in IT, in the corporate realm, public administration, and many more; while first steps have been made [13], a governance framework for blockchain systems in general, for example, examining the generic roles, responsibilities, decision rights, or incentives of actors in a blockchain system is yet to be defined. This gap in scientific literature and the practical relevance highlighted by the steadily increasing number of blockchain projects motivates our research. From both existing academic literature and our own cases, we (1) derive six decision problems within the blockchain domain (domain problem), (2) relate these to their root problem (abstract problem), and (3) shed light on blockchain-specific solutions to overcome these problems (domain solution). The latter is illustrated in a number of cases studied through semi-structured expert interviews with representatives from those cases and other complementary data. Studying their enactment revealed their relevance to major organizational theories in what we labelled "Patrolling the borders," "External Legitimation," "Reduction of Discretionality," and "Temporal Management."

This research answers the incumbent call for research on how blockchain systems are governed [13, 28]; not only to improve their well-functioning from an organizational perspective [75], but also to anticipate future inhibitors that may arise and the changes they bring to various domains [36]. Therefore, this research answers the following research questions:

Research Questions 1 (RQ1): What are major decision problems in blockchain systems?

Research Question 2 (RQ2): How are those problems dealt with in practice?

Research Question 3 (RQ3): What is the theoretical relevance of blockchain peculiarities?

The following section *Literature Review* provides an introduction to the research topic and introduces the reader to the field of governance in general as well as from a blockchain perspective. Next, within *Methodology*, we detail the underlying methodology in this research, followed by *Shaping Our Lens: A Focus on Decision Problems*, which presents the first part of our results with a narrow focus on blockchain decision problems. *Applying our Lens: Zooming in on Blockchain Governance Problems* then shows how these decisions are enacted within the application domains of supply chains, land registries, cryptocurrencies, and intellectual property rights management. Consequently, we discuss our results against the background of the works identified in *Literature Review* and well-established theoretical angles in *What Has Our Lens Made Visible?* Lastly, we conclude our work by giving an outlook for future research avenues within *Conclusion*.

Literature Review

The body of literature on blockchain has grown considerably, going well beyond its origins in engineering approaches. This section highlights the cornerstones of this literature. Before diving into them, we would like to anticipate that after we define and use our lens on the base of theorical and empirical work, we will be discussing our findings against broader theoretical concerns like: dichotomy of agency and context, legitimacy, uncertainty and risk in tightly coupled systems, and mis-matching timeframes.

Blockchain Systems

As this paper centers on governance, a technical explanation of how blockchains work is not considered here beyond what is directly relevant to our focus. To grasp the main differences in decision-making processes that blockchain offers, it is helpful to start with existing classifications of blockchain systems and to outline their main characteristics. A blockchain system is hereby defined as the underlying technology (blockchain) and its organizational embedment (the community surrounding the blockchain and its utilization). Following the notion of Peters and Panayi [91], a classification of blockchain systems can be seen along the access to transactions (public or private) and transaction validation rights (permissioned or permissionless), as seen in Table 1.

Table 1. Classification of blockchain types, adapted from Peters and Panayi [91].

		Access to Transaction Validation	
		Permissioned	Permissionless
Access to Transactions	**Public**	All nodes can read/submit transactions; authorized nodes validate transactions.	All nodes can read, submit, and validate transactions.
	Private	Only authorized nodes can read, submit, and validate transactions.	N/A

A blockchain system can provide trustworthy data (in the sense of trust in the maintainer of the system) to the extent that reliable data is entered in the first place [75]. This reliability is fostered through the blockchain's characteristics of decentralization (no central entity), persistency (transactions cannot be deleted), auditability (traceability of events), and anonymity (key pair authentication) [42, 118]; the latter may vary depending on the type of blockchain system utilized.

Perspectives on Governance

The term governance is used with different meanings in different application domains, with the most prominent being political [48], IT [112], and corporate [31]. According to well-known works from social sciences, modes of governance can be classified into markets, hierarchies, and networks [94, 114]. For our work, we understand governance as the means for organizational and economic coordination utilizing decision rights, incentives, and accountabilities [13], while we take a narrow empirical stance on decision problems. Decision-making rights and their enactment are thereby placed either on the individual actors' level (markets, free choice), the formal organization's level (hierarchy, authority), or the consortia's level (networks, consensus). To understand the nature of how decision rights are allocated and enacted in blockchain systems, the overall process of alignment, translation, and deployment of business goals into technological outcomes has to be understood. Hence, we consider the broader notion of the governance of IT systems;

this lens is helpful to understand the interplay between the emergence of requirements toward a technology and the factors that assure its successful implementation [37]. Weill [112] defined five core decisions to be made: IT principles (how IT is used in business), IT architecture (technical choices), IT infrastructure strategies (strategies for base foundation), business application needs (specifying business needs for development), and IT investment and prioritization (decisions on how project approval is made). This is not to assume IT only evolves within walled-off corporate environments. The history of inter-organizational systems is rich, specifically in business networks with high inter-organizational dependencies, such as supply chain management [73]. The collaborative use of information technology [96], or informational integration in general [30, 64], have frequently been considered of paramount interest, most recently for blockchain systems [78]. These efforts resulted in a de facto standard for electronic data interchange (EDI) and other collaborative planning methods such as efficient consumer response (ECR) or collaborative planning, forecasting, and replenishment (CPFR).

It is important to note, that blockchain systems have their origins in the free-and-open-source-software (FOSS) mode of production, which gained momentum from the late 90s. FOSS development exemplifies a mode of governance in the open [38] known as commons-based peer production [18]. It gained prominence by successfully developing foundational technologies that a vast number of systems depend upon (e.g., Linux). This mode of governance is marked by no central steering entity, constant forks, and, hence, a high customization of software towards a single user's needs. While authoritative actors emerge (e.g., Linus Torvalds with Linux), the absence of a formal authority, hence, raises the question of incentives and practices [66]. Even though blockchain technology finds its origins in the world of FOSS, and inherits some of its traits, some key decisions — mainly related to the immutability of the ledger — are peculiar and require specific attention.

Governance of Blockchain Systems

Public and permissionless blockchain systems, such as Bitcoin or Ethereum, have received increasing attention from researchers [28, 40, 76, 99]. The governance of these systems can be characterized as tribal [75]. As in tribes, actors tend to organize in loosely defined groups with shared interests and values. When interests diverge, some have the chance to branch out (forking) and create their own tribe (fork). Each tribe relies on a certain "togetherness" [75] to maintain the system. Incentives to influence the other actors' behavior hence emerge as crucial components in order to keep up with those mutual interests. The architects of those systems, for the initial design as well as later enhancements, are typically core developers (e.g., [21]). Open source principles, which are commonly adopted here and allow users to propose changes to the system as they see fit, can be supported by developers, but — differently from other FOSS projects — they need the agreement of other core actors, especially miners and token-owners. Having no entity formally in charge [76], those decision-making processes are often painfully complicated and ineffective, leading to governance crises that pose constant threats to the "tribe" [36].

This is not to say that a public and permissionless blockchain's decision-making shall be seen as completely decentralized. A number of authors [43, 60, 99, 111, 118] studied Bitcoin's governance and concluded the decision-making power to be unevenly distributed. Their arguments include inter alia (1) the inequality of mining power distribution and (2) the privileged standing of core developers in terms of software development. Glaser [51] also concedes that actual software development in blockchain systems is tightly bound to the control over the entire system. While the decision-making process involves miners, users and developers, prominent figures (e.g., Vitalik Buterin for Ethereum, Gavin Andresen for Bitcoin to a lesser extent) hold major influence over these systems; however, differently from other information systems, the developers' or public opinion leaders' influence can be counterbalanced by either miners' or users' [76, 111].

In the blockchain domain there is increasing awareness of those past governance issues and the shortcomings of the reductive assumptions associated with "code-is-law" [36, 40]. Current governance problems open up two ways forward [74]: Either, (1) blockchain communities push 'code-is-law' further (i.e., "more-of-the-same") but in a more robust manner, as seen in the development of on-chain governance structures within decentralized autonomous organizations[1] (DAOs), or (2) formal control in the form of off-chain governance bodies (e.g. foundations, consortia) has to be established. The prospect of authenticated records attracts interest from domains other than cryptocurrencies, contributing to the increasing popularity of permissioned blockchain systems led by consortia (e.g., R3 Corda). By their very nature, permissioned blockchains vary from permissionless ones in the restriction of validation or access rights or both [91]. Agreement upon data validity is thereby dependent on both well-allocated rights to write data (content) to the ledger and an appropriate consensus algorithm to preserve its state. Furthermore, the notion of smart contracts brings a form of algorithmic decision-making, providing an agreed-upon, deterministic sequence of events based on input criteria [50, 65].

Like other information systems, blockchain systems are subject to change over time [81]. In a similar vein, Morabito [76] describes the importance of studying the impact and the challenges brought by the evolution of decentralized blockchain-based systems and their governance. In addition, Walport [111] stresses that the successful implementation of blockchains requires adherence to the duality of both legal and algorithmic rule frameworks. Regulation of blockchain systems is also central to Okada et al. [85]: they discuss different modes of authority, incentive placements and the resulting consequences for blockchain systems.

Drawn from the previous arguments, it is clear that forms of organizing, and hence the decision-making process, in and around blockchain systems vary greatly. Thus, decision rights are hard to define and assign. It remains unexplored which decisions are deemed central to blockchain systems and which actors or organizations actually sit in the driver's seat, if there is one at all, and steer the development of blockchain systems. This demands exploration in the field.

Methodology

This research is product of a bottom-up, exploratory research. Therefore, no unique theoretical framework has driven our research design and process. This explains why we conclude proposing a toolkit instead of a unique conceptual view. This paper is embedded in a multi-year and multi-researcher study to explore blockchain systems in general and blockchain governance-related issues in particular. In terms of background, our research team covers information systems, organization studies, and design science expertise. This diversity allowed us, over the years of our common research, to triangulate our interpretations in an interdisciplinary manner. In addition, to continuously monitor and discuss developments in the blockchain domain light of its peculiar mode of governance, and to set them in relation to observations of our first studies on cryptocurrencies, a global, multi-disciplinary community of interest called Coding Value[2] was founded, comprising over 200 experts from academia as well as from practice.

As for the choice of methodologies to shed light on blockchain organizing in an exploratory manner, we proceeded as follows: following the actor-network-theory mantra of "follow the actors" — initially, in our case, a narrow view on blockchain developers — did not pay tribute to the interdependence of several actors that blockchain systems depend upon, as we previously argue. In addition, blockchain developers tend to stay hidden, while other actors such as users are arguably in the millions. Another approach would have been to "follow the actions" [35], which would have allowed us to be agnostic about the actors, but still would not have paid tribute to the scale the blockchain domain has reached over time.

Instead of following the actors (tend to stay hidden) or the actions (scale), it became visible from our project observations, discussions, and press articles, that those related to blockchain projects or crypto in general shared a common sense of what manifested central problems. Building upon this thought led us to our approach to follow problems as they materialized and, in particular, how they were being dealt with [59]. The fluidity of blockchain projects' members, the actors' underlying compatible interests, as well as shared values defined their mode of organizing, rather than clear organizational associations or stable identities, which led us to the approach of studying blockchain systems through the lens of a social movement [56]. This line of thought corresponds to our focus on organizing beyond formal organizations, and it pairs well with the postulated need to abandon the assumptions of (1) encapsulating information within organizations as if they were containers, and that (2) higher organizational levels disperse elements of work [115]. We extended this thought accordingly: context as well as agency, as Hayes et al. argue [57], are not pre-given but network-dependent. This is in line with the context of reference for cryptocurrencies, which does not pre-exist this phenomenon: the growth of crypto fostered interactions between organizations, users, regulators, developers, and geopolitics, among others. Therefore, our methodological stance stems from studying online practices as well as the modality in which these are performed as part of organizing processes, rather than seeing these through the lens of formal organizations [35].

Before specifying the methodology of this research and its narrow focus on decision problems, we set this research in context to already published works. As for our overall research output so far, initially, we focused on the understanding of properties of blockchain organizing from a general perspective. This was pursued within a first study on the significant empirical cases of land registries, which allowed us to put blockchain's peculiarities in the broader notion of common modes of governance [75]. But this study did not suffice to capture all peculiarities of blockchain organizing that emerged across different domains of application. In the time that followed, we narrowed our focus down to a more distinguished view between the peculiarities of organizing permissionless and permissioned blockchains. We built our argument on the empirical cases of land registries, several well-known cryptocurrencies, and cases from the supply chain domain, relating these to the notions of platforms and infrastructures [119] and the way these are said to be conflated in digital organizing [93].

For this particular study, in the form of an exploratory study [26, 106], we ensured a wide coverage of information and (1) derived codes based on practitioners' view and scientific literature, (2) found suitable cases to which we could apply those codes (interviews), and (3) utilized internal as well as external feedback for sense-making (data analysis and evaluation and refinement). Following these steps gave us a rich empirical basis which is, due to length limitations, only partly reported here.

Step 1: Literature Review

In developing an appropriate lens to study decision problems in blockchain systems, we were able to rely on a specialized and up-to-date literature basis established over the years and utilized by several researchers. Nevertheless, we strove to review the literature for the specificities of our research. In a first step, the scope of the search was set on governance in general, IT governance, its specificities of organizing, and how it translates to the blockchain realm. To ensure a consistent search, we first specified what is commonly understood as governance, and which parts we would specifically address. Next, we searched for literature on the main global repositories (ACM, Scopus, and Google Scholar), utilizing the following search terms (and their variations): "Blockchain governance," "inter-organizational governance," "shared governance," "blockchain decision-making," and "decentralized governance." This was a necessary step to identify, in how far our observations from other cases translate into academic discourse in order to find major decision problems in blockchain projects (RQ1). Within this search, only blockchain-related articles were considered. These articles can be found in the description of a decision problem in the following section. To ensure an overview as comprehensive as possible, and to also include practitioners' views on blockchain governance, a number of further information sources were used (as described in Step 3).

Step 2: Expert Interviews

To study how organizations meet these decision problems in practice (RQ2), we searched for mature blockchain systems as our empirical field. This proved difficult because blockchain's recent emergence has not allowed for many well-established systems. To ensure a comprehensive search, we utilized CoinDesk and CrunchBase (widely considered the most authoritative specialized news sources), and LinkedIn, and compiled a list of several hundred cases. Within this longlist, based on short case descriptions, we initially clustered along the four domains we aimed to study: supply chain management, intellectual property rights management, land registries, and cryptocurrencies. These domains were considered the most mature at the time of writing. Consequently, from a shortlist of cases we considered most likely to have the best organizational maturity based on media coverage, employee count, or starting year of project, we invited representatives for expert interviews, of which 18 accepted our invitations (Table 2). We thereby paid attention to maintain an even, thus comparable, number of cases (at least 3) per domain. As we could not triangulate one of these cases with other data, this case has been dismissed for consistency and comparability of results. It is important to note that our research design

Table 2. Interviewed cases.

Date	Interview	Case	Domain	Location	Maturity	Type	Interviewee Role
29.05.17	I1	1	Land Registry	Ghana	PoC	Public/Permissioned	CEO
31.05.17	I2	2	Land Registry	Honduras	PoC	Permissioned	Project Manager
02.06.17	I3	3	Supply Chain	USA	Operational	Permissioned	IT Employee
20.10.17	I4	4	Cryptocurrency	Global	Operational	Permissionless	Team Coach
25.10.17	I5	5	Land Registry	Sweden	Completed PoC	Permissioned	Project Lead
26.10.17	I6	6	Cryptocurrency	Global	Operational	Permissionless	Project Lead
30.10.17	I7	7	Supply Chain	Switzerland	Conceptual	Permissioned	Board Member
31.10.17	I8	8	Cryptocurrency	Global	Conceptual	Permissionless	Project Lead
01.11.17	I9	9	Supply Chain	China	Conceptual	Permissioned	CEO/Founder
03.11.17	I10	10	IPR	Global	Completed PoC	Permissioned	Associate Director
07.11.17	I11	11	Supply Chain	Belgium	PoC	Permissioned	Co-founder/CPO
10.11.17	I12	10	IPR	Global	Conceptual	Permissioned	Application Engineer
17.11.17	I13	11	Supply Chain	Belgium	Completed PoC	Permissioned	Business Developer
17.11.17	I14	12	IPR	Global	Operational	Permissionless	Application Director
20.11.17	I15	13	Land Registry	Georgia	PoC	Public/Permissioned	Security Managers
23.11.17	I16	13	Land Registry	Georgia	Conceptual	Public/Permissioned	Project Manager
23.03.18	I17	14	Cryptocurrency	Switzerland	Completed PoC	Permissionless	CEO

was informed by theoretical sampling: instead of aiming at a representative sample of a given population, we focused on classes of applications, then actually cases relevant to the problems we aimed to study; several cases were also brought forward and discussed within Coding Value. The interviews took the form of semi-structured expert interviews [77] and were recorded and transcribed for coding. We thereby created an interview guide inhering general questions, as well as permissionless- and permissioned-blockchain-specific questions, and we carefully adapted our interview guide throughout our research. In some cases, two representatives from the same company but in different positions were interviewed, allowing us to gain different perspectives on the same case, thus triangulating our interpretations.

Step 3: Grey Literature Review

As a background and complementary source of information to expert interviews, white-papers and a range of supporting documentation regarding these cases were helpful in understanding the features of each blockchain system and its high-level architecture. The purpose of this step was not to be dependent solely on interview statements, but to clarify (triangulate) interview statements, ensuring the internal validity of our methodology. Each blockchain initiative's website thereby served as a starting point for our search, and these proved to be helpful sources of information as they reflected opinions on the topic and addressed issues experienced by those initiatives. To not limit our data to our studied companies' views, we also strove to include press and opinion articles (e.g., on CoinDesk) on these cases written by externals. This allowed us to put their cases and anticipated risks in a broader context.

Step 4: Data Analysis

To begin the sense-making process, we analyzed relevant grey literature and interview transcriptions. The objective of using multiple sources of data was to compare and cross-check the data collected through interviews with different perspectives and triangulate our interpretations. Each interview was transcribed and coded. To achieve a rough understanding of our cases and to grasp their general properties, our initial coding dimensions centered around (1) the involved actors and their responsibilities, (2) the type of blockchain in use, (3) the chosen consensus mechanism, (4) decisions taken by the actors, (5) the current phase of the project, and (6) the expected advantages of using blockchain technology. As argued before, our lens has been informed by the wider frame of our overall research and refined in the analysis of our studied cases. Hence, in a subsequent coding step, we applied our lens to our cases for a comprehensive overview of each decision problem across cases. The results of this analysis concerned major blockchain governance decision problems as well as their enactment in practice, as described in the subsequent sections *Shaping Our Lens: A Focus on Decision Problems* and *Applying our Lens: Zooming in on Blockchain Governance Problems*.

Step 5: Evaluation and Refinement

Within our research, we iteratively sought feedback. Once an iteration of our results was conducted, we sought feedback by making our results available to co-researchers, practitioners working in the blockchain realm, major information systems conferences, and specialized workshops. This phase was conducted in an iterative fashion until saturation was achieved. The experts' feedback was then considered appropriately in the further design of this research.

Shaping Our Lens: A Focus on Decision Problems

To address RQ1, a review of academic literature, our extensive observations of blockchain projects, grey literature, and interviews revealed six major decision problems about blockchain governance (see Table 3; see online Appendix A for complementary interviewee quotes). We describe each decision in the following and relate all of them first to the literature and, in the next section, to our cases. Building upon grey literature and expert interviews, we then detail the fashion in which they are enacted, targeting RQ2. The first three decisions listed in the following section relate closely to conceptualizations of IT governance, thus this work focuses on adjusting them to blockchain specificities. The latter three are blockchain specific, thus they define blockchain governance and deserve particular attention.

Demand Management (DM)

Problem at Hand

User needs and information systems are naturally subject to evolution in terms of scale, functions, throughput, or others [81]. To manage this evolution, there must be a way to (1) capture, (2) funnel, and (3) agree upon changes to a system. These processes are not specific to blockchain systems; they have been at the heart of the research on IT demand management [69, 72] and major corporate IT development frameworks in general (e.g., ITIL, COBIT). The fulfillment of IT demands is subject to intertwined processes encompassing requirements engineering (e.g., specification of requirements), enterprise architecture management (e.g., fit to overall enterprise architecture), portfolio management

Table 3. Abbreviated summary of decision problems, problems at hand, and problems and solutions in the blockchain domain.

Decision Problem	Problem at Hand	Problem in the Blockchain Domain	Solution in the Blockchain Domain
Demand Management	User needs and IT change [81] Change process is central to several research streams [69, 72] This change process encompasses intertwined processes known from the corporate domain [69].	Practice shows that blockchains change and their modality of change is a key process [36, 61, 40]. Immutability and decentralization are affected by change Limited degrees of control through decentralization exacerbate change [61], but co-dependence of actors demands a change process.	Nowadays, most blockchains rely on informal consensus processes. Two ways forward are emerging [74]: ● **Off-chain** (Bitcoin, blockchain consortia, and others) ● **On-chain** (DAOs) coded consensus change processes.
Data Management	Data lays ground for numerous digital technologies [62, 58]. Data's value depends on its quality, which relies on specific properties [58, 108] and is hard to be maintained [11, 54, 87, 89], while several frameworks offer guidance.	Data management in blockchains is a vital research stream [3, 44, 76, 110], especially for compliance [14, 20] It regards two main aspects: data preservation and data input. ● Data **preservation**: Consensus algorithm ensures synchrony of data [76, 27], while being dependent on technical performance criteria [36, 3] ● Data **input**: "Garbage in, garbage out" referring to the varying quality of data inflow processing [7, 9].	Data **preservation** can be handled inter alia through, ● Design of underlying protocol ● Placement of nodes and choice of consensus algorithm Data **input**: Differentiation between the storage of trivial and non-trivial data. Known possibilities ● Incentives for data provision [116, 119] ● Delegation of data input to trusted parties, IoT-devices [110], external systems, or data triangulation [119]
System Architecture Design and Development	IT landscapes become increasingly complex [1, 23] while being contingent on individuals interpretation [22, 84], technical constraints [4], varying design processes [98] and modes of production [71], and its socio-technical framing [104].	Once deployed, blockchain systems are hard to change [74]. This path dependency requires a well-coordinated initial and subsequent architectural design [74, 117], with limited control that can be applied [76]. Developers are central stakeholders in blockchain systems [51, 60, 111]. Their centrality has two effects: ● Developers become **quasi-in-substitutable** [36] ● Developers exert influence **beyond technicalities**	Bitcoin inhered limited points of oversight and coordination over time [36], relying on informal discussions of core developers, so-called Bitcoin Improvement Proposals (BIPs), or coordination in forums or GitHub [110]. DAOs founded foundations to (1) serve as a focal point of reference in terms of project and development progress and (2) to allocate and budget funds for further system development.

(*Continued*)

Table 3. (Continued).

Decision Problem	Problem at Hand	Problem in the Blockchain Domain	Solution in the Blockchain Domain
Membership	N/A: Blockchain specific	Blockchains strive to keep human intervention to a minimum, by predefining users' rights [85, 91], and by influencing the openness of the platform, system performance [3], and privacy [20] issues. Blockchain systems compartmentalizing different kinds of data necessitate an identity assessment processes to grant read or write permissions only on subsets of data [6, 119]. Owners of these processes effectively steer the in- and outflow of users of the system, raising issues of inter-personal trust.	We observed several kinds of membership instantiations: • In permissionless & public blockchains, read and write rights are defined as open and participation is required [92, 118]. • Public & permissioned blockchains relying on proof-of-stake assign transaction validation rights to token holders. • In private & permissioned blockchains, read and write permissions are assigned and monitored by gatekeepers.
Ownership Disputes Tokenization	N/A: Blockchain specific	Blockchains allow for scarce data, which has two prospects: Clear data ownership and digital representation of physical assets. • The former allows for an explicit assignment of property rights through the use of a dedicated permission control system [6, 119]. • The latter regards the representation of physical assets through tokens [86] for a facilitated processing in the blockchain system [70], such as digitized land registry certificates [16].	Wallets serve as a means to assess and maintain ownership of digital assets. As wallets and digital assets have no physical representation, the allocation of ownership is limited to the degree that it would not stand a legal claim upon ownership. We are not aware of ownership dispute resolution systems in the blockchain domain.
Transaction Reversal	N/A: Blockchain specific	Unforeseen events, such as hacks, theft, or malfunctions occur frequently within the blockchain domain. In typical enterprise systems, transactions can be easily reversed. For blockchains, a transaction reversal contradicts its immutability. This has been inevitable in exemplary cases in the past. In these unforeseen events, stakeholders in a blockchain system must be empowered to reach consensus on how to proceed [76].	An effective means against fraudulent transactions is the concatenation of blockchains, or so-called anchoring services. Considering common blockchain architectures, there are limited ways of restoring a wrongfully transferred asset or granting a new private key in case of its loss – but the asset could be granted to new accounts upon human intervention and consensus.

(e.g., decision upon demand portfolio planning), and project management (implementation/approval of demand) [69].

Problems in Blockchain Systems

Practice has shown that blockchain systems are subject to change and that the way these changes are conducted is a key process. For example, the inability to achieve consensus on how to change its system led Bitcoin close to a stand-still, if not collapse, multiple times [36], leading to numerous forks over time [61]. Two of blockchain's key features are thereby affected: Immutability and decentralization. Undermining immutability — by means of forking the ledger to change the system — reverberates in the integrity of agreed upon functions, i.e. protocols or smart contracts [40] and the overall credibility of the ledger. Walport [111] strengthens this line of thought by arguing that in order to avoid degradation of the technology and to ensure longevity, blockchain systems should be continuously updated and enhanced. In addition, Okada et al. [85] emphasize the importance of organizational decision-making and a system's interoperability; also, standards ease challenges in interoperability as blockchains vary in codebase and infrastructure. Standards help organizations to select the most appropriate blockchain for their businesses [67], which has also been confirmed by several of our interviewees. As far as a blockchain system is decentralized, limited degrees of control can be applied, which was mentioned by several of our interviewees as a major hurdle. For example, changes to the system can be proposed, but other stakeholders can choose to decline them, which effectively disconnects them from the system [61]. The system, on the other hand, relies on user participation for both the value of its token and its security [119]. As a result, changes to the system are precarious but necessary as observed in practice [36, 40] and must be conducted in a coordinated manner.

Solutions in the Blockchain Domain

Questions arise regarding how novel business requirements of a blockchain system should be gathered, decided upon, and implemented. For example, for different decision types (strategic, tactical, or operational), who would be involved and decide on the adjustments (e.g., single actors vs. consensus among many), and how would the decision be made (e.g., ad hoc vs. planned)? In addition, the actors vary and can be internal (e.g., users) or external (standard-setting bodies, regulators). As seen in our related work, the most prominent blockchains nowadays still rely on informal consensus-finding processes. Related to the two ways forward in blockchain governance introduced in our related work [74], DAOs seem to be a promising approach. They formalize demand management and associated processes and give users a (decentralized) means to make their voice heard (tokens). Change proposals are thereby brought forward by their users, collaboratively specified and discussed, and decided upon; the result of the vote is binding and sealed through smart contracts. DAOs have their origin in the code-is-law movement around The Decentralized Autonomous Organization (TheDAO)[3] [40], and currently are being developed as what we termed code-is-constitution, meaning to define rules to change the rules.

Data Management (DAM)

Problem at Hand

Data lays ground for numerous digital technologies, such as modern decision-making systems [62], analytical applications in supply chains [58], or electronic data exchanges [79]. However, data's value depends on its quality, which is defined along the four dimensions of timeliness, accuracy, consistency, and completeness [58, 108]. The assurance of data quality is consistently regarded as a primal goal of data management [11, 54, 87, 89], which Pentek et al. [89, p. 74] summarize to "(…) include[s] the formulation of a data strategy, the definition of data management processes, standards, measures, the assignment of roles and responsibilities, the description of data lifecycle and architecture, and the management of applications and systems." To cope with data quality challenges, a plethora of reference guides or data management frameworks have been developed, such as the CDQ framework[4] or the DGI Data Governance Framework[5].

Problems in Blockchain Systems

How to manage data in blockchain systems is consistently seen as a major issue, as shown in its research stream [3, 44, 76, 110], especially when the handling of private data demands regulatory compliance [14, 20]. Data management in blockchain systems regards, broadly speaking, two aspects: data input and data preservation. The underlying issue of data preservation regards the fact that blockchain systems do not solely maintain data locally, but in collaboration with others through mining [76]. However, in order to be well-functioning, data must be synchronous among all node holders at the same time, which is at the heart of blockchains' consensus algorithms [27]. These design choices, on the other hand, can lead to performance issues when blockchain systems grow in number of processed transactions, as exemplified by Bitcoin's scaling debate [36] but is also seen on other platforms [3]. As a result, the way the data processing architecture is designed has an influence on the system's performance [3]. It's noteworthy, that the inability to reach a transaction throughput comparable to conventional databases has so far rendered blockchain technology unsuitable for high-frequency use-cases like micropayments [3, 32]. microp

Blockchains promise to overcome data quality issues in terms of consistency and timeliness among several actors by providing a single sourcing point, which is consistently named a top reason to deploy blockchain [53, 119]. While data in fact can be consistent and timely, its quality is not proven by blockchain itself. The underlying issue of data input therefore regards the inability of other actors to assess the rightfulness of entered data to the system. This effect is generally known as "garbage in, garbage out," referring to the varying quality of data inflow into a system and its consequent processing [7, 9]. Blockchain systems are particularly exposed to this problem because immutability extends the longevity of data of poor quality. In addition, users may avoid entering data as they could be held liable for wrongful entries after all [20]. Along this line, interviewee I1 points out: "(…) it's not (about) replacing the notaries' jobs, it's (about) making their jobs easier. (…) we are not saying: 'Hey, our technology is going to automate everything', because you can't automate quality control." Since blockchain's immutability constrains greatly data handling, one has to foresee the possibility of changing, deleting, or amending data when erroneous data has been entered or a new data regulation becomes effective, as currently seen with the GDPR in Europe [20].

Solutions in the Blockchain Domain

Data preservation can be handled through technical choices, such as the placement of nodes, the choice of consensus algorithms, the design of the underlying protocol; blockchain's immutability thereby assures that once entered, data stays the same, unless its change is demanded and agreed upon. The placement of nodes regards choosing whom to allow the access to transactions and whom to allow to validate transaction proposals, which is reflected in the classification of blockchain systems in Table 1 [91]. The mode in which transactions are validated refers to the choice of consensus algorithms, of which Bitcoin's proof-of-work [101] is still the most used. In order to deal with performance issues, researchers as well as practitioners developed a number of alternative consensus algorithms, such as variations of proof-of-stake [3,8] and proof-of-activity [19]. Proof-of-stake in particular is critically being debated as it divides validators along the number of tokens they hold [24, 80].

As for data input, it is important to differentiate between the storage of trivial (e.g., cryptocurrencies) and non-trivial (e.g., a list of attributes) data. In most cryptocurrencies to date, data is merely preserved and not further processed. In blockchain systems, which strive for process efficiencies [12, 117], input data is stored for further, often automatically executed processing, which is highly dependent on high quality data. It is also important to differentiate between varying modes of storage of data on blockchains, such as concatenations of various chains to store various kinds of data [10] or storing hashes as pointers to off-chain data [45]. There are several ways of increasing data quality in blockchain systems: One possibility regards incentives for data provision [116, 119]. For another, data input can be (1) delegated to trusted parties (e.g., notaries) or (2) delegated to IoT-devices (e.g., sensors), as observed in our studied cases, (3) assured through so-called oracles [110], which feed data from an external source, or (4) validated through data triangulation with different sources using smart contracts [119]. Several researchers are also working on solutions for deleting, changing, or amending data without affecting the system's data integrity. Their approaches include secure multiparty computation [2], redactable blockchains [5], and mutable blockchains [97]. In any case, it is worth mentioning that the immutability of the ledger may dissuade poor quality input to the extent that data enterers are aware that ledger transparency makes it easier to be found out later on.

System Architecture Design and System Development (SAD)

Problem at Hand

Information systems are the product of a design process and are therefore always subject to interpretation [22, 84]. There are several factors that define the design and maintenance of information systems, such as technical constraints [4], varying design processes [98] and modes of production [71], and its socio-technical framing [104]. The Open Group Architecture Framework (TOGAF[6]), an established and well-known enterprise architecture design framework, comprises the phases of designing, planning, implementing, and governing an enterprise IT architecture, modeled on the four layers of business, application, data, and technology. TOGAF, as well as many other enterprise architecture frameworks, arose from the need for a governance means in terms of oversight and coordination to deal with the increasing complexity of IT landscapes within and among enterprises [1, 23]. This includes the setting of enterprise-wide objectives and control mechanisms for varying IT development arrangements [102] and aligning business needs with IT demands [1]. According to Brosius et al. [23], Schmidt and Buxmann [103] as well as Lange et al. [68], enterprise architecture management is generally said to aim "(…) at effectiveness outcomes (e.g., the achievement of business goals and business-IT alignment), efficiency outcomes (e.g., mitigated IS landscape complexity, harmonized IS solutions), and general flexibility outcomes (e.g., utilization of applications) (…)."

Problems in Blockchain Systems

Once deployed, blockchain systems are hard to change [74]. Later changes require consensus among actors (as seen under demand management), and subsequent forks[7]. The initial architecture design as well as its subsequent development must therefore be well-coordinated, which is in line with several of our interviewees as well as literature [74, 117]. We named this process system architecture design and development, which describes who decides the requirements and functionalities of the initial as well as consequent blockchain system, for example, which technology is to be used, or how to ensure the system's interoperability when concatenated with other systems.

The decentralization of blockchain thereby limits the degree of control that can be applied [76]. This has paramount implications for the development and design of information systems: Without points of oversight and coordination processes, a goal-oriented and collaborative development of information technology under the measure of effectiveness, efficiency, and flexibility outcomes is highly exacerbated. Developers are arguably central stakeholders in blockchain systems as they have a major influence on the system's design and modes of maintenance [51, 60, 111]. Their centrality has two effects: These systems become increasingly dependent on the expert knowledge developers build over time, which then makes them quasi un-substitutable [36]. For example, Bitcoin's codebase, initially a rather basic blockchain system, became exponentially complex over time [21]. This also has governance implications as their expertise allows them to make better-informed decisions on the future system design. This is particularly precarious in cases where developers and users do not agree on how to proceed. Both Bitcoin and the Ethereum have shown their dependence on their core developers or influential figures in times of crisis multiple times [36, 40]. And their work is by no means perfect, as exemplified by the example of TheDAO, whose bug was produced not by amateurs but by a leading group of developers [41].

Solutions in the Blockchain Domain

It is evident in the blockchain domain, that the focal points of oversight and coordination are recognized as important pillars of their communities for system development and maintenance. To improve their practices, several DAOs founded foundations (e.g. Tezos, EOS, Ethereum) to (1) serve as a focal point of reference in terms of project and development progress and (2) allocate and budget funds for further system development. In contrast, in Bitcoin there have been limited points of oversight and coordination over time [36]. Most of the design and development has been conducted in a rather informal fashion and occurs either between core developers or in discussions in so-called Bitcoin Improvement Proposals (BIPs) in forums or GitHub [110].

Our cases show that system architecture design and development is often performed by either open source developers, an internal IT department, or a professional software development team, but always in collaboration with business stakeholders or its users. Several interviewees building public blockchain systems confirmed thereby the centrality of IT developers in their respective systems. Within several of our studied permissioned systems, our interviewees did not confirm their developers' centrality. In several of our cases there were procedures in place dictating how to develop and deploy code to production.

Membership (M)

Problems in Blockchain Systems

In order to avoid undesired behavior of users towards the system, platforms or information systems of any kind, explicitly or implicitly, have a built-in user management that defines an action space per user type [63]. This discrimination is a necessary control mechanism and is designed by the party in charge of the system. As exemplified by the previous decisions, blockchain systems rely on consensus forming among their users. To ease this process, blockchains strive to keep human intervention to a minimum, also by predefining users' rights [85, 91]. A fundamental decision regards thereby which users are allowed to read which transactions or to validate incoming ones. This decision has to be made with great care as it affects the openness of the platform, reliability of the ledger, system performance [3], and also privacy [20] issues. This decision is also motivated by the issue that blockchains broadcast all transactions to the entire network, making them, in theory, readable for all node holders, which is in contrast to distributed ledger systems [7]. Blockchain systems that compartmentalize different kinds of data are aware of these issues and establish identity assessment processes to grant read or write permissions only on subsets of data [6, 119].

If permissions to read or write data have to be granted based on user type, there must be ways of certifying users' identities. These roles, which we label gatekeepers, effectively steer the in- and outflow of users of the system. The definition of gatekeepers thereby is a central theme, raises the issue of inter-personal trust, and must be done with great care. The decision on membership in blockchains thereby regards both the assignment of read and write rights per user type as identity management as well as modes to entry/exit blockchain systems.

Solutions in the Blockchain Domain

The mode of entry or exit in blockchain systems depends highly on the type of blockchain in question (as seen in Table 1). Public permissionless and permissioned systems, by definition, do not explicitly define procedures for entry or exit. In Bitcoin (public permissionless) or Dash[8] (permissioned public) for example, users are free to join or to leave the network as they see fit. Permissioned private blockchains differ in this regard, as Okada et al. [85] stress the importance of a trusted authority who has the power over the system and can grant or deny permission to participate in the system, which is in line with several of our studied cases. I8 comments on central onboarding rights: "(…) the nodes are identified in the sense that they can only get smart contracts when the [central] node gives them access to the network. (…) which nodes have access to the network is governed by the community in our case." I1 comments on the importance of identities: "(…) this is where establishing identity control points is [important] (…). There is not going to be someone working within our system that we can't identify." Identity management also relates to the classification seen in Table 1, dealing with the specific rights a user has upon entry to the system. In Bitcoin, for example, read and write rights are defined as open and participation is explicitly required [92, 118]. Public and permissioned blockchains relying on proof-of-stake consensus, such as Dash, only assign transaction validation rights to token holders. In private and permissioned blockchains, read and write permissions are monitored by central decision makers: Gatekeepers. Dealing with personal data (e.g., in land registry or automotive records [16, 119]) requires a more fine-planned data access system. The type of identities thereby also gains prominence: Should users be anonymous, pseudonymous, or must there be a verified identity (e.g., for liability reasons)? The latter regards legality of actions and interoperability to public government infrastructures for identity verifications.

Ownership Disputes (OD)

Problems in Blockchain Systems

Ownership disputes are again unique to blockchain governance because they derive from the authenticity that blockchains grant. Blockchains allow for scarce data, which has two prospects: Clear data ownership and digital representation of physical assets. The former allows for an explicit assignment of property rights and control over personal data on data platforms through the use of a dedicated permission control system [6, 119]. The latter regards the representation of physical assets through tokens [86] for a facilitated processing in the blockchain system [70], such as digitized land registry certificates [16]. How to strengthen the link between digital and physical assets, however, is not resolved within the blockchain domain.

Solutions in the Blockchain Domain

With banks, fiat money serves as an allowance to be retrieved at an arbitrary cashier, and banks ensure the availability of that allowance to a certain degree. With the introduction of digitally verifiable assets, blockchains also introduced their own access systems: wallets. Having no physical representation of either one of these exacerbates the clear-cut allocation of ownership. While this technicality may be resolved, a pure digital ownership without legal grounding is hard to establish. What would happen if two users claimed ownership over the same asset? Blockchain systems must adhere therein to local jurisdiction, which has been frequently mentioned by our interviewees, and implement measures to reassign rightful ownership, which points at the importance of a clear-cut data management architecture. Interviewee I13 commented in this regard: "He can go to court to prove that he wasn't part of this deal and his property was stolen. The court will make a decision and the court will be using their authorized key [and] will publish the transaction in [the] blockchain that will say the property still owns to this person." It becomes evident that in blockchains there is a need to identify actors who resolve conflicts when multiple users claim the same property or if wallets holding assets are not accessible anymore.

Transaction Reversal (TR)

Problems in Blockchain Systems

Transaction reversal regards measures taken into account when unforeseen events (e.g., hacks, theft, malfunctions) happen to an information system. In typical enterprise systems, transactions can be easily reversed. This is not the case in blockchain systems. A transaction reversal contradicts a blockchain's immutability. This has been inevitable in exemplary cases in the past, like TheDAO outlined below. In these unforeseen events, stakeholders in a blockchain system must be empowered to reach consensus on how to proceed [76].

Solutions in the Blockchain Domain

A glaring example of a controversial transaction reversal — among others [88] — can be seen in TheDAO [40]. But not only miscoded smart contracts can cause the need for transaction reversals: Bitcoin, as I4 points out, is constantly under the threat of being attacked: "(…) [the] bitcoin network is the most hacked network of any network ever seen in the eternity of computing. It's [been] hacked 600 to 700 times every day because there is a lot of value for that. (…) So, that's why we know proof of stake and this private public key infrastructure is [generally] stable [although] it's being hacked." An effective means against hacks, as pointed out by further interviewees, seems to be concatenation of blockchains. Interviewee I5 regards checkpointing a state of data at a given time to another chain as a beneficial measure when agreement within one chain cannot be found. Concatenating even more chains is emphasized by I1: "Hacking one blockchain is next to impossible. Hacking four blockchains is obviously going to be exponentially more difficult than just one. It's not [only] times four, it's going to be a logarithmic increase of difficulty (…)." As for mistakes in data input, such as the wrongful transfer of ownership, I5 and I13 highlight the importance of not reverting a transaction for auditing reasons but to allocate a central, legitimized actor to write a new state of data into the ledger.

Considering common blockchain architectures, there is no way of restoring a wrongfully transferred asset or granting a new private key in case of its loss — but the asset could be granted to a new account (wallet) upon human intervention and consensus. I2 comments in this regard: "We're still people and we still need centralized parties that help us resolve conflicts. Software doesn't resolve conflict; it can just be a better record keeping system."

Applying our Lens: Zooming in on Blockchain Governance Problems

Deriving decision problems for blockchain systems (RQ1) served as a lens by which to see the decision problems that emerge from practice (RQ2). In the following, we illustrate their enactment in studied cases divided by domains.

Blockchains and Cryptocurrencies

With cryptocurrencies, there are differences observed, depending on the size of their community: In the case of Bitcoin, which is the largest studied case, demands are formulated and specified in online forums by any user, then agreed upon and implemented by developers; the adoption of a feature is then completed by deploying the updated version of the code to the user's node. However, major disagreements — especially about the block size (on which transaction volume and cost depend) — cannot be channeled by this process, resulting in repeated forks. But there are also rather hierarchically organized cryptocurrencies: Case 6, which is a Bitcoin fork, serves a rather small user base, and demand management is therefore conducted among its founders and, then, deployed to its users. Case 8 divides its user base in decision-making by assigning privileged rights to so-called master nodes, who decide among themselves which change to fund; however, proposals can still be proposed by anyone.

The case of blockchain-based cryptocurrencies concerns the first application area of blockchains overall. Table 4, below, illustrates the decision placement of cases 4 and 6, as well as case 8 (case 14 refers to a consortium and is hence not listed). In contrast to the previous cases, the blockchain-based cryptocurrencies are mostly built on public and permissionless ledgers, thus allowing members to partake in system architecture design and development (via community discussions and votes and all the typical processes of FOSS) as well as data management through mining (validating). In all systems, there is a group of core developers implementing the majority's will to their interpretation. There are limited measures (forks), however, if users conduct unintended transactions or seek support in disputes of asset ownership, pointing at blockchain's irreversibility. The initial design of the platforms, however, lies in the hands of its founders.

Table 4. Decision problems mapped to cryptocurrency cases.

	Case 4	Case 6	Case 8
DM	Users propose enhancements, developers decide	Team lead and two software developers	Users propose enhancements, auditors decide
SAD	Group of core developers	Anonymous developers	Company's core team members
TR	Individual user's responsibility	Individual user's responsibility	Individual user's responsibility
OD	Not applicable	Not applicable	Not applicable
M	Not applicable (Permissionless)	Not applicable (Permissionless)	Not applicable (Permissionless)
DAM	Consensus Algorithm	Consensus Algorithm	Consensus Algorithm

Blockchains and Intellectual Property Rights Management (IPR)

As for intellectual property rights management, we interviewed three experts from two companies (cases 10 and 12). Those projects aim to ease the management of intellectual property rights through unique identifiers and instant charges for usage of copyrights. Traditionally, those processes can be considered non-transparent and bureaucratic. The cases detailed in the following sections illustrate the aspired blockchain system and the cases' decision placements (see Table 5).

As for demand management, both systems vary in terms of decision-making power: While case 10 emphasizes the rather open, community-based vote, case 12 utilizes a permissioned system. Being backed by a foundation, case 10 derived its initial system architecture in collaboration with its users, while case 12's design is based on developer's choices. As for ownership disputes, both systems refer to actual courts. Data management is assured through consensus algorithms and the access to all transactions is public.

Table 5. Decision problems mapped to IPR cases.

	Case 10	Case 12
DM	Company decides based on community vote	PoC: Consensus among stakeholders
SAD	Foundation, software provider	Company's core team members
TR	Individual user's responsibility	Individual user's responsibility
OD	Appeal to courts	Appeal to courts
M	Not applicable (Permissionless)	Not applicable (Permissionless)
DAM	Community based	Consensus Algorithm

Blockchains and Supply Chains

Calls regarding supply chain inefficiencies and the need for informational and processual integration and transparency have been made for decades [107, 109], but often went unheard [29, 46]. Our collection of cases inheres four cases from the supply chain domain, partly varying in motivation to apply blockchain technology. Case 3 (platform developer, hence not mentioned in Table 6) and case 9, for example, target the product flow (know-your-object) for not only cost efficiencies but also transparency along the supply chain. Case 7, on the other hand, utilizes IoT-sensors for good distribution practice, measuring and guaranteeing the temperature of medical goods to other supply chain participants. Case 11, a port administration in Belgium, aims to automatize the check-in and check-out of its hundreds of daily customers and their containers, storing a unique identifier for each of them in their blockchain system.

As can be seen in Table 6, the decision rights for demand management are centralized in consortia, where formal consensus among stakeholders has to be found. This is also due to the permissioned nature of all blockchain systems. As case 11 regards a public function, the state imposes standards. Consortia and their (business) users consequently exhibit power over the system's architecture and its further development. As for the transaction reversals, all three use cases do not foresee measures to reverse those; this may be due to the fact that none of those cases are yet operational. In ownership disputes, all cases refer to courts. As for the membership, the systems of cases 7 and 9 plan to become permissioned and public: users may thus read entries, but validation is permissioned. Data management is assured through mining in cases 7 and 9, while case 11 utilizes a permissioned solution.

Table 6. Decision problems mapped to supply chain cases.

	Case 7	Case 9	Case 11
DM	External Consortium	External Consortium State sets standards	External Consortium State sets standards
SAD	Developers propose, consortium decides	Focal company in collaboration with state agency	Company decides, Consortium prioritizes
TR	Individual user's responsibility	Individual user's responsibility	Individual user's responsibility
OD	Appeal to courts	Appeal to courts	Appeal to courts
M	Not applicable	Not applicable	Port authority with companies
DAM	Sensor-based, Consensus Algorithm	Consensus Algorithm (PoS)	Contractual (Smart Contracts)

Blockchains and Land Registries

The prospect of registering land on a blockchain has gained increasing attention in recent years, predominantly in developing countries, where trust in formal authorities tends to be weaker. Blockchains could be used not only to replace third parties, but also to digitize paper-based and lengthy processes and to reduce costs. Our collection of cases considers four systems with similar goals (cases 1, 2, 5, and 13).

In the studied Land Registry systems, as a state function is performed, the state maintains the control over demand management, which resembles a hierarchical governance (see Table 7). We acknowledge private and permissioned blockchains, when led by a single party, hardly constitute a novelty as their practices, based on our observations, do not differ from practices seen in the corporate domain. As a state function is performed, the state maintains control over the system architecture design and development as well as standards or enhancements. Further, the state assures data management through the ledger, through concatenation of different blockchains, as well as through closer collaboration with affiliates (notaries, banks), using auditory nodes. In case of transaction reversals or conflict resolution, a user must appeal to court. While the partaking actors in the ecosystem do not change, users still benefit from transparency and reliability of records.

Table 7. Decision problems mapped to land registry cases.

	Cases 1, 2, and 13	Case 5
DM	Dictated by State Agency	Dictated by State Agency
SAD	State Agency and associated actors	State Agency
TR	Appeal to courts	Appeal to courts
OD	Appeal to courts	Appeal to courts
M	State Agency and affiliates	State Agency and affiliates
DAM	State Agency, Auditors	State Agency, Auditors

What Has Our Lens Made Visible?

In *Shaping Our Lens: A Focus on Decision Problems*, we have identified decision problems that blockchain systems have to deal with; this answered RQ1. To answer RQ2, we have shown how those decision rights are mapped in a variety of cases in *Applying our Lens: Zooming in on Blockchain Governance Problems*. As for RQ3, a wider discussion follows. Considering the matrices produced by matching the main aspects of decision problems and the empirical domains of application, we have distilled the main points that characterize blockchain governance and thus influence the types of decisions to be made (RQ1) as well as their enactment (RQ2) as follows: 1) patrolling borders, 2) external legitimation, 3) reduction of discretionality, and 4) temporal management. After references to the previous sections, each of these types is discussed in its theoretical relevance. This offers a theoretical toolkit, rather than a unified theory, for theoretically informed analyses of blockchain systems and beyond.

Patrolling Borders

A general problem of distributed systems, which acquires a peculiar flavor in blockchains, is the definition of who is in and who is out. FOSS is defined by abolishing any formal barrier to inclusion, and the same applies to blockchains to the extent that software production is involved. However, since the value of what blockchains authenticate derives also from miners/maintainers and users, different sorts of border controls are in place

[120]. Related to previous cases, it is remarkable how in permissioned blockchains, patrolling the borders is a far-reaching and effective control mechanism. In fact, since once an actor is in, preset rules apply, keeping actors out is an effective tool to avoid undesired behaviors. Governance issues from other cases, such as centralization of mining power, coordinated takeovers [36], or even take-downs [40] are hereby counterbalanced through a steering body and a partly walled-off system. Unless another actor's identity is stolen, the blockchain avoids unwanted access [42]. Even then, the clear audit trail of a blockchain [105] would allow the tracing back of misbehavior and reversal of transactions (in permissioned systems). Using unique and verified identifiers is well exemplified by the case of a Belgian port authority (case 11), where the monitoring of in- and out-flow is automatized and reduces governance costs of oversight. In more general terms, controlling the in- and out-flow of any resource can be an effective management tool in systems characterized by low to no hierarchy among the insiders.

In any formal organization, there are ways of defining who is in or out. In the market, disposable capital is the main definer. The aforementioned blockchain cases suggest the analogy of a club, whose main distinction is between inside and outside, members and the rest of the world. Contemporary information systems, and thus their analyses [115], need to acknowledge that the in or out distinction does not necessarily correspond — in fact it often does not correspond — to formal organizational boundaries. Indeed, the value of a club is exactly in allowing members' relationships across companies, public and private sectors, professions, and the like. A club's function as boundary spanner — while creating and policing its own boundaries — shows how organizations may also be obstacles to organizing [35], that is, there are valuable organizational actions that would be impossible without crossing the organizational boundaries. As long as organizational boundaries are perceived as clear, organizations are seen as organisms and/or cybernetic system. More suitable analogies for blockchains are club, Hansa [74], consortium, or even tribe in more fragmented and conflicting environments [75]. From the aforementioned cases, it can be noted that a much finer granularity of border patrolling is possible. Involved parties may agree on flexible or dynamic "gates" that allow or impede participation, then put in place a policing mechanism to enforce those agreements.

Last but not least, two entangled problems relate to the redefinition of boundaries and access control:

(1) The dichotomy of infrastructures versus platforms [33], with the former defined by wide accessibility and public interest, and the latter by multi-sided markets and profit seeking behaviors, respectively
(2) The prisoners' dilemmas that actors in low trust environments cope with continuously [49], and which impede the stabilization of agreements, in turn to be encoded in distributed ledgers.

External Legitimation

Blockchain technology finds its origins in the rejection of external authorities but, interestingly enough, states and other authorities are now adopting and deploying blockchains. Even if in most cases their control and power over these multi-party systems is relatively limited, when they are present, their role is not marginal, as it can be seen in the rather centralized decision-making placement in cases 1, 2, 5, and 13. Indeed, especially when the state weights in, legitimacy is outside of the consensus mechanisms inscribed and deployed by blockchains. The most evident outcome of state presence is the possibility of some sort of appeal that, contrary to the dogma of immutability [42], allows the reversion of undesirable entries or the exercising of further control, like excluding undesired actors. This centralization of decision rights, which may as a result correspond to the hierarchical ideal-type [114], raises the question of whether those prospected solutions indeed overcome core problems found nowadays in and around land registries [52, 100]; for example, decisions on data management as well as on reversing transactions would remain in the hands of the state or state-dependent actors (notaries). The prospected efficiency gains, however, seem widely desirable.

On the theoretical side, the unachievable self-containment of blockchains — and the consequent role of external legitimacy — calls for limiting the unfettered claims of regained agency that blockchains promise to their adopters. Blockchains, in fact, elude both internal legitimacy (acceptance based on nodes' consensus only) and external legitimacy (consensus derives from a well-defined context and its authorities). Instead, blockchains produce and rely upon a middle ground defined by the joining parties — which are not "into each other" but not external either — and their own contextual constraints.

The above implies that we have to refrain from going back to the conceptualization of context as pregiven [115]. Institutionalism [83] has traditionally highlighted the formal and informal constraints that shape actions exercised by the social environment within which organizations operate. Neoinstitutionalism [95] introduced the concept of an organizational field, which transcends organizations' immediate surroundings and comprises all organizations engaged in the same kind of activity (higher education, car manufacturing, etc.). Even though the latter concept is broader, it does not account for the diversity of contexts with which different blockchains interplay with. It is of course possible that over time, a blockchain organizational field would emerge, thus blockchains would be subject to similar pressures across the field. Whether this happens or not, all cases above illustrate how the context of reference for the blockchain emerging phenomenon is "network dependent," that is, usually disparate contexts like cryptographic software development communities, jurisdictions, landowners in emerging economies, miners, and artists, among others, are pulled together and provide novel modes of legitimacy before isomorphic pressures [39] spread throughout the field. Thus, by understanding the scattered but newly interdependent contexts of reference, we can shed new light on if or how legitimacy is gained in global context, and, thus, how innovation may succeed or fail.

Reduction of Discretionality

Since blockchains are basically enforced consensus algorithms, ad hoc decisions (i.e., discretionality) are intended to be minimized to the early stages of rules setting. Once they are built into algorithms, human intervention ends up being reduced, to the ideal extreme of people kept "out of the loop." Despite this, enhancement, membership, and off-the-chain conflict resolutions leave the door open for ad hoc decision-making. As can be seen in our case collection, conflict resolution protocols remain not in place or through real-life courts, membership is either regulated through gatekeepers or entirely open, and discussions on demand management is either enacted hierarchically (land registries), in consensus among few (supply chains), or in consensus among many (cryptocurrencies). These are all loopholes through which discretionality finds its way back in, and stands in contrast to the deterministic fashion in which smart contracts promise to function [65], which questions smart contract adoption maturity [50]. Thus, automatic and human decision-making appears to take place side by side, sometimes in competition, but algorithmic governance is merging with, rather than substituting, other modes of governance.

Reduction of actors' discretionality can be seen as an attempt to reduce the overall uncertainty of a system, thus, to mitigate risk. However, we should not be deterministic about this. As Perrow [90] made clear, tightly coupled systems — like those blockchains produce to the extent that involved parties are tied together — might be riskier because of unintended consequences and cascade effects that propagate quickly across a system whose nodes are synced and where human supervision is marginalized. As a result, a micro-level reduction of discretionality does not necessarily exclude/mitigate uncertainty and risk at an aggregate level. The creation of tightly coupled systems with no room for discretion may, to the extreme, be a recipe for disaster.

Temporal Management

Last but not least, all blockchains provide inalterable time-stamped records. Beyond this basic feature, most cases show some sort of temporal dimension in the form of enhancements, access control of new members, and reversion of transactions, which is in line with other operational blockchains [36, 40]. As with all information systems [22], the analyzed blockchain cases were initially designed according to a core group's preferences, which might mismatch with later needs. This places initiators as key stakeholders exercising major influence over blockchain systems [51, 60]. In other words, once the bootstrap problem is solved by reaching a critical mass, the same features of success in an environment may end up hampering further growth [55].

All of these aspects add human dimensions to decision-making and spread human influence on blockchain systems over long periods of time. This rather long time frame could be problematic for management because this new type of system may not live, at least in its current forms, as long as the functions that it is intended to perform. This opens the problem of future transitions to new technologies [81, 82] and for one, it points to the formerly introduced notion of tribal behavior [75] of users. On top of backward compatibility issues, two opposite problems arise: Lock-in effects and longevity. Both are central in relation to the immutability of records blockchains offer. Despite best intentions, anticipating long-term transformation of technologies proved impossible. Thus, it remains impossible to avoid risks of lock-in, even if open standards and architectures may mitigate these risks [47]. Needless to say, the lock-ins are acutely problematic when distributed ledgers are foundational for other activities like trades. Longevity of records may not be a paramount concern to the extent that stable and widely legitimized organizations, like states, can weigh in to certify what is needed. If certification capacity is completely reduced to hashed digital records, the unpredictability of the future and trust come together to the extent that no legitimator of last resort is available. As in tightly coupled systems, a reduction of checks and balances may increase rather than reduce uncertainty and risk.

Conclusion

This research studied blockchain systems through the lens of six decision problems emerging from blockchain governance: problems of demand management, data management, system architecture design and development, membership, ownership disputes, and transaction reversals. The first three are new instantiations of known information system research problems, thus they can be seen as ‘old wine in new bottles’. The latter three sit at odd with existing concepts, so they need to be understood — “walking in someone else’s shoes” — to further information system research in this emerging field. Illustrating their enactment on empirical domains guided our understanding of how power in those cases is distributed and in which fashion (algorithmic, ad hoc, formal, informal). The findings from the application of our lens suggest four dimensions of theoretical relevance, which can be synthesized as follows:

(1) The redefinition of borders and tools for their patrolling marks a major difference from the bazaar mode of governance [38] without falling back onto existing conceptualizations [94]. The blurring of the distinction between agency and context questions a basic assumption of cybernetics dating all the way back to its founder: Wiener [113] and Beer [15] who brought it to management studies.
(2) Descending from the previous, legitimacy does not come from inside or outside organizations, but is an ad hoc network-dependent arrangement produced by the parties involved, each with own context of reference. This exceeds the concept of context in Institutional theories [83, 95].
(3) While the reduction of discretionality, and the loathed politics, may be aimed at making the world fairer and more predictable, the cautionary tales of tightly coupled systems should raise a red flag and encourage a more critical approach to the consequences in practice of blockchain-based systems [90]. On the side, the design challenge of creating more loosely coupled systems while preserving some blockchain peculiarities is open.
(4) Timestamping and immutability are the peculiar features the blockchains bring about. As for tightly coupled systems, the theoretical challenge is in how those systems play out in practice and interact with organizations and society in relation to aspects that elude design, like long-term longevity. Here the main contribution is to studies on information infrastructures in practice, especially: Ciborra et al. [34], Bowker and Star [25], Hanseth and Lyytinen [55].

Of course, this research is not free of limitations. First and foremost, governance, whether implicit or explicit, emerges in practice and over time, and case studies can only depict snapshots at given times; hence, it would be interesting to see, in which domains blockchain technology is most adopted for one. We encourage researchers to iteratively study the governance of specific blockchain systems over time and to make conclusive statements about their evolution. Even though we paid close attention to properly shaping our lens, it does not and cannot address all peculiarities in relation to blockchain systems. Furthermore, permissioned blockchain systems in particular can be considered to be in their infancy, meaning the number of established and operational cases is still relatively limited. All things considered, our research, therefore, rather than making conclusive statements, strives to highlight and contextualize emerging problems in an exploratory manner, and propose cornerstones for further research. Our research not only answers the call for research on governance in and around blockchain systems, but also anticipates the consequences of those decisions in practice, which may also affect practitioners.

In conclusion, for further research, several things could be considered. As we argue, blockchain organizing exceeds firm boundaries and demands to define suitable modes of mutual dependency of multiple formally independent actors. Incentives constitute a possible glue between these actors and should be further studied. On the same line, besides decision problems, accountability problems could also be discussed. Even if blockchain organizing resembles to some degree the fluidity of FOSS, peculiar actor types can be derived and their roles and accountabilities described, as already initialized in early studies in this direction [61]. Finally, it is worth considering whether those blockchain systems end up allowing users to have more influence on decisions, or if blockchain systems are ultimately deprived of what is automatized by consensus algorithms. One way or another, following what people put their trust in and when, is a promising way to understand blockchains in practice.

Notes

1. Decentralized Autonomous Organizations (DAOs): Virtual organizations run by agreed upon code. Famous, and heavily funded (>US$500 million combined) examples include EOS (https://eos.io), Tezos (https://tezos.foundation), Aragon (https://aragon.one), The Decentralized Autonomous Organization, and D-Finity (https://dfinity.org)
2. https://codingvalue.weebly.com
3. The Decentralized Autonomous Organization: At it's time the largest crowdfunding project to date. A malfunctioning smart contract led to the loss of a significant amount of its funds. The discussion on how to proceed — reverting the malfunction or living with the consequences of lost funds — caused heated debates, resulting in the split of Ethereum's community [40].
4. https://www.cc-cdq.ch/cdq-framework
5. http://www.datagovernance.com/the-dgi-framework/
6. https://www.opengroup.org/togaf
7. There are several types of forks (i.e., soft- and hard forks) that vary in scope and consequences. For reasons of simplicity, we use the term "fork" interchangeably throughout this paper.
8. https://www.dash.org

Acknowledgements

An earlier version of this paper was presented at the Distributed Ledger Technology, The Blockchain Minitrack of the 2019 Hawaiian International Conference on System Sciences (HICSS), where it received the Best Paper Award in the Internet and the Digital Economy Track. First and foremost, we thank our interviewees for their invaluable efforts and time. We are further thankful for the helpful comments of three HICSS and two *JMIS* reviewers, the guest editors of this special issue, attendees of our paper presentation at HICSS, and members of Coding Value. Lastly, we particularly want to thank Geetha Parangi for her invaluable contribution to an earlier version of this paper.

ORCID

Rafael Ziolkowski http://orcid.org/0000-0002-4476-7735
Gianluca Miscione http://orcid.org/0000-0003-1479-6567

References

1. Ahlemann, F.; Stettiner, E.; Messerschmidt, M.; and Legner, C. *Strategic Enterprise Architecture Management: Challenges, Best Practices, and Future Developments*. Berlin; New York: Springer, 2012.
2. Andrychowicz, M.; Dziembowski, S.; Malinowski, D.; and Mazurek, L. Secure multiparty computations on bitcoin. In *Proceedings of the 2014 IEEE Symposium on Security and Privacy*. IEEE Computer Society, Washington, DC, USA, 2014, pp. 443–458.
3. Anh, D.T.T.; Zhang, M.; Ooi, B.C.; and Chen, G. Untangling blockchain: a data processing view of blockchain systems. *IEEE Transactions on Knowledge and Data Engineering*, *PP*, 99 (2018), 1366–1385.
4. Aniche, M.; Yoder, J.W.; and Kon, F. Current challenges in practical object-oriented software design. In *Proceedings of the 41st International Conference on Software Engineering: New Ideas and Emerging Results*. IEEE Press, Piscataway, NJ, USA, 2019, pp. 113–116.
5. Ateniese, G.; Magri, B.; Venturi, D.; and Andrade, E. Redactable blockchain – or – rewriting history in bitcoin and friends. In *2017 IEEE European Symposium on Security and Privacy (EuroS P)*. 2017, pp. 111–126.
6. Azaria, A.; Ekblaw, A.; Vieira, T.; and Lippman, A. MedRec: using blockchain for medical data access and permission management. In 2016 *2nd International Conference on Open and Big Da-ta (OBD)*. IEEE, Vienna, Austria, 2016, pp. 25–30.
7. Babich, V.; and Hilary, G. Distributed ledgers and operations: what operations management researchers should know about blockchain technology. *Manufacturing and Service Operations Management*, 22, 2 (2020), 223–240.
8. Bartoletti, M.; Lande, S.; and Podda, A.S. A proof-of-stake protocol for consensus on bitcoin subchains. In M. Brenner, K. Rohloff, J. Bonneau, A. Miller, P.Y.A. Ryan, V. Teague, A. Bracciali, M. Sala, F. Pintore, and M. Jakobsson, (eds.), *Financial Cryptography and Data Security*. Cham: Springer International Publishing, 2017, pp. 568–584.
9. Bateman, A.; and Cottrill, K. Blockchain's garbage in, garbage out challenge. 2017. https://supplychainmit.com/2017/10/19/blockchains-garbage-in-garbage-out-challenge/.
10. Bates, C. Bitland Global - Whitepaper. 2016. https://bravenewcoin.com/assets/Whitepapers/Bitland-Whitepaper.pdf.
11. Batini, C.; Cappiello, C.; Francalanci, C.; and Maurino, A. Methodologies for data quality assessment and improvement. *ACM Computing Surveys*, *41*, 3 (July 2009), 1–52.
12. Bauer, I.; Zavolokina, L.; Leisibach, F.; and Schwabe, G. Value creation from a decentralized car ledger. *Frontiers in Blockchain*, *2*, 30 (2020), 1–14.
13. Beck, R.; Müller-Bloch, C.; and King, J. Governance in the blockchain economy: a framework and research agenda. *Journal of the Association for Information Systems*, *19*, 10 (October 2018), 1020–1034.
14. Bell, T.W. Copyrights, privacy, and the blockchain. *Ohio Northern University Law Review*, *42*, 2 (2016), 1039–470.
15. Beer, S. *Decision and Control: The Meaning of Operational Research and Management Cybernetics*. John Wiley & Sons, London, New York, Sydney, 1966.
16. Benbunan-Fich, R.; and Castellanos, A. digitization of land records: from paper to blockchain. In *Proceedings of the 39th International Conference on Information Systems*. San Francisco, CA, USA, 2018.
17. Benkler, Y. *The Wealth of Networks: How Social Production Transforms Markets and Freedom*. New Haven, CT: Yale University Press, 2006.
18. Benkler, Y. Peer production, the commons, and the future of the firm. *Strategic Organization*, *15*, 2 (2017), 264–274.
19. Bentov, I.; Lee, C.; Mizrahi, A.; and Rosenfeld, M. Proof of activity: extending bitcoin's proof of work via proof of stake. *ACM SIGMETRICS Performance Evaluation Review*, *42*, 3 (2014), 34–37.

20. Berberich, M.; and Steiner, M. Blockchain technology and the GDPR - how to reconcile privacy and distributed ledgers reports: practitioner's corner. *European Data Protection Law Review (EDPL)*, *2*, (2016), 422–426.
21. Bitcoin Core. *bitcoin: Bitcoin Core integration/staging tree*. Bitcoin, 2018.
22. Bloomfield, B.P.; and Danieli, A. The role of management consultants in the development of information technology: the indissoluble nature of socio-political and technical skills. *Journal of Management Studies*, *32*, 1 (1995), 23–46.
23. Brosius, M.; Aier, S.; and Haki, M.K. Introducing a coordination perspective to enterprise architecture management research. In *2017 IEEE 21st International Enterprise Distributed Object Computing Workshop (EDOCW)*. 2017, pp. 71–78.
24. Buterin, V. Proof of Stake: How I Learned to Love Weak Subjectivity. *Ethereum Blog*, 2014. https://blog.ethereum.org/2014/11/25/proof-stake-learned-love-weak-subjectivity/.
25. Bowker, G.C.; and Star, S.L. *Sorting Things Out: Classification and Its Consequences*. MIT Press, Cambridge, Massachusetts, 2000.
26. Briggs, R.O.; and Schwabe, G. On Expanding the Scope of Design Science in IS Research. In H. Jain, A.P. Sinha and P. Vitharana, (eds.), *Service-Oriented Perspectives in Design Science Research*. Berlin, Heidelberg: Springer, 2011, pp. 92–106.
27. Cachin, C. Blockchain, Cryptography, And Consensus. 2017. https://www.zurich.ibm.com/cca/talks/20170622-blockchain-ice.pdf.
28. Campbell-Verduyn, M., ed. *Bitcoin and Beyond: Cryptocurrencies, Blockchains, and Global Governance*. Abingdon, Oxon; New York: Routledge, 2017.
29. Cao, M.; and Zhang, Q. Supply chain collaboration: Impact on collaborative advantage and firm performance. *Journal of Operations Management*, *29*, 3 (March 2011), 163–180.
30. Chen, M.-C.; Yang, T.; and Li, H.-C. Evaluating the supply chain performance of IT-based inter-enterprise collaboration. *Information & Management*, *44*, 6 (September 2007), 524–534.
31. Chhotray, V.; and Stoker, G. Governance: from theory to practice. Palgrave Macmillan UK, 2009, pp. 214–247.
32. Croman, K.; Decker, C.; Eyal, I.; Gencer, A.E.; Juels, A.; Kosba, A.; Miller, A.; Saxena, P.; Shi, E.; Sirer, E.G.; Song, D.; and Wattenhofer R. On scaling decentralized blockchains. In *International Conference on Financial Cryptography and Data Security*. Springer, 2016, pp. 106–125.
33. Constantinides, P.; Henfridsson, O.; and Parker, G.G. Introduction—platforms and infrastructures in the digital age. *Information Systems Research*, *29*, 2 (May 2018), 381–400.
34. Ciborra, C.; Braa, K.; Cordella, A.; et al. *From Control to Drift: The Dynamics of Corporate Information Infrastructures*. Oxford, England: Oxford University Press, 2000.
35. Czarniawska, B. *A Theory of Organizing: Second edition*. Cheltenham, UK: Edward Elgar Publishing, 2014.
36. De Filippi, P.; and Loveluck, B. *The Invisible Politics of Bitcoin: Governance Crisis of a Decentralized Infrastructure*. Rochester, NY: Social Science Research Network, 2016.
37. De Haes, S.; and Van Grembergen, W. IT governance and its mechanisms. *Information Systems Control Journal*, *1*, (2004), 27–33.
38. Demil, B.; and Lecocq, X. Neither market nor hierarchy nor network: the emergence of bazaar governance. *Organization Studies*, *27*, 10 (2006), 1447–1466.
39. DiMaggio, P.J.; and Powell, W.W. The Iron cage revisited: institutional isomorphism and collective rationality in organizational fields. *American Sociological Review*, *48*, 2 (1983), 147–160.
40. DuPont, Q. Experiments in algorithmic governance: a history and ethnography of "The DAO," a failed decentralized autonomous organization. In M. Campbell-Verduyn, (ed.), *Bitcoin and Beyond: Cryptocurrencies, Blockchains and Global Governance*. Routledge, Routledge, London, UK, (2017), pp. 157–177.
41. DuPont, Q. *Cryptocurrencies and Blockchains*. Medford, MA: Polity, 2019.
42. DuPont, Q.; and Maurer, B. Ledgers and law in the blockchain. *Kings Review (23 June 2015) http://kingsreview. co. uk/magazine/blog/2015/06/23/ledgers-and-law-in-the-blockchain*, (2015).

43. Dwyer, G.P. The economics of Bitcoin and similar private digital currencies. *Journal of Financial Stability*, *17*, (2015), 81–91.
44. Eberhardt, J.; and Tai, S. On or off the blockchain? Insights on off-chaining computation and data. In F. De Paoli, S. Schulte, and E. Broch Johnsen (eds.), *Service-Oriented and Cloud Computing*. Cham, Switzerland: Springer International Publishing, 2017, pp. 3–15.
45. Exonum. Blockchain Land Registry — National Agency of Public Registry in the Republic of Georgia — Exonum. 2018. https://exonum.com/napr.
46. Fawcett, S.E.; McCarter, M.W.; Fawcett, A.M.; Webb, G.S.; and Magnan, G.M. Why supply chain collaboration fails: the socio-structural view of resistance to relational strategies. *Supply Chain Management: An International Journal*, *20*, 6 (September 2015), 648–663.
47. Fishenden, J.; and Thompson, M. Digital Government, Open Architecture, and Innovation: Why Public Sector IT Will Never Be the Same Again. *Journal of Public Administration Research and Theory*, *23*, 4 (October 2013), 977–1004.
48. Fukuyama, F. What is governance? *Governance*, *26*, 3 (July 2013), 347–368.
49. Gambetta, D. *Codes of the Underworld: How Criminals Communicate*. Princeton, New Jersey: Princeton University Press, 2011.
50. Gatteschi, V.; Lamberti, F.; Demartini, C.; Pranteda, C.; and Santamaría, V. Blockchain and smart contracts for insurance: is the technology mature enough? *Future Internet*, *10*, 2 (February 2018), 20.
51. Glaser, F. Pervasive decentralisation of digital infrastructures: a framework for blockchain enabled system and use case analysis. In *Proceedings of the 50th Hawaii International Conference on System Sciences*, 2017.
52. Goldstein, M.; and Udry, C. The profits of power: land rights and agricultural investment in Ghana. *Journal of Political Economy*, *116*, 6 (December 2008), 981–1022.
53. Gratzke, P.; Schatsky, D.; and Piscini, E. Banding together for blockchain. *Deloitte Insights*, 2017. https://www2.deloitte.com/insights/us/en/focus/signals-for-strategists/emergence-of-blockchain-consortia.html.
54. GS1. Data Quality Framework. 2014. https://www.gs1.org/services/data-quality/data-quality-framework.
55. Hanseth, O.; and Lyytinen, K. Design theory for dynamic complexity in information infrastructures: the case of building internet. *Journal of Information Technology*, *25*, 1 (March 2010), 1–19.
56. Hargrave, T.J.; and Van De Ven, A.H. A collective action model of institutional innovation. *Academy of Management Review*, *31*, 4 (2006), 864–888.
57. Hayes, N.; Miscione, G.; and Westrup, C. Overflows of technological innovation in emerging economies: the case of M-Pesa. (2013). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2617305
58. Hazen, B.T.; Boone, C.A.; Ezell, J.D.; and Jones-Farmer, L.A. Data quality for data science, predictive analytics, and big data in supply chain management: an introduction to the problem and suggestions for research and applications. *International Journal of Production Economics*, *154*, (August 2014), 72–80.
59. Hoppe, R. *The Governance of Problems: Puzzling, Powering and Participation*. Policy Press, Bristol, UK, 2011.
60. Hsieh, Y.-Y.; Vergne, J.-P.; and Wang, S. *The Internal and External Governance of Blockchain-Based Organizations: Evidence from Cryptocurrencies*. Rochester, NY: Social Science Research Network, 2017.
61. Islam, N.; Mäntymäki, M.; and Turunen, M. Understanding the role of actor heterogeneity in blockchain splits: an actor-network perspective of bitcoin forks. In *Proceedings of the 52nd Hawaii International Conference on System Sciences*. Hawaii, 2019.
62. Janssen, M.; van der Voort, H.; and Wahyudi, A. Factors influencing big data decision-making quality. *Journal of Business Research*, *70*, (January 2017), 338–345.
63. Jøsang, A.; and Pope, S. User centric identity management. In *in Asia Pacific Information Technology Security* Conference, *AusCERT2005*, *Austrailia*. 2005, pp. 77–89.

64. Kembro, J.; and Selviaridis, K. Exploring information sharing in the extended supply chain: an interdependence perspective. *Supply Chain Management: An International Journal*, *20*, 4 (June 2015), 455–470.
65. Kitchin, R. Thinking critically about and researching algorithms. *Information, Communication & Society*, *20*, 1 (January 2017), 14–29.
66. Krogh, G.V.; Haefliger, S.; Spaeth, S.; and Wallin, M.W. Carrots and rainbows: motivation and social practice in open source software development. *MIS Quarterly*, *36*, 2 (2012), 649–676.
67. Kshetri, N. Will blockchain emerge as a tool to break the poverty chain in the Global South? *Third World Quarterly*, *38*, 8 (August 2017), 1710–1732.
68. Lange, M.; Mendling, J.; and Recker, J. An empirical analysis of the factors and measures of Enterprise Architecture Management success. *European Journal of Information Systems*, *25*, 5 (September 2016), 411–431.
69. Legner, C.; and Löhe, J. Improving the realization of IT demands: a design theory for end-to-end demand management. *Proceedings of the 33rd International Conference on Information Systems*, December 2012.
70. Lemieux, V.L. Evaluating the Use of blockchain in land transactions: an archival science perspective. *European Property Law Journal*, *6*, 3 (2017), 392–440.
71. Li, K.; Xiao, J.; Wang, Y.; and Wang, Q. Analysis of the key factors for software quality in crowdsourcing development: an empirical study on TopCoder.com. In *2013 IEEE 37th Annual Computer Software and Applications Conference*. 2013, pp. 812–817.
72. Mckeen, J.; Smith, H.; and Gonzalez, P. Managing IT Demand. *Journal of Information Technology Management*, *23*, 2 (2012), 17–28.
73. Mentzer, J.T.; DeWitt, W.; Keebler, J.S.; Min, S.; Nix, N.W.; Smith C.D.; and Zacharia Z.G. Defining supply chain management. *Journal of Business Logistics*, *22*, 2 (September 2001), 1–25.
74. Miscione, G.; Klein, S.; Schwabe, G.; Goerke, T.M.; and Ziolkowski, R. Hanseatic governance: understanding blockchain as organizational technology. In *Proceedings of the 40th International Conference on Information Systems*, Munich, 2019.
75. Miscione, G.; Ziolkowski, R.; Zavolokina, L.; and Schwabe, G. Tribal governance: the business of blockchain authentication. In *Proceedings of the 51st Annual Hawaii International Conference on System Sciences*. Oahu, Hawaii, USA, 2018.
76. Morabito, V. *Business Innovation Through Blockchain*. Cham, Switzerland: Springer International Publishing, 2017.
77. Myers, M.D.; and Newman, M. The qualitative interview in IS research: examining the craft. *Information and Organization*, *17*, 1 (January 2007), 2–26.
78. Nakasumi, M. Information sharing for supply chain management based on block chain technology. In *2017 IEEE 19th Conference on Business Informatics (CBI)*. 2017, pp. 140–149.
79. Nicolaou, A.I.; Ibrahim, M.; and van Heck, E. Information quality, trust, and risk perceptions in electronic data exchanges. *Decision Support Systems*, *54*, 2 (January 2013), 986–996.
80. Houy, N. It will cost you nothing to “kill” a proof-of-stake crypto-currency. *Economics Bulletin*, *34*, 2 (January 2014), 1038–1044.
81. Nitto, E.D.; Ghezzi, C.; Metzger, A.; Papazoglou, M.; and Pohl, K. A journey to highly dynamic, self-adaptive service-based applications. *Automated Software Engineering*, *15*, 3–4 (December 2008), 313–341.
82. Norta, A. Establishing distributed governance infrastructures for enacting cross-organization collaborations. In A. Norta, W. Gaaloul, G.R. Gangadharan and H.K. Dam (eds.), *Service-Oriented Computing – ICSOC 2015 Workshops*. Berlin Heidelberg: Springer, 2016, pp. 24–35.
83. North, D.C.; and Alt, J. *Institutions, Institutional Change, and Economic Performance*. Rochester, NY: Social Science Research Network, 1990.

84. Oinas-Kukkonen, H.; and Harjumaa, M. Persuasive systems design: key issues, process model and system features. *Communications of the Association for Information Systems*, *24*, 1 (2009), 485–500.
85. Okada, H.; Yamasaki, S.; and Bracamonte, V. Proposed classification of blockchains based on authority and incentive dimensions. In *2017 19th International Conference on Advanced Communication Technology (ICACT)*. 2017, pp. 593–597.
86. Oliveira, L.; Zavolokina, L.; Bauer, I.; and Schwabe, G. To Token or not to Token: Tools for Understanding Blockchain Tokens. In *Proceedings of the 39th International Conference on Information Systems*. San Francisco, CA, USA, 2018.
87. Otto, B.; Hüner, K.M.; and Österle, H. Toward a functional reference model for master data quality management. *Information Systems and e-Business Management*, *10*, 3 (September 2012), 395–425.
88. Pauw, C. EOS BP, Explained. *Cointelegraph*, 2019. https://cointelegraph.com/explained/eos-bp-explained.
89. Pentek, T.; Legner, C.; and Otto, B. Towards a reference model for data management in the digital economy. In *Proceedings of the 12th International Conference on Design Science Research in Information* Systems *and Technology*. Karlsruher Institut für Technologie (KIT), Karlsruhe, Germany, 2017, pp. 73–82.
90. Perrow, C. *Normal Accidents: Living with High Risk Technologies - Updated Edition*. Princeton, New Jersey, USA: Princeton University Press, 2011.
91. Peters, G.W.; and Panayi, E. Understanding modern banking ledgers through blockchain technologies: future of transaction processing and smart contracts on the internet of money. *arXiv:1511.05740 [cs]*, (November 2015).
92. Pilkington, M. *Blockchain Technology: Principles and Applications*. Cheltenham, UK: Edward Elgar Publishing, 2015.
93. Plantin, J.-C.; Lagoze, C.; Edwards, P.N.; and Sandvig, C. Infrastructure studies meet platform studies in the age of Google and Facebook. *New Media & Society*, *20*, 1 (2016), 293–310.
94. Powell, W.W. Neither market nor hierarchy. *Research in Organizational Behavior*, *12*, (1990), 295–336.
95. Powell, W.W.; and DiMaggio, P.J. *The New Institutionalism in Organizational Analysis*. London, UK: University of Chicago Press, 1991.
96. Prajogo, D.; and Olhager, J. Supply chain integration and performance: the effects of long-term relationships, information technology and sharing, and logistics integration. *International Journal of Production Economics*, *135*, 1 (January 2012), 514–522.
97. Puddu, I.; Dmitrienko, A.; and Capkun, S. μchain: how to forget without hard forks. *IACR Cryptology ePrint Archive*, *2017*, (2017), 106.
98. Razavian, M.; Tang, A.; Capilla, R.; and Lago, P. In two minds: how reflections influence software design thinking. *Journal of Software: Evolution and Process*, *28*, 6 (2016), 394–426.
99. Reijers, W.; O'Brolcháin, F.; and Haynes, P. Governance in blockchain technologies & social contract theories. *Ledger*, *1*, (2016), 134–151.
100. Rizzo, P. Blockchain Land Title Project "Stalls" in Honduras. *CoinDesk*, 2015. http://www.coindesk.com/debate-factom-land-title-honduras/.
101. Nakamoto, S. Bitcoin: a peer-to-peer electronic cash system. *Independent*, (2008).
102. Schilling, R.D.; Haki, K.; and Aier, S. Dynamics of control mechanisms in enterprise architecture management: a sensemaking perspective. In *Proceedings of the 39th International Conference on Information Systems*. San Francisco, CA, USA, 2018.
103. Schmidt, C.; and Buxmann, P. Outcomes and success factors of enterprise IT architecture management: empirical insight from the international financial services industry. *European Journal of Information Systems*, *20*, 2 (March 2011), 168–185.
104. Seth, F.P.; Mustonen-Ollila, E.; and Taipale, O. The influence of management on software product quality: an empirical study in software developing companies. In B. Barafort, R.V. O'Connor, A. Poth, and R. Messnarz (eds.), *Systems, Software and Services Process Improvement*. Berlin Heidelberg: Springer, 2014, pp. 147–158.

105. Snow, P.; Deery, B.; Lu, J.; Johnston, D; and Kirby P. Business processes secured by immutable audit trails on the blockchain. 2014. http://www.bcventures.net/uploads/3/9/8/6/39865783/_factom_whitepaper.pdf.
106. Stebbins, R.A. *Exploratory Research in the Social Sciences*. Thousand Oaks, London, New Delhi: Sage, 2001.
107. Steinfield, C.; Markus, M.L.; and Wigand, R.T. Through a glass clearly: standards, architecture, and process transparency in global supply chains. *Journal of Management Information Systems*, *28*, 2 (October 2011), 75–108.
108. Stentoft Arlbjørn, J.; and Haug, A. Barriers to master data quality. *Journal of Enterprise Information Management*, *24*, 3 (April 2011), 288–303.
109. Stevens, G.C.; and Johnson, M. Integrating the supply chain … 25 years on. *International Journal of Physical Distribution & Logistics Management*, *46*, 1 (January 2016), 19–42.
110. Swan, M. *Blockchain: Blueprint for a New Economy*. Sebastopol, California, USA: O'Reilly Media, Inc., 2015.
111. Walport, M. Distributed ledger technology: beyond blockchain. *UK Government Office for Science*, London, UK, (2016).
112. Weill, P. Don't just lead, govern: how top-performing firms govern IT. *MIS Quarterly Executive*, *3*, 1 (2004), 1–17.
113. Wiener, N. *Cybernetics; or Control and Communication in the Animal and the Machine*. Oxford: Wiley, 1948.
114. Williamson, O.E. *Markets and Hierarchies: Analysis and Antitrust Implications: A Study in the Economics of Internal Organization*. Rochester, NY: Social Science Research Network, 1975.
115. Winter, S.; Berente, N.; Howison, J.; and Butler, B. Beyond the organizational "container": conceptualizing 21st century sociotechnical work. *Information and Organization*, *24*, 4 (October 2014), 250–269.
116. Zavolokina, L.; Spychiger, F.; Tessone, C.J.; and Schwabe, G. Incentivizing data quality in blockchains for inter-organizational networks "learning from the digital car dossier. In *Proceedings of the 39th International Conference of Information Systems*. San Francisco, CA, USA, 2018.
117. Zavolokina, L.; Ziolkowski, R.; Bauer, I.; and Schwabe, G. Management, governance, and value creation in a blockchain consortium. *MIS Quarterly Executive*, *19*, 1 (February 2020).
118. Zheng, Z.; Xie, S.; Dai, H.-N.; Chen, X.; and Wang, H. *An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends*. In *Big Data (BigData Congress), 2017 IEEE International Congress on. IEEE*, 2017, pp. 557–564.
119. Ziolkowski, R., Miscione, G., and Schwabe, G. Consensus through Blockchains: exploring governance across inter-organizational settings. In *Proceedings of the 39th International Conference on Information Systems*. San Francisco, CA, USA, 2018.
120. Ziolkowski, R.; Parangi, G.; Miscione, G.; and Schwabe, G. Examining gentle rivalry: decision-making in blockchain systems. In *Proceedings of the 52nd Annual Hawaii International Conference on System Sciences*. Maui, Hawaii, USA, 2019.

About the Authors

Rafael Ziolkowski (ziolkowski@ifi.uzh.ch; corresponding author) is a doctoral student and research assistant at the Information Management research group at the University of Zurich, Switzerland. He holds a Master's degree in Information Systems from the University of Duisburg-Essen, Germany. His research interests are at the intersection of technology and modes of organizing, interorganizational system governance, the applicability of distributed ledger technologies, and distributed ledger technologies in general.

Gianluca Miscione (gianluca.miscione@ucd.ie) is Assistant Professor at the School of Business of University College Dublin, Ireland. He conducted and contributed to research in Europe, Latin America, India, East Africa, and on the Internet. His research focuses on the interplay between

technologies and organizing processes with a specific interest on innovation, development, organizational change, social networks, and trust. His uses qualitative and mixed methodologies.

Gerhard Schwabe (schwabe@ifi.uzh.ch) is Professor in the Department of Informatics at the University of Zurich, Switzerland, where he leads the Information Management research group. He received his doctoral and postdoctoral education at the University of Hohenheim, Germany. He researches the intersection of collaborative technologies and information management. He has studied collaboration in commercial and government organizations at the granularity of dyads, small teams, large teams, organizations, communities, and social networks, frequently in collaboration with companies and public organizations. He has published numerous papers in major journals and conference proceedings, in information systems as well as in computer science.