From authentication to 'Hanseatic governance': Blockchain as organizational technology

Conference Paper · January 2019

5 authors, including:

Gianluca Miscione
University College Dublin
180 PUBLICATIONS   **577** CITATIONS

SEE PROFILE

Stefan Klein
University of Münster
204 PUBLICATIONS   **2,724** CITATIONS

SEE PROFILE

Gerhard Schwabe
University of Zurich
348 PUBLICATIONS   **3,011** CITATIONS

SEE PROFILE

Rafael Ziolkowski
University of Zurich
12 PUBLICATIONS   **70** CITATIONS

SEE PROFILE

Some of the authors of this publication are also working on these related projects:

Coding Value View project

Blockchain Car Dossier View project

Year: 2019

From authentication to 'Hanseatic governance': Blockchain as organizational technology

Miscione, Gianluca ; Goerke, Tobias ; Klein, Stefan ; Schwabe, Gerhard ; Ziolkowski, Rafael

Abstract: Blockchain technology provides a distributed ledger and is based on a logic of peer to peer authentication. It gained prominence with the rise of cryptocurrencies but provides a much broader field of possible application, including – but not limited to – land and other registries, global trade systems. While it has been originally closely linked to a libertarian, anarchic agenda, recent developments of commercial applications have illustrated that it can been dissociated from a particular ideological framing. The purpose of our paper is to identify and classify core properties of blockchain as an organizational technology and related modes of blockchain governance. We do this by looking at a number of case studies which highlight a number of governance design issues as well as unintended effects of the technology and related design choices. We are exploring the linkages between blockchain application properties and related design options and choices.

Provided by the author(s) and University College Dublin Library in accordance with publisher
policies. Please cite the published version when available.

Title	þÿFrom authentication to Hanseatic governance : Blockchain
Authors(s)	Miscione, Gianluca; Goerke, Tobias; Klein, Stefan; et al.
Publication date	2019-01-15
Conference details	London School of Economics and Political Science (LSE) seminar series organized by the Department of Management, London, UK
Item record/more information	http://hdl.handle.net/10197/10575

From authentication to 'Hanseatic governance': Blockchain as organizational technology

Gianluca Miscione, University College Dublin

Tobias Goerke, University of Münster

Stefan Klein, University of Münster

Gerhard Schwabe, University of Zürich

Rafael Ziolkowski, University of Zürich

Abstract.

Blockchain technology provides a distributed ledger and is based on a logic of peer to peer authentication. It gained prominence with the rise of cryptocurrencies but provides a much broader field of possible application, including – but not limited to – land and other registries, global trade systems. While it has been originally closely linked to a libertarian, anarchic agenda, recent developments of commercial applications have illustrated that it can been dissociated from a particular ideological framing. The purpose of our paper is to identify and classify core properties of blockchain as an organizational technology and related modes

of blockchain governance. We do this by looking at a number of case studies which highlight a number of governance design issues as well as unintended effects of the technology and related design choices. We are exploring the linkages between blockchain application properties and related design options and choices.

Extended abstract.

Blockchain arose from the intention of creating native digital currencies. It originated online like many Free and Open Source Software (FOSS) projects: with an idea shared publicly and early prototypes developed by volunteers. Despite its origin, blockchains escape the main tenets of current theories about online organizing. So, we need to take a step back and look at those conceptualizations.

Information infrastructures opened up for a very successful mode of organizing, which is well-exemplified by FOSS and Wikipedia. This mode of governance has been labeled 'bazaar' and relies upon nearly zero marginal cost of reproduction and distribution of information goods, which are -as a consequence- 'non-exclusive' (i.e. one's use does not exclude anyone else's). The bazaar's peculiarities lay in its mode of production, usually referred to as 'commons-based peer production' (CBPP), and the prominence of free participation and reputation above other rewarding mechanisms.

The radical openness that this mode of governance exploits in practice and celebrates in theory questioned copyright and the mode of production and distribution it entails. So, it originated disruptions in a number of industries, starting with music. Despite the democratic allure of those stances, it has to be noted that they provided advantages to the emergence of the contemporary IT oligopoly to the extent it relies on free access to software and data and re-organized software developers' work (Parker, Van Alstyne, & Jiang, 2016).

Against this background, our research problem is that the 'bazaar' does not explain essential peculiarities of blockchain as an organizational technology. More specifically, blockchains authenticate each item from all its copies, which are not all the same any more. Thus, each item is unique, therefore 'exclusive' (i.e. one's use prevents others'). Blockchains achieve that through distributed consensus, which needs cooperation of the majority of participants and generates scarcity of the items it authenticates. In turn, scarcity triggers rivalry between actors longing for a limited number of tokens. The consequences of this peculiar arrangement are evident by considering the consequences of forking a blockchain. The new 'forked' ledger may use the same software, but the authenticity and value of the items it records are not the same.

Even though they are far from disappearing, permissionless blockchains have been battered by substantial governance problems. The need for more effective governance tools can take the shape of more sophisticated blockchains that predefine the rules of future changes. An alternative, which is discussed here, is letting consortia-based blockchains to retain some ad-hoc decision-making powers to cope with the inevitable unpredictability of future situations. This mode of governance differs from the bazaar without falling back into existing idealtypes of governance like market, hierarchy, or network. Hanseatic governance is characterized, we argue, by:

a) partial delegation of typical organizational functions like consensus and authentication to technology,

b) need to anticipate and negotiate early on in the consortium building and development process the known, and possibly unknown, scenarios ahead of the initiative,

c) traceability and reliability of the records, especially when they exceed specific organizational domain or jurisdiction.

1. Introduction

Destroying a hard disk is not the same as burning money. Files can be copied back easily, money does not have backup copies. Online, all data used to be the same, there is no inherent difference between original and copy. Since reproduction and distribution of information goods have nearly zero marginal cost, scarcity of data has been a non-issue. In other words, information goods are non-exclusive, one's use does not exclude everyone else's. This is a root cause of both major transformations of industries, starting with music, and novel organizational forms like Free and Open Source Software (FOSS) and Wikipedia. The inherent difficulty of containing data replication and distribution made information technologies effective in reducing transaction cost, but also ill-suited to provide money, which must be non-counterfeitable (thus inherently exclusive), without an external guarantor. Over the decades, especially in the domain of 'Digital Rights Management', attempts to re-introduce authentication into digital environments have been pursued through chips, digital certificates of different sorts, and designated organizations issuing and guaranteeing them. While those efforts have been useful for formal organizations adopting IT and fencing their digital networks, not least because they have to rely on recognized legal entities, the internet remained the realm of abundant and uncertified data. The novelty introduced in this domain by blockchain is the distributed mode of authentication vis-a-vis certification authorities with own mechanisms of accreditation and auditing. So, one may see webpages (or remixes on YouTube) at one extreme of the spectrum of freedom, Wikipedia as an instance to distributed and moderated content production. FOSS is more stringent, at the very least because it has to run, blockchains can be placed at the opposite extreme of webpages to the extend their tokens are authenticated. In other terms, we see a gray scale that covers from pure information goods all the way to transaction records.

The blockchain circumvents non-exclusivity of information goods and brings exclusivity and scarcity via native authentication into the digital environment. It proved digital scarcity viable by making transactions public and by letting the 51% of computing power (there are alternatives) authenticate transactions through a hashing algorithm (Bitcoin uses SHA-256) run by so-called miners. This means that a blockchain provides a unique and immutable ledger whose integrity is protected by a combination of technical and governance designs. Those ledgers locate each and every item and differentiate it from any other at any point in time. So, they can record transactions (of financial exchanges or supply chains, for example) or registries (vehicle records and cadasters are considered in this article). In practice, it makes no sense to copy items out of the blockchain that authenticates their validity. It would be like handwriting '100 Euros' on a piece of paper hoping to buy something with it.

Cryptocurrencies like Bitcoin proved at scale blockchain functionalities, which introduce non-replicability into digital environments through distributed authentication. The organizational counterpart of authenticity is both cooperation to keep the system as a whole running reliably, and rivalry between actors longing for a finite number of tokens or authenticated records. The capacity of authentication, defined by consensus algorithms and sealed continuously by miners, is relevant for governance purposes because it introduces a sense of togetherness due to shared interest. This is different from other information goods (like music or software) and the peculiar 'bazaar' governance (Raymond, 1999) (Demil & Lecocq, 2006) that they brought about through recent decades. Thus, since blockchains embed organizational functions like consensus and authentication, they can be seen as an instance of organizational technologies as distinct from other information technologies deployed for organizational purposes.

Against this background, identifying the features of this emerging mode of governance, which we later discuss as 'Hanseatic', is the overall objective of this paper. After presenting cases from the blockchain domain, we discuss them proposing the analogy to the Hanseatic League, which dominated trades and governance in Northern Europe for centuries. It was a confederation of fairly independent cities when nation-states had not consolidated yet; it was driven by guilds and aimed at facilitating and defending trade through alliances before the Rule of Law became hegemonic across Europe. In short, we place our interest in governance and distributed ledgers against the broader background of changing relations between formal organizations and large information systems (information infrastructures), and we argue that the analogy of a mode of governance that predated modern states captures relevant aspects that pass unseen adopting existing conceptualizations. Narrowing it down to an exploratory research question, our focus is on: How is blockchain governance different from the governance of Free and Open Source Software (FOSS), often referred to as 'bazaar'?

The rest of the paper is organized as follows. First, we define our theoretical background in relation to FOSS, its bazaar mode of governance and commons-based peer production (CBPP). Then, we highlight why native authentication brings something new and relevant to the digital environment. The paper continues by describing the research methods used for different empirical cases considered. These are, firstly, the Bitcoin scaling and the Decentralized Autonomous Organization's (DAO) governance problems. Secondly, two cases of coalition-based blockchains are examined: a distributed ledger to address information asymmetry in the second-hand car market and land registries. Those cases are then analyzed regarding their applicability to the cornerstones of 'Hanseatic governance', which is then discussed against established modes of governance.

2.   Literature review

Since design and practice often differ substantially (Ciborra, 2000), we searched for literature about blockchain, organization, and governance with a specific interest for blockchains in actual use, rather than for publications outlining the potentials of this new architecture. Empirical studies remain sparse, so our selection criterion left us with a relatively small number of works to consider: not least because of the long-time cycle of implementing IT, studying them, and going through peer-review processes, we could not find much academic literature based on studies of actually implemented and blockchains used in real-life settings. Consequently, despite our keen intention of differentiating between speculations about the potentials of blockchain and actual uses, it was often difficult to discriminate between what was aimed at by designers and researchers from what was happening in practice (Grover, Kar, & Ilavarasan, 2018).

In recent years, Bitcoin first and blockchains later have attracted wide-spread interest (Swan, 2015). Computer scientists have been first movers to approach this emerging phenomenon and proposed many variants of the architecture concept outlined originally by Nakamoto (2008). Nakamoto's problem for creating a purely digital currency was enabling unique identifiers, like the URL for example, without relying on any organization, like the ICANN. Solving this problem would have allowed a peer-to-peer cash system out of the 'protection' of formal organizations, which were seen as enemies in the cyberlibertarian culture where it originated.

It has to be noted that rights-protected information goods have been an area of research and economic interest at least since copyright became an issue. For what concerns digital goods, digital certificates were tried. They were always managed by certifying organizations in charge of their accreditation and auditing. Sometimes, certificates were paired to microchips soldered directly into the hardware. Implementing and enforcing these

mechanisms has repeatedly proven precarious because of technical, organizational, and even legal vulnerabilities. Those initiatives and research lines are only marginally considered here because crypto-currencies and blockchains come from a different context. Nonetheless, their distributed mode of authentication might end up in having an effect where other initiatives failed.

We proceeded as follows. Scientific publications, practitioner's reports, and the interview data were fed into an iterative sense-making process: the authors coded and conceptualized the information individually. Codes were initially seeded by using concepts characterizing established governance mechanisms. These individually gathered insights were then discussed by all authors. We also exposed immediate results and sought for input from the Coding Value research project. This input was then used to revisit the data and further develop our concepts. This iterative approach was finished when theoretical saturation was reached.

To date, Morabito (2017) offers the most exhaustive overview of the state-of-the-art of blockchain in organizations. The salient applications presented therein are Coinbase, Everledger, Factom, eHealth, electricity management, and finance. Those cases were useful for us navigating and putting into perspective materials about the actual implementations we found, and to decide what to concentrate on empirically. Interestingly, the blockchain architecture is believed to fit into widely diverse domains in terms of scope or transactional volume: from land registries to supply chain management systems, from intellectual property right management to money transfers and payments. In all those domains, the incumbents are intermediaries or third-party guarantors, which the blockchains aim at substituting. Overall, Morabito (2017) warns about the risks of privatizing state functions through blockchains as they contribute to "a process of undermining public institutions, the superiority of economics

over politics, and the change of citizens into customers (…), which perpetually empowers markets to the disadvantage of citizens", which is in line with Atzori (2015).

Walsh et al. (2016) conducted a literature review to gain an overview of blockchain characteristics, a necessary step to define blockchain types. Key blockchain characteristics are: level of permission, restriction of public access to data, modes of consensus, modularity, scalability, interoperability, and anonymity. Four possible and distinctive types emerge: Decentralized/Extensible (Bitcoin), Decentralized/Inextensible (Counterparty), Centralized/Extensible (Ripple), and Centralized/Inextensible (R3). Empirical investigation is expected to uncover a number of operational issues associated with different types, e.g. issues of governance, political aspirations, control, risk and resistance to change from those continuing to use traditional systems. Scholz and Stein (2018) foreground the organizational aspect of blockchain and aim at showing specific novelties in comparison to other types of organizations.

We grouped other contributions according to their focus on public services or private sector. From the former, a case study in healthcare by Ekblaw, Azaria, Halamka, and Lippman (2016) analyze MedRec, a system that gives patients a comprehensive, immutable log and easy access to their medical information across providers and treatment sites. Leveraging a blockchain, MedRec manages authentication, confidentiality, accountability, and data sharing, all of which are crucial considerations when handling health data. In the private sector, the most developed domain appears to remain finance, not least because of the investors and general public's attention that cryptocurrencies attracted. Morisse (2015) surveys 42 papers about cryptocurrencies in terms of methods, concepts, and approaches and finds that cryptocurrencies had not reached IS research, at least in 2015. The work by Du, Pan, Leidner, and Ying (2018) is particularly interesting for their attempt to conceptualize the differences between the affordances that blockchain offers and what actually happens during a

blockchain implementation in a FinTech context. Studies on security were also receptive of this emerging phenomenon. Herbert and Litchfield (2015) research the application of property rights in the case of blockchain-based software piracy prevention. Karame, Androulaki, Roeschlin, Gervais, and Čapkun (2015) analyze the probability of double-spending on the Bitcoin blockchain and claim that the current Bitcoin log does not provide sufficient information to provide satisfactory accountability, which would facilitate to blacklist malicious nodes.

3.   Theoretical framework

This section is articulated in three parts. After an outline of IT governance, the 'bazaar' mode of governance is detailed together with its peculiar mode of production, called Commons-based-peer-production. Despite their common origin, blockchain cases present a different governance mode because authenticity is central and miners and users have a heavier influence on constraining software developers' freedom.

The unconstrained data abundance that information infrastructures provide has been disrupting industries for several years. Internet companies not older than 20 years like Google and Amazon have taken center stage and become IT multinationals with the greatest capitalizations and societal impact. More central here is that open information infrastructures originated new organizational forms that Raymond (1999) first, and Demil and Lecocq (2006) later, labelled 'bazaar'.[1] Rather than formal organizations, referred to as 'cathedrals', online

---

[1] Regarding terminology, this article uses 'form of organization' and 'mode of governance' interchangeably. This is not only due to the literature of reference, which oscillate between the two terms (Demil & Lecocq, 2006; W. Powell, 2003), but also to our broad understanding of organizing, which underpins both. Following Czarniawska (2014), we understand organizing as a process that is broader than organizations, which are a relatively structured and stable way of organizing.

Regarding the concept of power, to which governance is clearly related, we understand it as the ability to get others to behave as they would not. This definition allows to see power also where no direct command and control can be exercised. This relational definition of power

organizing resembles a bazaar, where atomized individuals organize on the basis of merit and reputation. David D. Clark, an early internet architect, captured this mode of governance with a slogan that has become famous: "We reject: kings, presidents, and voting. We believe in: rough consensus and running code." Remarkable successes of this form of organizing, also referred to as 'commons-based peer production' (CBPP) (Y. Benkler, 2006) originated FOSS (Coleman, 2012) and Wikipedia (Jemielniak, 2014) (Aaltonen & Lanzara, 2015). The enthusiasm for the openness that the internet has allowed has been huge, it has questioned and eroded the centrality of formal organizations in organizing societies, and originated numerous and sometimes influential concepts like the 'wisdom of the crowds' (Surowiecki, 2005), 'open innovation'(Chesbrough, 2003), 'the wealth of networks'(Y. Benkler, 2006), and 'generativity' (Zittrain, 2006).

Bitcoin first, and other blockchains in subsequent years, originated from the same bazaar mode of governance, which relies on globally distributed technical skills, privacy concerned actors, rejection of corporations and states. However, blockchains develop differently from FOSS because miners and users, who maintain and rely on the blockchain, diminish software developers' freedom of taking the technology where they like. For these reasons, the bazaar does not explain blockchain-related governance. We contend that the bazaar misses a) significant consequences of digital organizing in general and b) blockchain-related governance in particular. Regarding the former, bazaar's advocacy for openness has overlooked a far-reaching and unintended consequence of its own principle. On one side it is undeniable that removing restrictions to access and distribution of software and data have reduced the cost of acquiring the means of production in the networked environment (Lyytinen & King, 2006). On the other side, what was not obvious to openness advocates is

---

includes different modes of organizing like markets, networks, hierarchies, or bazaar, and accounts also for powerful forces like prices, agreements, social norms, contingencies, hype, charisma, etc.

that FOSS, and user-generated data, have facilitated enormously the emergence of the contemporary global IT oligopoly. For example, a multinational corporation like Facebook does not need to pay for the FOSS it relies upon heavily, nor for data, which users generate. So, theories that captured very neatly the *zeitgeist* of the internet bazaar of the 90s and 00s, lack concepts to foresee – if not to thwart – the massive centralization that network effects produce online, and internet companies bank upon. In short, many more people can now produce data and software outside of stringent profit logics (Yochai Benkler, 2016). However, the bazaar governance lacks explanatory concepts and normative tools to anticipate and perhaps prevent the rise of large platforms that exploit openness, thus dominate the digital economy. Openness and decentralization do not necessarily go hand in hand.

Against this broad background, blockchain re-introduces scarcity where abundance has become taken-for-granted, and opens a prospect for different rules and coalition-based governance. Bitcoin was the first blockchain that tested at scale a rewarding mechanism for keeping faceless and globally dispersed actors complying with its rules of authentication. For such reason, blockchains are peculiar and interesting for governance: they promise to scale easily when they reach a critical mass, but they are difficult to manage because of lack of both formal organizational structures and clear boundaries to police. Major governance problems, which we exemplify later by discussing the Bitcoin blocksize conflicts and the failure of the Decentralized Autonomous Organization (DAO), prospect two ways forward: more governance 'on-chain' and permissioned/consortia-based blockchains. Since the former are still in their inception stages, this paper focuses on the latter and relies on cases from the second-hand car market and land registries. Before going there, the bazaar and the related commons-based peer production (CBPP) need to be described in greater detail.

3.1. IT governance

First, we explored how blockchain relates to existing studies about IT governance. The premise is that governance rules and mechanisms are subject to design. Typically, they are embedded in an institutional structure, which ensures their enforceability and provides mechanisms for conflict resolution. The institutional structure comprises technical and organizational forces (e.g. platform, electronic market, permissioned blockchain, laws, rules, etc.) and can be a business model (Riemer, Gogolin, & Klein, 2005).

The term IT Governance has been used since the early 1990s (Henderson & Venkatraman, 1993) and became more prominent later in the decade with the works by (Brown, 1997) (Sambamurthy & Zmud, 1999), while IT projects grew in complexity. IT infrastructures developed into stable components of organizational IT portfolios (Peter Weill & Broadbent, 1998), thus were suitable for strategic planning. Later, IT governance was defined by (P. Weill & Ross, 2004) as the framework for decision rights and accountabilities to encourage desirable behavior in the use of IT. In P. Weill and Ross (2004) framework, political idealtypes are used to describe how people in the enterprise make key decisions. Their quite articulated conceptualization is very precise, thus inflexible, to apply to blockchains, especially when they are used by 'crowds' or across organizations. Constantinides and Barrett (2014) offer a rich case of governing the information infrastructure of a health care system as collective action, which may be extended beyond the boundaries of a hierarchy like a public service.

In both permissionless and consortia-based blockchains, the influence of actors in the position of exercising decision rights is curbed because consensus is automatized and distributed. Still, one may say that decisions are displaced rather than abolished, for instance to the design of blockchain consensus algorithms. While this is undeniable, there are no unequivocal and unanimous rules or procedures of governance (a clear example is the never-

ending unruly conflict about Bitcoin block size presented below). So, to understand blockchain and governance, we need to move to theories that account better for what happens when consensus and authentication play a role that did not exist in the bazaar.

The book by Musiani, Cogburn, DeNardis, and Levinson (2016) looks at social and political sciences to account both for the elusiveness to control that the Internet and the services based on it showed to traditional decision makers, and for new ways power is being exercised through IT. In sum, the spectrum of positions about IT and governance is wide and spans from traditional managerial command and control approaches to international anarchy. Such diversity suggests that there are basic differences about the understanding of what IT are, and how to govern (through) them. For now, we turn briefly our attention to a classic debated of organization studies, hierarchy vs. market, in order to introduce and problematize the 'bazaar governance' (Demil and Lecocq 2006). In the discussion, those issues are expanded upon.

According to Williamson (1975) "governance is a means by which to infuse order in a relation where potential conflict threatens to undo or upset opportunities to realize mutual gains". Williamson (1975) core theoretical stance is that transactions entail uncertainty about their outcome, due to the bounded rationality and opportunism of agents, so its cost discriminate between market and hierarchy we the most suitable governance mode. Malone, Yates, and Benjamin (1987) stress how IT may favor markets more than hierarchies. W. W. Powell (1990) picked on this dichotomy and argued that market logics might operate within hierarchies (incentives, for instance) and hierarchies onto markets (sub-contracting). Then, he proposed the network as a new form of organization, which is most suited to domains where measurements are difficult, and trust among parties has a paramount role. According to Demil and Lecocq (2006), none of these modes of governance suits well the online organizing that FOSS exemplifies.

First, we continue our theoretical framework by introducing the bazaar as a mode of governance that was inspired by FOSS and its peculiar Commons-based-peer-production. Then, we conclude our theoretical stance by problematizing the explanatory power of those concepts for blockchain-related phenomena.

3.2. The transgression of online openness: Bazaar

Especially from the 90s onward, the idea and practice of sharing software code freely, thus impeding its trade as a property, was against all the received wisdom of product management, and the business model of software multinationals like Microsoft. Despite that, FOSS mode of governance proved so effective that it became exemplar for open distributed networks. Its successes resonate in the main tenets of the bazaar as a form of governance and of the Commons-Based Peer Production (CBPP), which we present in the next section.

The FOSS literature has explored different aspects of this mode of organizing. Main foci have been: motivation and incentive (typically addressed based on voluntary work and reputational benefits), protection of the commons against overuse and vandalism, emphasis on the creativity that commons licenses allow. Besides its positive effects (facilitating pro-social dynamism, creating social welfare), unintended effects emerged (in particular free riding and appropriation for commercial purposes other than software trade).

This mode of digital organizing that originated FOSS transgressed basic principles of established modes of governance. Because of its substantial difference, the study of Demil and Lecocq (2006) proposes to add a fourth governance idealtype, named 'bazaar', to W. W. Powell (1990) tripartite categorization of governance forms. Their work, empirically grounded into FOSS production, found that Powell's threefold characterization was not satisfactory to explain the then booming phenomenon of FOSS, and by extension the information economy.

FOSS took a hegemonic position over the internet not only by ignoring much of the received wisdom about IT governance, but also projecting the possibilities of open collaboration beyond software development. For instance, Wikipedia or voluntary geographic information with OpenStreetMap (and user-generated content more broadly) have shown that formal organizations are not the only way of getting things done; consumer electronics and open internet services have replaced business technologies in leading the ways of innovation; crowdfunding has unveiled the blindspots of traditional investors' preferences.

The bazaar mode of governance takes its moves from the non-appropriability of digital data, protected by open licenses, which allow unrestricted access to the source code so to prevent anyone from profiting from software ownership. Based on those principles, Stallman (2002) started the free software movement in the 80s. He advocated against regulating software through existing copyright laws and proposed the 'copyleft', which uses existing intellectual property rights to prohibit anyone from owning software code, thus maintains it as a public good. Rather than principles of fairness, higher organizational agility and software quality were the arguments put forward against proprietary software by the cognate open source movement. Despite spats and tensions between them, free software and open source (commonly grouped under the umbrella term of FOSS) gave a great impulse to the rise of the internet. Detractors claimed that without economic incentives to trade software, and the hierarchies to manage its development, FOSS would have failed. Instead, it thrived with an organizing mode that Raymond (1999), who developed Fetchmail (a FOSS email client), likened to a 'bazaar' as opposed to the 'cathedral' of software corporations. Starting with the popularization of the internet, especially with the World Wide Web, this utopic vision of non-scarcity has become commonsensical. On the internet, everything has been expected to be 'free' as in 'free speech' and as in 'free beer'.

Following the more articulated theorization of the bazaar by Demil and Lecocq (2006), the non-appropriability that open licenses guarantee reduces the transaction cost of FOSS substantially. The consequent governance mode is an 'architecture of participation' which provides non-financial incentives for contribution and protects the outcome from 'vandalism': by giving their software away – thus trusting openness and transparency – developers build up their reputation, which in turn they can spend providing assistance on the software they know (Shaikh & Henfridsson, 2017). So, the bazaar operates at an aggregated low level of control on actors' behaviors, not least because – having full access to source code – anyone can always 'fork' their software and develop it their own way.

Since FOSS licenses are viral, forking reinforces the commons by spreading it rather than diminishing it. So, FOSS generates limited polarization of public vs. private compared to the long-lasting debate around the 'tragedy of the commons'. As discussed at the end of the next section on CBPP, the problematic unintended consequences of FOSS is that it facilitated monopolistic businesses (like global platforms) which rely heavily on software without commercializing it, thus not breaking its rules nor vandalizing it. The same ease of forking is not there with blockchains because, even if the software can be used elsewhere freely, the authentication that miners provide and users expect would not be provided by the new ledger, like the handwritten 100 euro banknote. This difference is central in our overall argument and will be expanded upon after the section on CBPP.

3.3. Commons-Based Peer Production

Yochai Benkler (2016) stresses that in the CBPP, the core institutional feature is the fact that anyone can use and repurpose the resources on symmetrical terms, without requiring permission from any single property owner or administrator. This is the institutional framework that allows access to and use of resources in the distributed, self-directed form typical of the bazaar. Organizational governance and managerial resource and task definition

and allocation utilize combinations of participatory, meritocratic (do-ocracy) and charismatic, rather than proprietary or contractual models. In other words, tasks are not assigned but picked up by volunteers without coercion in a "diverse, uncertain, complex project space". Collaboration results to be based on self-organizing rather than explicit coordination.

Under conditions of diffuse and low capital requirements (i.e. means of production are cheap and widely available) and highly modularity of tasks (low interdependency), CBPP showed comparative advantages for innovation over more traditional modes based on cathedrals or pure markets. Understanding this organizational innovation requires an explanation of the advantages that loosely-coupled networks of diversely experienced and motivated individuals have over firms or markets as innovation and knowledge production models. CBPP is characterized by:

- highly distributed low-cost means of production (computers and communication networks),

- easy access to information, including software, due to copyleft and nearly zero marginal cost,

- globally dispersed and available human capital.

The combination of those elements has been allowing to cope with projects whose high complexity and uncertainty would have driven both plan-prone hierarchies and profit-seeking traders away. The following figure places CBPP at the forefront of innovation when diversity of knowledge and uncertainty are high.

In sum, the main governance innovation of CBPP is its confluence of technological, organizational and institutional innovations. CBPP allows diverse individuals, who would not have been able to communicate and coordinate in advance, to explore collaboratively an opportunity space made of resources, problems, people, and potential solutions, self-assign

and harness their tacit, creative, or otherwise hard-to-communicate knowledge or facility. These loosely-coupled networks can identify or contribute to defining a problem or solution, and they can do so relying on diverse, often non-monetary motivations that do not incur into the limitations imposed by the need to formalize and standardize their insights, efforts, or experimental successes for transmission into formalized channels of markets or hierarchies (Provan & Kenis, 2008).

Advocates and commentators of the CBPP have been aware also of the vulnerability and precariousness that the commons are exposed to. An inherent weakness of this mode of governance are rogue actors, private organizations, or even governments themselves, finding loopholes, undermining, circumventing, or destroying regulation or changing them in their favor. There is another issue which is worth stressing here because it offers a theorical view onto the re-introduction of scarcity into the digital environments that blockchains allow.

Despite its extraordinary successes, it is important to stress that the openness on which the bazaar and CBPP are based upon does not necessarily result in open and democratic consequences, and this is not only because of the vandalism their advocates use to be concerned about. Here the reference is to the emergence and consolidation of the IT oligopoly, which diminishes both business and consumers' freedom. As a matter of facts, multinationals (and 'cathedrals' in general) could and do use FOSS freely without having had to develop it, nor to have paid for the high risk of innovation by absorbing the costs of frequent failures. They can do that while complying with the copyleft when they use FOSS because platform multinationals do not make money out of software trade. Nonetheless, they remain the main beneficiaries of the availability of high-quality and free software, so much so that they are main contributors to the Linux Foundation. Comparing extremes, a minuscule minority may have gained the freedom to run and tinker with Linux on their PC, but datacenters run the same free operating system to monetize billions of users' data. In practice,

cathedrals can sit back, look at what emerges successful from global crowds' constant trial-and-errors, and cherry pick what to adopt. Thus, long-term and large-scale FOSS implications appear to differ from its micro-intentions and principles. Unrestrained participation turns to mean 'participation of the fittest', paraphrasing Darwin.

To conclude the section on the bazaar and its unique mode of production, the celebrated openness of information infrastructures, where there is always an elsewhere where commons-based peer production (CBPP) can grow, has not posed any relevant obstacle to the emergence of monopolistic platform companies that rely on free availability of software and data, without trading software itself. Thus, they remain indifferent, or even support, the viral nature of open licenses while profiting from its quality and convenience. So, the defense of openness does not prevent the winners from taking most if not all, while the rest is free to experiment on the fringes, swallowing energy drinks and (pipe-)dreaming of being the next winner. Raymond proved right in recognizing that the bazaar can work very effectively and efficiently. However, the theoretical and practical consequences of this mode of governance need scrutiny. Rather than furthering the study of unintended consequences of the bazaar openness, this paper looks at blockchain initiatives, which reverse the tide of non-scarcity that the bazaar floated upon. Blockchains come from the CBPP milieu, but also bring remarkable differences. The organizational characteristics of CBPP are: i) decentralization of conception and execution of problems and solutions, ii) harnessing of diverse motivations, including non-monetary motivations, and iii) separation of governance from property. The last one is relevant to focus on because it is the main difference from other FOSS projects. As described previously about the bazaar, the copyleft does not allow appropriation of software. So, bazaar governance is the open-ended outcome of actors building their reputation while remaining under low control and incentive pressures. Blockchains instead, allow property of tokens, enforce incentives, thus exercise a certain control on all parties involved. This is expanded upon in the following section.

3.4.   Using and transgressing the bazaar: trusting authentication without authenticators

We keep the description of blockchain architecture to the minimum needed for the argument. The main originality of this architecture is that it allows authenticating items without relying on a designated actor responsible for it. For Bitcoin, the largest blockchain in existence, this happens by making all transactions public and letting all the nodes of the network (miners) to certify each transaction. A transaction is authenticated by the 51% of computing power available. As a result, on a blockchain, copies are not all the same as they used to be.

Blockchains are based on consensus mechanisms translated into algorithms for mining, which protects integrity of transactions and ledger. The operational and technical governance mechanisms (roles, rights, obligations, incentives) have been designed by individuals or (designated) providers/ owners of blockchains. The integrity of individual instances of blockchains is subject to the quality of the design. Despite usual claims about trustlessness, use of blockchains always requires users' trust into institutions and/or systems (especially in permissionless blockchains where institutional safeguards are missing).

The intended effects of blockchains are: facilitating peer transactions without institutional support (e.g. financial system, state institutions), peer control without government oversight, availability of smart contracts for enforcing integrity. Side effects need not be overlooked, especially for what concerns the progressive monopolization of mining, and the incomplete (smart) contracts, which will be exemplified later in the DAO case.

Against the background of non-scarcity that the bazaar openness guarantees and the CBPP depends upon, the major innovation introduced by blockchain - and proved viable at global scale by Bitcoin - is distributed authentication to avoid both double-spending and reliance on external guarantors. Authentication is here intended in its basic meaning of

certification of genuinity, i.e. each of the limited number of tokens in existence can be traced back to an owner at any point in time. This means that, although most blockchain software is open source, thus it would fall under the bazaar governance mode, tokens' authenticity, thus blockchains' value, depend also on miners and ledger's users. This digitally native way of authenticating digital items introduces exclusivity, thus scarcity and rivalry. So, it constitutes a qualitative shift from the abundance of information goods.

In other words, money is not data, even if it is digital. If at some point some open source web browser users are dissatisfied with the software, they can decide to fork the code and develop an independent version to fit their own and new users' preferences. When this happens, users of both versions maintain the capacity to use their software for most if not all web browsing purposes. This is not the case with blockchains, whose main purpose is to guarantee the authenticity of the data they collate. When a fork takes place, data on the forked ledgers may differ, and the expected immutability be undermined.

Adoption of blockchains comes with the trust, or at least the assumption that algorithms can govern organizational relations. Along this line, Lustig and Nardi (2015a) investigate how Bitcoin's algorithm has gained authority and legitimation in allowing new trades. In this sense, algorithms are discussed as a way of directing human activities by defining what to rely upon. They criticize, like Dodd (2018) does, the emic views of people promoting Bitcoin for their naive assumptions about technological neutrality and independence from allegedly corrupted politics. A similar approach can be seen in the discussion on blockchain-based state governance (Atzori, 2015; MacDonald, Allen, & Potts, 2016).

Even if we agree that algorithms are not neutral in transforming human behaviors, organizations, and societies, we find that a narrow focus on algorithms does not account for novel aspects that blockchains bring to the fore when compared to the bazaar: authentication

is guaranteed by miners and legitimized by users. These two types of actors pass overlooked by a narrow focus on algorithms. In practice, if we consider only algorithms, we would not see much difference between blockchain software, and blockchain in actual use, which authenticates its records. The constitutive role of miners and traders beside software developers makes blockchain a relevant instance of organizational technologies as distinct from information technologies. Especially the centrality of consensus making and maintenance sets blockchain design, development, deployment, assessment, and evolution apart from technology that only compute and transmit information while leaving consensus to organizations. In short, governance cannot be conceived as an add-on topic but needs to be considered as constitutive of blockchain.

Studies that tackle governance issues explicitly, often discuss issues related to jurisdiction, which is often uncertain because blockchains shift responsibility for the authentication of transactions from recognized guarantors to allegedly independent miners, or other consensus mechanisms, which can be located outside of formal organizations and jurisdictions' reach. This makes those dispersed actors not easy to hold accountable. As a consequence, legal uncertainty in transactions increases. A way to mitigate this uncertainty are so-called smart contracts, envisioned as a layer on the top of blockchains. They gained popularity, yet rose controversy. For example, Maurer and DuPont (2015) reflect on the applicability of smart contracts and their relationship to law. They claim that distributed, autonomous, and self-executing contracts may not be feasible due to their non-contractual basis. Indeed, traditional contracts reduce uncertainty by committing all signatories, who remain subject to the Rule of Law. Thus, since blockchains may exceed jurisdictions, they can fall in the cracks between inconsistent regulations. We consider smart-contracts in relation to the case of the Decentralized Autonomous Organization (DAO), whose failure exposed the limitations of a governance conceptualization that pursues the possibility of creating complete contracts, thus sidelining people and institutional context's role. In sum, the consequences for

governance of blockchain-based authentication are studied against the limitation of the bazaar organizing.

4.   Methods

Initially, as typical for exploratory research (Stebbins, 2001) (Briggs & Schwabe, 2011), we used all available sources to uncover interesting phenomena. To derive appropriate concepts to describe them, Langley (1999) offered a particularly helpful guide for 'quantification strategy' (foregrounding of events) and 'temporal bracketing'. Specifically, we reviewed the still scarce, but rapidly growing body of work for reports on blockchain governance, alongside scanning more than six hundred sources for related materials collected by the research project Coding Value, as well as research databases and search engines such as Scopus, Web of Science, and Google Scholar among others. We utilized various search strings consisting of 'blockchain' and 'governance' to ensure wider coverage of research domains, such as organizational and social sciences.

The empirical part of this study comprises two parts: the first is about two exemplar governance crises that blockchains encountered in their evolution: a) the conflicts about Bitcoin block size (an apparently simple technical issue with far-fetched consequences), and b) the failure of the Decentralized Autonomous Organization (DAO), which showed the risks of assuming the possibility of 'complete contracts'. The second empirical part is grounded in cases that adopted a consortium-based approach to avoid the governance problems that Bitcoin and the DAO manifested.

The Bitcoin block size and DAO cases were easy to select because they have been very hotly debated in the global crypto scene because foundational aspects like transaction costs and smart-contracts were at stake. For the Bitcoin and DAO cases, we have conducted two extensive documentary studies. Since both were public events, meaning that they happened on the open internet, direct observation was possible on selected channels like

Twitter, Reddit, public repositories and the specialized press that was following those events closely.

Our focus on consortium-based blockchain is the result of long-term engagement in interorganizational systems and a large design science research project dedicated to improving the used car market. The consortium developing and deploying a distributed ledger for the second-hand car market is studied through participant observation in the frame of design research. While all authors are well-aware of the progress of this research project, two authors have prominent roles in it and have been documenting it extensively. Design and deployment of a distributed ledger to make information about second-hand cars more reliable required to gain an extensive overview on the state-of-the-art of blockchain projects. This allowed to narrow down the key aspects that the following case-studies should highlight: relevance of blockchain in low-trust environments, prominence of record immutability, governance of access rights, and modes for modifying those rights.

Those same aspects were considered in the selection of other significant consortium-based cases. We reviewed existing research with empirical components, Then, we searched online for active and promising initiatives, and we focused on blockchain application of land registries because they offer an original angle on trust, immutability, access, and governance more broadly. Of the many initiatives we found, we analyzed 126 blockchain-based companies from a variety of online sources like Crunchbase and Coindesk for their governance characteristics. Identifying relevant cases has proved a difficult task because of the novelty of this domain and the hype that wraps it. Indeed, there are countless startups, initiatives, GitHub projects, but few running implementations, which also causes empirically grounded research to be scarce. On the basis of what read in papers, practitioners' reports, grey literature, specialized press, blogs, etc. we shortlisted five cases in three continents to

focus on. This meant going deeper in a documentary analysis of the grey literature and interviewing prominent actors of those initiatives.

5. Loss of innocence: no 'complete contracts'

The empirical section is articulated in two major parts: the first presents two major governance crises that affected the two main blockchains currently in existence: Bitcoin and Ethereum. Those ruptures made deeper functioning and risks visible. The second part presents consortia-based blockchains, which prospect a viable alternative to the shortcomings of assuming the possibility of automatizing governance.

5.1. Bitcoin scaling crisis

Let us consider the most prominent blockchain to date: Bitcoin. Attributed to its growing rate of adoption, Bitcoin's number of transactions increased. As a result, the blockchain eventually started manifesting bottlenecks in authenticating all transactions in a timely fashion. Since its underlying protocol fixes Bitcoin's throughput (transactions handled per time unit), developers proposed various modifications to solve imminent scaling problems. These were supposed to recover Bitcoin's prospects to be used as a global electronic cash and micropayment system. However, none of these solutions has so far been broadly agreed upon, and in retrospect, this so-called scaling debate repeatedly plunged the community into crises.

At the core of the scaling problem, there is Bitcoin's 1MB block size limit. It was initially set in 2010 by its anonymous founder, Satoshi Nakamoto[2], aiming to prevent attackers from launching denial-of-service attacks by creating large blocks that would cripple validators and thereby the network. This parameter has not been changed since, although

---

[2] Git commit: https://github.com/bitcoin/bitcoin/commit/a30b56ebe76ffff9f9cc8a6667186179413c6349#diff-118fcbaaba162ba17933c7893247df3aR2614

Bitcoin's developers publicly recognized the imminent scaling issues shortly after the limitation's introduction. The reason for this dormancy is manifold: first, solving the scalability issue is only possible by amending Bitcoin's protocol, which is a delicate procedure and can, when failed, divide the network. Such changes are called 'forks', as they differently continue a shared transaction history as soon as the amended and incompatible ruleset is applied. Second, Bitcoin's security relies on the economics evoked by the protocol. It is thus not entirely clear which consequences entail when the parameter is changed. E.g., it is assumed that a too large block size would paralyze the network, bloat the blockchain, and increase costs required to run a node. As a result, power would be concentrated among a few validators, weakening decentralization, and lastly, decrease security. Lastly, multiple approaches were so far proposed; however, it seems not yet decided which one suits the community, its various players, and incentives best.

After the problem's identification, solutions and their impact have been openly discussed in mailing lists, forums and social networks like Reddit and Twitter. In 2015, these preparations brought forth the first remarkable amendment suggestions: Bitcoin Improvement Proposals (BIP) 100[3] and 101[4]. The former suggested to introduce a variable block size and the latter proposed to increase it from 1MB to 8MB straightaway. BIP 101 was first implemented by Bitcoin XT, one of Bitcoin's first hard-forks, which could after all not establish itself as the 'new Bitcoin'. Another fork, called Bitcoin Classic was created in response to XT's failing and aimed to set the block size at 2MB. At the same time, Bitcoin Unlimited emerged and allowed users to signal their preferred block size limit. Ultimately, none of these alternatives gained sufficient momentum, and the forks' node counts started

---

[3] http://gtf.org/garzik/bitcoin/BIP100-blocksizechangeproposal.pdf

[4] https://github.com/bitcoin/bips/blob/master/bip-0101.mediawiki

approaching zero[5]. Around that time, it started to become clear that the block size was going to have far-fetching consequences. In a nutshell, large blocks would make Bitcoin like global cash because they would increase volume capacity and reduce transaction cost, so to open the way to countless microtransactions (even finer granularity than current plastic money). Small blocks would make Bitcoin more like gold, something to hoard for its deflationary characteristic. Looking back at those days later, one may argue that this shortsighted turf war was a main cause of the bubble bust in 2018, when crypto had not reached a wide enough user base as cash, nor the safe haven perception that gold gained over millennia.

Bitcoin Unlimited developers started another more organized attempt and proposed Bitcoin Cash in May 2017. The fork was eventually created in partnership with Bitcoin XT's community the same year on August 1st. All previously named solutions depict hard-forks, meaning there is no backward-compatibility, which causes them to originate a transaction chain distinct from Bitcoin's. They furthermore need to be maintained by different miners, traders, and developers. An alternative and less strict solution to hard-forking came from the SegWit (Segregated Witness) soft-fork. Although it was initially proposed in 2015 as BIP 141 to solve an unrelated issue, namely transaction malleability, it also allows for more transactions within a block without increasing the actual block size, which is achieved by relocating the transaction's signature storage. The soft-fork has been activated by Bitcoin's miners on August 23rd 2017, and can since be utilized by any transaction on the Bitcoin network. Beyond its immediate effect on Bitcoin's throughput, the thereby introduced transaction malleability is regarded as a precondition for more sophisticated `off-the-chain' second-layer solutions, e.g., the Lightning Network. These allow for a virtually unlimited number of low-fee microtransactions and are therefore hoped to solve scaling problems. However, neither the soft- nor the hard-fork solution are generally accepted, proved, or

---

[5] https://medium.com/@WhalePanda/roger-ver-from-bitcoin-jesus-to-bitcoin-antichrist-69fc7a17c622

adopted, yet. To a greater degree, there is political competition, radicalization, and fight

between supporters of the two solutions, which is examined in the following paragraphs.

When in March 2017 both Bitcoin's average block size reached the 1MB size limit[6],

and the Bitcoin Cash fork was announced, the debate got heated once again and was even

feared to spark a 'civil war'. Since Bitcoin was reaching fresh all-time highs during this

period ($1.270 on March 6, up from $760 on January 6)[7], the discussion was particularly

relevant and the actors highly financially incentivized. The debate was mainly characterized

by two opposing groups, of which the Bitcoin Cash supporting faction argued that Bitcoin

was meant to be a low fee cash system at any time and thus needed to be amended right away.

They further opposed the planned activation of SegWit due to its algorithmic complexity. In

contrast, 1MB advocates were looking at Bitcoin as a 'store of value'[8] and was unwilling to

implement unproven changes. Instead, they looked to implement the well-researched and

lower-risk SegWit soft-fork later that year, which would serve as a basis for second layer

solutions like the Lightning Network. Both groups nearly religiously justified their goals and

means, interpreting Nakamoto's initial vision and Bitcoin's whitepaper as being supportive of

their respective goals.[9]

Being frustrated about the Bitcoin core developers' passivity, fork supporters, led by

the initiator Roger Ver, assumed that they were impeding change purposefully. Furthermore,

they stated the involvement of a Blockchain company, called Blockstream, to be the cause of

---

[6] https://www.blockchain.com/charts/avg-block-size?timespan=all

[7] https://coinmarketcap.com/currencies/bitcoin/

[8] https://www.coindesk.com/what-is-the-bitcoin-block-size-debate-and-why-does-it-matter

[9] This article lists what of the whitepaper has been adapted and what not: https://www.coindesk.com/what-bitcoins-white-paper-got-right-wrong-and-what-we-still-dont-know

this.[10] Since it funded both Bitcoin's development and simultaneously created own products that could have benefited from an imperfect network, there allegedly was a conflict of interest. Others regarded these as 'conspiracy theories'[11], solely arranged to justify the forking of the network. They further accused Ver of spamming Bitcoin's network to increase transaction fees, reduce its usability and poach users in preparation for the fork's launch. At this point, each side got repeatedly accused of manipulating and censoring social media to influence the upcoming forking event's outcome. Thus, heavy fights were staged on Reddit and Twitter, where forking efforts were commonly disregarded by discrediting Bitcoin Cash, e.g., by dismissing it as a scam and referring to it as `bcash'. This intended to deprive its namely relation to the initial chain, and to discourage investors by reducing its prospects of success. Roger Ver was further blamed of deploying 'sock puppets' to influence online forums' sentiments[12]. Despite both sides' dishonesty, Bitcoin Cash was successfully launched in August 2017 and reached a total market share of nearly 10%.[13] Thus, most users valued the original Bitcoin chain more. After its launch, Bitcoin Cash was the target of multiple unsuccessful spamming attacks aiming to paralyze the network.[14] The consensus' state was furthermore highly opaque during this time due to the attendance of hidden actors that contributed to the situation's complexity: investors' manipulation and speculation caused exchange prices not to reflect the networks' actual valuations, and members noted to 'not expect anything more [than making money] from this'.[15] Moreover, the outcome was significantly dependent on one more, purely financially motivated group that had decisive power over governance processes: miners. They earn block rewards and transaction fees in

---

[10] https://medium.com/@octskyward/on-block-sizes-e047bc9f830

[11] https://www.reddit.com/r/Bitcoin/comments/65a4z4/why_has_raising_the_blocksize_limit_become_so/

[12] https://www.reddit.com/r/Bitcoin/comments/87t3ot/delicious_proof_that_roger_employs_sockpuppets/

[13] https://coinmarketcap.com/charts

[14] https://ambcrypto.com/bitcoin-cash-bch-under-attack-individual-vs-investors/

[15] https://bitcointalk.org/index.php?topic=2040221.940

return for validating and maintaining Bitcoin's public ledger by authenticating and recording all transactions. Thus, miners were making money out of the high transaction costs granted by the status quo. However, some large mining businesses unexpectedly supported Bitcoin Cash, supposedly due to bribery as many users presumed on social media. Further consequences arising out of the debate's forks and their relatively high valuation are expressed by effects like the 'Forking Craze'[16]: many forks emerged as individuals recognized the simplicity of forking Bitcoin without adding actual improvements or technical know-how. This complicated any serious consensus making processes after that since actual proposals can hardly be distinguished from 'money grabs'.

5.2. The Decentralized Autonomous Organization

The Decentralized Autonomous Organization (DAO) was a social experiment in organizational governance. Its goal was to bring forth a decentralized and innovative business model, which would allow a group of investors to transparently, democratically and fairly fund collectively voted projects using the raised cryptocurrency capital. Being built upon Ethereum's smart contract feature, *The DAO* was the first of its kind. It has initially been proposed by a small blockchain venture, called Slock.it, and was created in close cooperation with its community and allowed various actors to get involved with the project's development process. This spirit of openness and decentralization helped *The DAO* to gain traction and success quickly.[17]

This visionary platform launched on April 30, 2016, after the closing of the to-date most successful crowd sale on May 28th. It raised approx. 14% of Ethereum's total currency supply and has been the largest initial coin offering (ICO) by then. Despite *The DAO*'s high valuation and its smart contract's rather compact source code, multiple programming flaws

---

[16] https://www.bloomberg.com/news/articles/2018-01-23/bitcoin-may-split-50-times-in-2018-as-forking-craze-accelerates

[17] https://blog.slock.it/the-history-of-the-dao-and-lessons-learned-d06740f8cfa5

existed within the launched product. These were identified and fixed by its developer in June of the same year. One error, however, went unnoticed and was exploited by an anonymous hacker on June 17th, who drained about a third of the enclosed funds. The thereby obtained funds were, because of technical failsafe methods, not freely withdrawable. Instead, the attacker had to initiate *The DAO*'s inbuilt mechanism of exiting the organization. This process, also known as the 'split-function'[18], would create a new child DAO solely comprising the withdrawing user's funds and thus allow the holder to create and approve a proposal to disburse the funds to an arbitrary address – for which the voting period of 28 days applied. This timeframe allowed for mutual consideration among the developers, users, and miners regarding the measures to be put in place. However, it quickly became apparent that this issue was out of *The DAO*'s control. Its smart contract had been executed accordingly to its design and credited to the idea of decentralization and 'code is law' principles, the contract contained no inbuilt measures to expropriate the hacker, who complied with the contract's rules and thereby, at least technically, obtained the funds legally. As a result, *The DAO*'s incident was only, if at all, to be solved on underlying layer, i.e., Ethereum's blockchain. The project's prominence henceforth put financial, media, and legal pressure on Ethereum's community to make an appearance and decide on the event's handling. The project's community, attributed to the idea of decentralized governance, vividly engaged in the decision-making process on open social platforms to contradictorily decide about a smart contract's repeal, which intends to autonomously and unambiguously adjudicate. The open discussion provides well examinable evidence of social consensus mechanisms and the case's prevailing sentiments, as will be displayed in the following paragraphs.

---

[18] https://blog.slock.it/the-history-of-the-dao-and-lessons-learned-d06740f8cfa5

https://github.com/slockit/DAO/wiki/How-to-split-the-DAO

Following the exploit, a group of *The DAO*'s and Ethereum's lead developers and community members teamed up quickly and convinced major exchanges to halt the native Ethereum's token (ETH) trading, which was the currency of the stolen capital. Simultaneously, white-hat counter attacks drained and secured the remaining funds, which by the community was perceived as them taking the 'role of fiduciary to *The DAO* and its members'. Having averted further and imminent threats, long-term strategies were discussed. These inevitably consisted of either ignoring and accepting the exploit or introducing changes to Ethereum's protocol, i.e., forking. These changes would either blacklist all the contract's outgoing transactions (for the attacker to be unable to withdraw stolen funds) or remove malicious transactions from Ethereum's supposedly immutable blockchain altogether. The former type of protocol change portrayed a solution in which past transactions would not have to be invalidated, i.e., a soft-fork. Although it depicted a middle ground, it had to be excluded from consideration due to technical impediments. Thus, two opposing main factions remained in this debate, namely such that called for an amendment, i.e. a hard-fork, and such that opposed any interference. Supporters of the latter persuasion argued that 'transactions are immutable and code is law'.[19] Expressed technically, there should never be a hack of the ledger because reversing the exploit would contradict both core beliefs and purpose of decentralization. Members of this sentiment considered any intervention a 'centralized bailout [of a] decentralized protocol'[20] and described *The DAO* as being 'too big to fail'[21]. Besides, the problem was not considered to be Ethereum's, but *The DAO*'s and so users blamed Slock.it for having produced a contract whose 'code was rushed [and its] governance weak

---

[19] https://www.reddit.com/r/ethereum/comments/4unpm3/the_dao_and_the_benefactors/

[20] https://www.reddit.com/r/ethtrader/comments/4oif5c/fck_this_dao/

[21] https://www.reddit.com/r/ethereum/comments/4oithy/a_too_big_to_fail_political_hard_fork_is_very/

and untested'.[22] By contrast, forking advocates regarded the proposed amendment to depict 'business as usual'[23], claiming[24] that fixing bugs within protocols has always been part of iterative development processes. These same people also argued that *The DAO* was well-known to be a 'highly experimental technology'[25], therefore wishing to quickly move on while memorizing the incident as a 'very expensive lesson learned'[26]. By arguing so, they framed the interpretation according to the bazaar mode of production and away from the authenticity and immutability aspect that blockchains are rooted in.

Ultimately, 'compulsory voting'[27], as one user put it, decided on the outcome. The process to vote on and identify the most supported solution was technically realized by miners submitting their hash power to the favored chain. The faction opposing the fork eventually turned out to be in the minority and blamed, among others, Ethereum's founder, Vitalik Buterin, for exerting his political clout in favor of an intervention. The presence of Ethereum's 'benevolent autocrat' became well visible in this situation, distinguishing it from Bitcoin and its anonymous founder who withdrew completely and appeared no more during debates to voice his well-respected opinion, letting factions fight flying the flag of his writings. One user voiced his view on the situation by concluding 'chancellor Vitalik on brink of first bailout for DAOs'; a comment that was even published on Bitcoin's blockchain.[28]

---

[22] https://www.reddit.com/r/ethereum/comments/4ostmj/the_dao_hack_a_lesson_in_true_decentralisation/

[23] https://www.reddit.com/r/ethereum/comments/4op69x/no_hard_fork_does_not_mean_dao_holders_lose_all/

[24] https://www.parity.io/attack-on-the-dao-what-will-be-your-response/

[25] https://www.reddit.com/r/ethereum/comments/4oiqj7/critical_update_re_dao_vulnerability/

[26] https://www.reddit.com/r/MakerDAO/comments/8b0xib/maker_weekly_discussion_april_9/

[27] https://www.reddit.com/r/ethereum/comments/4stiuh/dao_hardfork_implementations_almost_ready/

[28] https://btc.com/86f03176beef99ac2f5adecd39b964f874f5ec615a9d01e88ac781c6e669753c It is worth noting here that cryptocurrencies, characterized by deflationary tendencies (no one can arbitrarily increase the monetary mass, unlike banks), matured a deep resentment for bailouts and quantitative easing policies, which characterized the last decade.

Having introduced the hard-fork to undo the exploit, *The DAO*'s investors could reclaim their lost tokens. Although this solution was acceptable for the majority of stakeholders, some miners and users refused to acknowledge the new protocol and continued to apply the original rule-set. This inevitably caused the fork and induced a chain-split, dividing the project into two distinct branches. While the original blockchain is since referred to as `Ethereum Classic', the current Ethereum main chain is actually the forked one, not the original. Following this precedent and its obvious consensus-making difficulties, one user aptly wondered 'if there will ever be a consent on proposals with that many shareholders'.[29]

Altogether, a single project's failure, operating on an open platform, became a broader community's concern, forcing it into internal disputes and re-interpreting its core values: As no compromise solution was available, any decision would either lead to infringing Ethereum's immutability and thereby betraying decentralization's and its fundamental values, or losing valuation and the user's assets. One part regarded the outcome a 'legitimate community response'[30] and did not consider decentralization to imply being 'static, stupid or powerless against attackers'.[31] Others saw the tyranny of the majority in the voted solution the '[ending] of what Ethereum was always meant to be'[32] and considered the existence of this outcome evidence that soon 'money [would] be censored'[33], too. However, most of the fork opposers ultimately applied the new rule-set, understanding Ethereum to be a 'democracy, not technocracy'[34] in which 'all that matters is consensus'[35], even if executed algorithmically.

---

[29] https://www.reddit.com/r/ethereum/comments/4ihkld/the_dao_must_diversify/

[30] https://www.parity.io/attack-on-the-dao-what-will-be-your-response/

[31] https://www.reddit.com/r/TheDao/comments/4oisep/ether_safe_but_dao_cancelled_were_getting_a_refund/

[32] https://www.reddit.com/r/ethereum/comments/4oj7ql/personal_statement_regarding_the_fork/

[33] https://www.reddit.com/r/ethereum/comments/4oiib4/dao_is_safe/

[34] https://www.reddit.com/r/Futurology/comments/2bypb7/does_an_automated_society_still_need_humanrun/

[35] https://www.reddit.com/r/Bitcoin/comments/2fch11/would_you_argue_that_bitcoin_has_more_or_less/

5.3. More of the same: governance on-chain: 'code is constitution'

Considering the two previously examined cases of forkings, paired with the ease the bazaar can be swept by network effects, blockchain's main tenets need consideration beyond the easy enthusiasm that has characterized this emerging architecture. Parts of the technical community recognized early on the inherent power-accumulation issues of proof-of-work systems and started inventing alternative mechanisms. These were to spread decision-making equally among all actors and thus essentially set to establish a democracy on the blockchain. The consequential 'on-chain governance' systems extend the DAO's core idea by formalizing governance or voting rules at the protocol layer and thus enable all actors, i.e., validators, users and developers alike, to participate. Therefore, code moves one level deeper and becomes the quivalent of a constitution, according to which laws can be defined. These initiatives aim at avoiding the governance problems that block size and DAO exemplified without giving in the a return of more traditional and established modes of governance, based on human and discretionary decision-making.

Being among the first of its kind, the previously examined DAO showed close resemblances to on-chain governance by incorporating voting processes into its smart contract. Thus, *The DAO* is the predecessor of more recent on-chain governance efforts. Leveraging and extending the failed experiments' vision, the Tezos network was launched in early 2018. It aims at becoming a 'self-amending' cryptocurrency and to provide a platform which can be shaped by its users who can propose and vote changes to efficiently amend the network when needed, e.g., update algorithms or to patch vulnerabilities. Further extending this idea, Aragon aims to decentralize the creation and maintenance of organizational structures and lets its users easily create custom, private and transparent DAOs.

Elucidated by these project's visions, governance on-chain, i.e., scripted into the Blockchain's protocol, promises to disrupt traditional mechanisms as they finally allow for

large networks to be governed collectively, which has effectively not been possible before[36].

Such being the case, it might be argued that the newly enabled governance mode is one of

Blockchain's pivotal disruptive properties.

However, there are drawbacks and risks in designing such systems. To achieve on-chain governance, protocols are compelled to operate upon a 'one coin, one vote' policy to prevent sybil attacks, i.e., users who create multiple blockchain accounts to forge identities and thus voting power. As opposed to the democracy principle 'one head, one vote', these systems reward wealth with power and may rather be termed plutocracies, which entails serious hazards: bribery, cartels, low voter turnout, centralization. Ultimately, instead of attaining their goal of bringing people back into governing blockchains, on-chain governance systems, in their current state, may be pushing them even farther out. Furthermore, as humans can change systems they do not like, on-chain systems are still subject to forking, as e.g. happened to Tezos shortly after its launch. Hence, they may be said to inherit their predecessor's vulnerabilities due to the illusive possibility of 'complete contracts', and add new ones to them. In any case, since these are very early days of on-chain governance, which is like moving from 'code is law' to 'code is constitution', they cannot be studied in practice. Rather than speculating if they can bring or not more democracy, we focus on more advanced experimentations that rely on the establishment of consortia, which retain powers on the networks they sustain.

6.   Hanseatic governance: building coalitions

As anticipated, consortia-based blockchains aim at retaining the peculiarities of blockchain as a distributed architecture for authentication without the governance problems that hindered the evolution of permissionless blockchains. They aim at that goal with case-

---

[36] http://faculty.cbpp.uaa.alaska.edu/afgjp/PADM601%20Fall%202011/Modes%20of%20Network%20Governance.%202008.pdf

specific tailoring of access and authentication rights, allocation of responsibilities, reliance on existing jurisdictions and institutional contexts.

6.1.   The CarDossier

The main case we use to illustrate consortia-based blockchain projects deals with the used car market, where: a) good and bad cars are not easy to distinguish, thus worse cars drive better ones out of the market (Akerlof, 1978), and b) parties with better information are more likely to strike better deals. In other terms, information asymmetry is inherent to the used-car market. We were early on interested in how far blockchain's immutability may reduce information asymmetry between buyers and sellers, thus reducing the negative influence of 'lemons' onto the used car market. Consequently, when we applied for funding, we adopted an information management angle rather than an economic one. The sought effect might be a better market, but this was beyond the scope, and the time constraints, of our work. Our interest was how to manage information differently. We would not know if industry partners would welcome our project as we might affect existing business models. From a broader perspective, multiple actors in the automotive domain – especially used-car dealers – live off the mistrust and fragmentation of information sources. The former induces the latter: Even if the information is shared, one cannot assess its truthfulness easily because various 'truths' from various sources may circulate. In other words: traceability and authenticity of information, which blockchain provides natively, may reduce the current asymmetry of information.

The ability to make a good assessment of a car's value relates to the completeness and reliability of information about it. However, obtaining all car information can be a daunting endeavor. During the years long lifecycle of a car, numerous actors (insurances, repair shops, state agencies, and many more) are involved. They contribute to a long-term authentication process (comprising proof of ownership, repairment, insurance/driver's license validity) while

collaborating only to the necessary degree; this leaves all information about a car fragmented at best, which entices to opportunistic behavior. These information silos do not only exist inside of companies but also in the market. There have been many efforts to aggregate, consolidate, and commercialize car-related data. Alongside with AutoCheck and Carfax being the most prominent ones, numerous companies source data from dealers, DMVs, repair shops, or from car owners for compensation, thus profit from selling car history reports to end customers. While sourced data can generally be believed to be consistent, performed analyses and conclusions in forms of a report may vary as they are subject to company-specific measures and interpretation. Besides, these platforms generally are not accountable for the provided data's accuracy. To which platform should end customer turn their attention? What if data of one platform conflicts with another? The secondary market of car-related information resembles a bazaar, which undermines the overall reliability of information not least because these platforms create a data abundance which leaves buyers uncertain. In practice, it became apparent that creating a more consistent and reliable record of cars would have required the coordinated effort of many actors. In the following, we inspect a solution that strives to overcome some of these challenges.

The CarDossier is a Swiss-based project initiated in early 2017 which aims to develop a platform for car-related data and has been funded by the Swiss commission of technology and innovation. It is being run by a coalition of major stakeholders in the Swiss automotive market: The biggest importer and repair shop of cars, a major insurance, a road traffic agency, researchers, a mobility service provider, as well as legal and IT experts. These founding partners were motivated to build a platform that opens up a multi-sided market for digital information goods where private as well as corporate actors monetize their data upon provision and usage, rather than giving it away for free as per the current dominant business model of global online platforms. One core use case certainly overlaps with Carfax's and AutoCheck's car history reports. Going beyond this use case, having truthful data accessible

to others allows the digitization and automation of tedious, repetitive, and error-prone activities (e.g. Collecting, authenticating/sealing, sharing documents) nowadays conducted manually and inefficiently. For another, and maybe even more importantly, the overall reliability of data is considerably higher as companies would contribute to and rely upon one source for data for in-house processes, which diminishes parts of inconsistent information silos. Unreliable data for in-house processes has been confirmed by our project partners to be one of the main driver for their part-taking in this consortium. Hence, initial business cases were clear very early on, quite differently from the bazaar governance that leaves those reflections for later stages.

The CarDossier coalition comprises organizations of all points of the value chain, as well as competitors. While the project advanced, governance challenges became prominent. Interestingly enough, this does not hinder the belief in the prospective gains of the platform. One major challenge referred to the coordination of interests and a subsequent agreement on core collaboration traits. To stabilize the coordination of these, as an anchor on known (legal) grounds, and as the first point of contact in case of conflicts, the CarDossier coalition founded an association to provide a clearer point of reference for governance of the shared platform. Rather than expecting to be able to anticipate the details of future relationships between actors, thus develop on-chain governance, as the believers in complete contacts would do, this coalition agreed on an association's statute (pact) comprising core rules such as membership rights and obligations, the association's purpose, fee structures, and thereby serves as a playbook for a novel application domain to defend and facilitate the trade of (novel) goods. If conflicts emerge in the future, standard societal and legal modes of conflict resolution would apply. One may object that this choice limits innovation potential, but participants decided to build on the existing institutional context, which is conceived as an enabler rather than an obstacle to innovation. For instance, a cantonal traffic authority weighted in to instill credibility into the project since its inception.

With an agreed-upon common understanding, decision rights became central. Within the association, all major decision rights are taken at the association's board meetings. Their demands are translated into system requirements and then developed and enacted by a third-party platform provider. Members (also private actors) are allowed to propose and discuss changes to the system. The weight of each one's vote varies. For the first two years, to develop the core of the platform and to make the platform running, the coalition of founding members keeps 51% of overall voting power, while joining partners earn voting amounts corresponding to their investments with fixed minima and maxima. After the initial phase, votes will automatically be weighted via smart contracts upon defined criteria, such as prior voting participation, financial contribution, data contribution, reputation, and many more. This way, platform participants are incentivized to participate and earn influence in return, which formalizes one's contribution to the platform. Instead of giving a fixed amount of votes, we aspire to achieve this way a fairer variable distribution of votes. What's more, by facilitating to make voices heard, decision-making, as well as decision enforcement, social consensus is achieved on blockchains; especially decision enforcement distinguishes the CarDossier from other bazaar projects as forking is not an option.

While the previous measures aimed at internal coordination activities, also contextual awareness has shaped our action. Legal experts and state authorities inhere pivotal roles to this endeavor as major challenges lay on the legal and regulators' side. E.g., in the beginning, the coalition planned to found a for-profit legal entity to pay respect to the trade of data and the revenue it entails. Eventually, the coalition opted for a non-profit association for several reasons, with one being central: A for-profit legal entity would draw similarities to other platforms such as Facebook or Google, with the primal goal of profit maximization rather than participants' diverse interests. For example, the CarDossier heavily relies on the participation of private actors such as car owners to obtain information which otherwise would be unavailable; they have to feel sure that their data is in safe hands. Another reason is

the participation of state agencies and other public institutions in the platform, as well as the integration of their processes, which is substantially eased if conducted through an entity with no primal profit interests. Finally, the participation of the latter is crucial as it instills trust into the association in the eye of everyone, and by this may increase data reliability.

Alongside with the character of the legal entity, data privacy emerged as a defining problem for the coalition, especially for the choice of the technological platform. Personal and car-related data cannot be distinguished easily from each other. While the sharing of the latter is generally harmless, the former is quite sensitive, and heavily regulated, especially by the GDPR. Since drawing the line between the two is not straightforward, the system has had to be designed compartmentalizing different kinds of data to be legally compliant. A first proof-of-concept built on Hyperledger was disregarded because of this matter: Distributing all data to all participating nodes, even if encrypted, proved not viable for our project. Encryptions weaken over time which would require regular re-encryption. Furthermore, as all data is shared, the association would have no mean to terminate local data usage as every participant would manage a full node independently. The CarDossier coalition, together with regulators, IT as well as legal experts, therefore decided to move in a joint effort to the so-called R3 Corda platform, a distributed ledger technology (DLT). In a nutshell, data is merely shared and persisted between participants of a single transaction and not distributed to all. Not only does this allow for a significantly higher transaction throughput, but it also allows for easier compliance to data security regulations as the GDPR, which took effect in May 2018 in the European Union. The GDPR grants individuals the right to require the deletion of, simply speaking, personal data. This contradicts the immutability property of blockchains. On our Hyperledger prototype, this would have meant hard-forking and re-encryption upon every single deletion request. Corda proves viable in this regard, as data is effectively considered deleted when participating parties discard their transaction.

The CarDossier not only provides a single source for car data, but also immutable, shared, and agreed upon functions in forms of smart contracts. The aspired efficiency gains tackle rather linear inter-organizational processes with pre-defined outcomes; the assessment of those outcomes also needs to be based on pre-set and agreed characteristics. One example of a scripted process refers to the rules of data access management. These rules are inscribed in smart contracts and vary per role (a role represents an actor in the ecosystem); a role merely sees data which it is allowed to see. A role can further inhere rights to perform specific functions, such as issuing an electronic vehicle registration document (road traffic agency) or the insurance certificate (insurer). These smart contracts, same as seen in the case of *The DAO*, come with the promise of completeness; the functions of control and supervision of these are thereby inscribed in the protocol and displaced from external guarantors.

Concluding, establishing a market for authentic information does not come easy. Its shape and functioning are not only endogenous of the coalition, but also exogenous, to the extend existing businesses, regulators, and public opinion are seen as a resource rather than an obstacle to innovation.

6.2. Blockchain-based Land Registries

When the blockchain hype hit the shores of other application domains, the land registry domain emerged as a promising use case for blockchain systems as noted in the World Economic Forum early on Hutt (2016). Blockchain-based land registries come with the promise of overcoming several of the challenges of this complex and multi-stakeholder (land-owners, brokers, notaries, banks, and state agencies) inter-organizational setting with far-fetched ramifications in all parts of economy and society. The processes of authenticating rightful land ownership and the rightfulness of a land ownership transfer vary vastly among countries, but several commonalities are observed: They can be considered slow, sparsely digitized, often opaque, costly, and embedded into a very low trust environment. Because of

its high valuations at stake, not least for its use as collateral, land registration is heavily exposed to fraudulent behaviors which have been particularly problematic in developing countries (De', 2005; De' & Sen, 2004). Especially in developing countries, the considerably high costs contribute to a high percentage of land left unregistered, up to approximately 78% in Ghana (Kshetri, 2017).

Most of those records are paper-based, which have provided an acceptable level of longevity and reliability, generally speaking. It comes as no surprise that mostly, but not only, developing countries put a particular emphasis on this matter. Land tenure is indeed seen as a basis for further economic development, including financing through collaterals. However, there is empirical evidence for the contrary as paper-based documents can be altered, deleted, or lost: E.g., when a devastating earthquake hit Haiti, many land records were destroyed. This incident caused not only a wave of land ownership disputes lasting until today, but it also hindered other, essential processes such as the reconstruction of lost sites (Moloney, 2010). Not only natural catastrophes endanger the reliability of records, but also political instability, corruption, fraud, or, in extreme cases, invasions. Fraudulent renting, expropriations, extortion, and bribery are similarly well documented as corruption in dealing with governmental or notary third parties. This is not to say that blockchains would overcome all these challenges, neither can it help in verifying land titles – but it may ease these and thereby increase the reliability of records by digitizing records as well offering a tamper-resistant, decentralized database[37]. However, this effort cannot be pursued in isolation because the system would not overcome common reasons for failure, like corruption. Its potential might be fulfilled when several parties collaborate for data longevity and share the audit of data and

---

[37] Reese, F. 2017. "Land Registry: A Big Blockchain Use Case Explored," CoinDesk, , April 19. (https://www.coindesk.com/blockchain-land-registry-solution-seeking-problem, accessed November 26, 2018)

actions (Ziolkowski et al. 2018) - Land title oversight and management needs thereby to be displaced from single entities to a coalition of stakeholders.

As for efficiency gains, a blockchain system promises to decrease costs and time spent dramatically; the same could hold true for the transparency and reliability of records. On a blockchain, both costs could be reduced to no more than 0.05-0.10 USD per transaction (Kshetri 2017). From a temporal perspective, the processes of land registration or transfer might be conducted within minutes instead of days or months (Nimfuehr 2017). In the following, we inspect two cases of blockchain-based land registries in more detail, namely in Georgia and Honduras. We believe these cases cover the essential traits of other blockchain-based land registry systems as well, like those we studied in Sweden and Ghana. All of these cases officially announced projects to store and transfer records of land ownership via blockchain which we started to observe very early on. It is remarkable, how over time other states, cities, or regions announced to pilot blockchain-based land registries as well, such as Vermont in the USA, Dubai, Kenya, Ukraine, UK, Andhra Pradesh in India, Russia, Japan, as well as Brazil.[38] While most of these are prototypes in early stages, we believe our observed cases to consider the most matures ones.

---

[38] - Zuckerman, M. J. 2018. "Vermont's Pilot Program Completes First US All-Blockchain Real Estate Transaction," Cointelegraph, , March 8. (https://cointelegraph.com/news/vermonts-pilot-program-completes-first-us-all-blockchain-real-estate-transaction, accessed December 4, 2018).

- Hochstein, M. 2017. "Dubai Land Department Launches Blockchain Real Estate Initiative," CoinDesk, , October 10. (https://www.coindesk.com/dubai-land-department-launches-blockchain-real-estate-initiative, accessed December 4, 2018).

- Mwathane, I. 2018. "MWATHANE: Blockchain Technology: Are Kenya's Land Registries," Daily Nation. (https://www.nation.co.ke/oped/opinion/Blockchain-technology/440808-4749098-tras4j/index.html, accessed November 27, 2018).

- Tian, C. 2017. "Ukrainian Government to Start Blockchain Land Registry Trial in October - CoinDesk." (https://www.coindesk.com/ukrainian-government-to-start-blockchain-land-registry-trial-in-october, accessed December 4, 2018).

- Das, S. 2017. "Japan Could Place Its Entire Property Registry on a Blockchain," CCN, , June 22. (https://www.ccn.com/japan-place-entire-property-registry-blockchain/, accessed December 4, 2018).

Case 1: Georgia

"The economist Hernando de Soto told us that only one third of all people can prove they own their land. Apart from the legal uncertainty, there is $ 20 trillion in dead capital, as land with unexplained legal titles cannot be sold. So, we told him, 'Find us such a country and we bring the land register to the Blockchain for free. And that was Georgia." Marc Taverner, BitFury

Indeed, nowadays merely 15-20 % of the overall land is registered in Georgia[39]. Geographically, Georgia lays between Russia and Turkey while bordering the Black Sea. Its population amounts to 3.7 Million citizens and is concentrated mostly around its capital city Tbilisi. Historically, Georgia was part of the Soviet Union with small periods of independence. Following the fall of the Soviet Union, Georgia regained its independence which preserved ever since.

Merely 15 years ago, Georgia found itself on rank 127 out of 133 in the Corruption Perception Index, next to Cameroon and Tajikistan (CPI 2003). In 2017 Georgia managed to obtain rank 46 out of 180, placing itself next to Spain and Malta (CPI 2017). This is to say that reliability, transparency, and integrity of public services were and are pivotal to Georgia's

---

- De, N. 2017a. "Indian State Partners With Blockchain Startup for Land Registry Pilot," CoinDesk, , October 10.

(https://www.coindesk.com/andhra-pradesh-partners-with-chromaway-to-develop-blockchain-land-registry, accessed November 26, 2018).

- De, N. 2017b. "Russia's Government to Test Blockchain Land Registry System," CoinDesk, , October 20.

(https://www.coindesk.com/russias-government-test-blockchain-land-registry-system, accessed November 26, 2018).

- De, N. 2018. "UK Land Registry Begins New Phase of Blockchain Research Project," CoinDesk, , October 5.

(https://www.coindesk.com/uk-land-registry-begins-new-phase-of-blockchain-research-project, accessed December 4, 2018).

- Mendes, K. 2018. "Can Blockchain Save the Amazon in Corruption-Mired Brazil?," Reuters. (https://www.reuters.com/article/us-brazil-property-blockchain-idUSKBN1FE113).

[39] Graglia, M. 2017. "Tbilisi Agreement Heralds Significant Expansion of Blockchain to Manage Property Registries," New America. (https://www.newamerica.org/future-property-rights/blog/blockchain-for-property-rights-georgia/, accessed December 4, 2018).

recent efforts which led to a wave of investments and reorganizations that made Georgia a progressive country in digitizing public services; due to their efforts, Georgia gained the 4th place worldwide in ease for Registering Property[40]. Despite these efforts, there was still room for development, and one of the most promising use cases to be expanded relates to the Land Property Rights Management. Associated actors, such as banks, notaries, and Georgia's National Agency of Public Registry (NAPR) are loosely coupled and cannot trace processes amongst each other, mistakes occur, and they are costly to correct, also for citizens. Furthermore, relating to the spirit of earlier day's corruption, all NAPR servers are centralized, and data can hence (1) easily be modified upon ones liking or, in extreme cases (2) destroyed by physical force by misbehaving actors. The control of the Land Property Rights Management, and therefore its reliability, is thereby centralized at the state's level. This centralization poses a risk. In the extreme case of an invasion, which is less remotely possible than for countries in other circumstances, invaders could overtake the control on land titles and alter land ownership without the possibility to retrace changes or even regain its original state. This risk is particularly alarming when reviewing Georgia's political past: The last war with Russia (Russo-Georgian War) dates merely ten years back; less than four years ago, Russia annexed Crimea, which is only across the Black Sea from Georgia. NAPR employees have mentioned all of these as a motivation in their recent effort to build a blockchain-based land registry[41]. However, Georgia cannot make this effort itself. To overcome these challenges, especially regarding geopolitical risks, Georgia sought and found a solution which we detail below.

---

[40] World Bank. 2018. "Rankings," World Bank. (http://www.doingbusiness.org/en/rankings, accessed December 4, 2018).

[41] Shin, L. 2017. "The First Government To Secure Land Titles On The Bitcoin Blockchain Expands Project," Forbes. (https://www.forbes.com/sites/laurashin/2017/02/07/the-first-government-to-secure-land-titles-on-the-bitcoin-blockchain-expands-project/, accessed December 4, 2018).

In 2016, the NAPR started a project together with Bitfury, a company specialized in blockchain platform development, for a blockchain-based land registry. Their primal goals have been to digitize and facilitate transacting in registering and transferring land ownership. In a first phase, around 1.3 Million paper-based records of land ownership have been digitized and imported into a private and permissioned blockchain.[42] This phase has been completed successfully in 2017. Relying on the digital version of all records, Bitfury implemented a set of smart contracts for the process of buying and selling land which aims to replace the previously manually conducted authentication processes which regard the second and ongoing phase of development. This innovation tackles an important issue: The exchange of money and land ownership does not coincide, and parties find themselves waiting months for one or the other; in extreme cases, they find out after months of waiting that their request could not be processed due to errors. The set of smart contracts aims to synchronize payment and land ownership transfer. These payments are thereby also insured by the Georgian National Bank, which holds 40-45% of Georgia's real estate market. The smart contract's functioning is currently piloted and, whenever a transaction is conducted, an entry is made on both the concurrent as well as the blockchain system.

Besides the decrease of transaction costs in the land registry or transfer by avoiding costs associated with hiring and dealing with legal authorities, blockchain systems are also expected to increase the reliability of records. The main issue, which too often is conflated with immutability, is how to certify data quality before it gets on the immutable ledger. In Georgia, the NAPR is responsible for data entry to the system, which requires trust in its reliability. For the sake of transparency, the NAPR foresees two measures: firstly, it allows parties to access the ledger, which contains all historical data, and thereby to control the well-

---

[42] Snip, I. 2017. "Georgia: Authorities Use Blockchain Technology for Developing Land Registry | Eurasianet." (https://eurasianet.org/georgia-authorities-use-blockchain-technology-developing-land-registry, accessed December 4, 2018).

functioning of the system (banks, notaries, NGOs, and later also citizens). Secondly, its own blockchain is concatenated with another one to implement a backup function: The state of the ledger is backed up to the Bitcoin blockchain in the form of a hash at specified points in time through a digital time-stamping service.[43] This method offers a proof-of-existence and serves as a checkpoint to prevents fraudulent tempering of past transactions; the Bitcoin blockchain thereby assures a given state of the land registry ledger at a given time. Interestingly enough, this may open up a new legal dimension as it may decouple claims on land ownership from its local jurisdiction, which may prove helpful when records are in doubt; local authorities would not help, Georgia's system fails to work, or, in extreme cases when the state is overtaken.

The governance of Georgia's land registry is organized in collaboration with several parties and the NAPR. Although their blockchain system is technically consensus-based, the NAPR is leading the effort while holding major decision rights, among other things on system design, data authenticity, and access control. This principle is also reflected in the technical architecture: Transactions are validated solely by the NAPR, while other parties hold so-called auditor nodes. As of now, auditor nodes are planned to be given to banks, notaries, as well as NGOs – all together, hence, share the oversight of the system (Ziolkowski et al. 2018). As the gatekeeper to the system, the NAPR effectively steers the in- and outflow of participating actors. The NAPR further can exclude unwanted actors or reverse fraudulent transactions, which downplays blockchain's decentralization principle. Indeed, the NAPR imposes its decisions onto others, which is remarkable for blockchain systems which are rooted in the rejection of authorities. As major decision rights are centralized at the NAPR's, its governance might point towards a hierarchy, in which transacting agents follow a formal

---

[43] Shin, L. 2016. "Republic Of Georgia To Pilot Land Titling On Blockchain With Economist Hernando De Soto, BitFury," Forbes, , April 21. (http://www.forbes.com/sites/laurashin/2016/04/21/republic-of-georgia-to-pilot-land-titling-on-blockchain-with-economist-hernando-de-soto-bitfury/, accessed May 18, 2017).

line of authority with bureaucratic procedures, which are partly automatized. However, auditor nodes allow for a level of transparency, thus accountability to avoid abuses.

Case 2: Honduras

Honduras is the second largest country in Central America bordering with Guatemala, El Salvador, and Nicaragua.[44] Its population amounts to 9.2 Million citizens. The overall economic situation can be characterized by a high unemployment rate and an unequal distribution of income.[45] Furthermore, land ownership is distributed unequally with a high concentration in a few private hands, while 60% of land titles are left undocumented.[46] The latter is left to several kinds of disputes, such as conflicts, displacement of indigenous groups, and fraudulent appropriation of land (Chavez-Dreyfuss 2015). As an example, an audit performed in 2015 by the Honduran government found over 712 irregularities in property registrations, 466 of which were of related to fraudulent acts (Collindres et al. 2016). What is more, misappropriation of land ownership became common (Benbunan-Fich and Castellanos 2018; USAID 2018). In a similar vein, merely 15 years ago, Honduras found itself on rank 107 out of 133. In 2017, Honduras remains on rank 135 out of 180.

The low percentage of rightful land title coverage is not to say that land ownership was unknown but handled rather informally, e.g., via oral agreements (Nelson 2003). It became a priority for the government to resolve this issue so landholders could rightfully defend their claims. But Honduras' issues in the land market were rooted deeper: Lack of complete land information, uncertain validity of land titles, as well as inefficiencies regarding cadastral malfunctions (Benbunan-Fich and Castellanos 2018; Nelson 2003). Conclusively, Honduras lacks an integrated land registry; while there are various property registration

---

[44] Nelson, R. T. 2003. Honduras Country Brief: Property Rights And Land Markets, p. 44.
[45] Benbunan-Fich, R., and Castellanos, A. 2018. Digitalization of Land Records: From Paper to Blockchain, p. 9.
[46] Chavez-Dreyfuss, G. 2015. "Honduras to Build Land Title Registry Using Bitcoin Technology," Reuters. (https://in.reuters.com/article/usa-honduras-technology-idINKBN0O01V720150515).

offices there is little effort for aggregated views (Nelson 2003). There have been previous attempts for land registry improvement by digitizing records and storing them in a centralized database. These efforts fell short to several issues, e.g. unauthorized changes due to carelessness or corruption or even duplicated land titles (Benbunan-Fich and Castellanos 2018). From a cost perspective, registering land in Honduras nowadays takes six procedures over 22 days with costs approximately 5.7% of the property value (Collindres et al. 2016), which places Honduras on rank 95 worldwide in ease for registering property (World Bank 2018). In consideration of these facts, the idea to modernize the country's land registry with a distributed tamper-proof blockchain database was born. Honduras was among the first-movers for evaluating a blockchain-based land registry system for their use; the recognition of local problems and their efforts to overcome these has been reflected with associated publicity, covered inter alia by NASDAQ, Forbes Magazine, and Estrategia y Negocios. The Honduran-Factom partnership improved the country's image worldwide (Collindres et al. 2016).

In stark contrast to Georgia's rather short history of its cadastral system, entries in Honduras' cadastral system date back to the 1880s. This is to say that the reliability of these paper-based records is endangered by theft, arson, or misuse (Collindres et al. 2016). Consequently, the backup of these entries has been considered a pressing issue. This use-case quickly became a central in their line of thought when the Honduran government initiated talks in January 2015 about a potential blockchain-based system with Factom, a Texas-based blockchain startup (Benbunan-Fich and Castellanos 2018). For another, the blockchain has been viewed as an effective means to aid the local judiciary by providing verifiable and precise audit trail to hold criminals accountable; this is particularly important as under Honduran law, public documents (granted by public institutions) inhere a presumption of good faith – they are valid unless stated otherwise (Collindres et al. 2016). As corruption in Honduras also has also roots in public institutions, there were few means to come by so far.

It is important to note that these talks followed an amendment of the Honduran constitution to decentralize governance, comparable to states within the US. This amendment led to the creation of new Zones for Employment and Economic Development (ZEDEs) and following its reorganization, common standards had to be developed (Collindres et al. 2016). Therefore, in March 2015, representatives of ZEDE as well met with a Committee for the Adoption of Best Practices (CAMP) where Factom presented a blockchain-based solution to overcome cases of corruptions in the concurrent land registry system.

Factom's proposed solution would maintain a layer on top of the Bitcoin blockchain with time-stamped records (Lemieux 2016). These records would either represent land ownership or land transfer, with proof of existence, proof of process, and proof of audit (Lemieux 2016). As with every blockchain implementation, data input is crucial and goes beyond Factom's implementation; Factom's solution merely preserves what has been given as input, e.g., owner of a parcel, parcel size. The entry point of data, hence, must be defined as a trusted third party such as a notary, which grants a land title. To record land ownership on the blockchain, the land title has to be scanned where meta-data is retrieved and sent to three individuals for cross-checking. Upon agreement on the displayed information, the land title is forwarded to be stored on-chain – in the case of disagreement, the process returns to land title registration (Benbunan-Fich and Castellanos 2018; Lemieux 2016). Putting land title registration out of the hands of single entities promises to overcome individual weak links in organizations, which may overcome corruption. Land title registration thereby becomes a collaborative effort.

As Benbunan-Fich and Castellanos (2018) found, the negotiations for piloting a blockchain-based land registry started shortly after the ZEDE meeting, followed by a signed Memorandum of Understanding and a non-binding letter of intent. The pilot was supposed to be developed for the fourth largest city La Ceiba. However, ever since project inception, the

Honduran Government was reluctant to talk publicly about the initiative, which, as later was commented by officials, was due to the release of confidential information to the public. In 2016, the first news displaying political difficulties in the implementation of the project became public (Anand et al. 2016), which was then confirmed by Factom's CEO (Factom 2015). The project quickly became controversial among political parties, which caused it to stall. It remained stalled during and after the Presidential elections in 2017.

7.   Discussion: Scripta volant, Signata manent

A Latin proverb declaims: 'verba volant, scripta manent'. Literally, it translates 'spoken words fly away, written words remain'. Since the Romans, information technologies changed. So, this proverb needs an update to capture the authenticity that the written word used to have before the inflation it suffered in recent decades: 'scripta volant, signata manent', which means 'written words fly away, sealed words remain'.

So far, we argued that the blockchain architecture originated from the need of avoiding double-spending, i.e. duplication of data, without putting any formal organization in charge of this intermediary authentication. The origin of this decentralized mode of authentication followed the process of many other Free and Open Source Software (FOSS) projects: a concept is shared publicly (Nakamoto, 2008) and early prototypes are developed by volunteers. Despite its beginning, blockchains escape the main tenets of bazaar mode of organizing, which is rooted into FOSS. This motivated us to: a) spot the differences, b) show exemplar cases of governance difficulties of major blockchains, c) describe how consortia-based blockchain are circumventing those difficulties. Throughout the rest of this document, those differences are discussed against established conceptualizations of governance.

Information infrastructures opened up for a very successful mode of governance of which FOSS and Wikipedia are glaring examples. Their 'bazaar' mode of governance relies upon licenses that protect the nearly zero marginal cost of reproduction and distribution of

information goods. As a consequence, those information goods are non-exclusive because one's use does not exclude anyone else's. While the prominence of free participation and reputation above other rewarding mechanisms have been pinpointed, little has been put forward regarding how this way of governing innovation has favored the emergence of the contemporary IT oligopoly, to the extent it relies on free access to software and data.

Against this background, our research problem has been that the 'bazaar' does not explain essential peculiarities of blockchain as an organizational technology. Lustig and Nardi (2015b) pose special attention onto algorithms as defining aspect of Bitcoin, whereas we argue that ledger's maintainers and tokens' users characterize the governance of blockchain as much as the stakeholders it affects. Indeed, beyond software development, the authenticity of the ledger is what maintainers guarantee and users rely upon. Authenticity is not a straight product of algorithms (incidentally, it should be noted that many previous digital certificates were technically sound) but a sustained long-term effort that all involved parties contribute to and depend upon. Beyond software developers, miners (or whoever maintains the ledger) and traders (or whoever uses the tokens for the most diverse purposes) gained a prominent role in governance.

In other words, blockchains authenticate each item from any copies, which would not be all the same any more. Each item is unique, therefore 'exclusive' (i.e. one's use prevents others'). Blockchains achieve that through distributed consensus, which needs cooperation of the majority of participants and generates scarcity of the items it authenticates. In turn, scarcity triggers rivalry between actors longing for a limited number of tokens. The consequences of this peculiar arrangement balancing cooperation and competition are evident by considering the consequences of forking a blockchain. The new 'forked' ledger may use the same software, but the authenticity and value of the items it records is not the same. We

have illustrated those problems and rationales through examples of actual forks of the major blockchains in existence: Bitcoin and Ethereum.

Even though they remain the biggest and possibly most influential ones, permissionless blockchains have been battered by substantial governance problems, which have hampered them. The need of more effective governance might take the shape of more sophisticated blockchains that predefine the rules of future changes, so to avoid the kind of conflicts demonstrated by Bitcoin block size conflicts and DAO reversal. These efforts rely on so-called 'on-chain' governance. Even if in principle they are possible, little has happened in practice, yet. So, we have focused on the alternative, which is consortia-based blockchains. Coalitions of actors, rather than trying to foresee future situations, then designing possibly suitable modes of governance based on incentives and algorithms, retain a certain level of ad-hoc decision-making powers. This discretionary power, coupled with the reliance on the existing institutional context, allows them to cope with the inevitable unpredictability of future situations.

This mode of governance, which we call 'hanseatic' is characterized by:

a) partial delegation of typical organizational functions like consensus and authentication to technology,

b) need to anticipate and negotiate early on in the consortium building and development process the known, and possibly unknown, scenarios ahead of the initiative,

c) traceability and reliability of the records, especially when they exceed specific organizational domain or jurisdiction.

To introduce those characteristics more in detail, we first need to discuss our cases against established conceptualizations.

Both FOSS and blockchains rely on a higher level of publicity of actions compared to more traditional modes of organizing like hierarchies or markets (Williamson, 1975). FOSS keeps the software code public to improve its quality while minimizing transaction costs. The centrality of copyleft as a peculiar kind of contract and the focus on transaction cost are insufficient to explain how blockchains relate to the public and use openness. In particular, a certain rivalry among participants coupled to trust in the reliability of the system as a whole (forking is more damaging than in normal FOSS projects) are more prominent. Interestingly, this reminds of Simmel's definition of money as 'a claim upon society'. Let us leave aside, for the time being, what 'society' stands for here. Actors in bazaars and blockchains gain the capacity of making claims in very distinct ways: in bazaars reputation is of paramount relevance whereas blockchains provide a less disputable a more scalable anchor: tokens which can stand for something else, and cannot be tempered with. So, legitimacy of its mode of authentication is central.

Blockchain mode of authentication marks a central difference from FOSS. FOSS and blockchain may share origins in the creative ways of CBPP, but the value of an authenticated token depends on more than software. Miners and users, as all cases showed, have a heavier weight than in FOSS when it comes to give legitimacy of what is on a blockchain and its value. Anyone can run a Bitcoin software, but only nodes on the main blockchain can trade on that price (or other values for different applications). The others do not enjoy the same level of trust and legitimacy. More precisely:

- While in FOSS projects the majority cannot enforce its decisions onto everyone, because anyone can fork their own version relying on publicly available code at low cost while preserving their own use value, in blockchain matters majority decisions are enforced and forking poses substantial costs on all users;

- Contrary to open source licenses that prevent anyone from appropriating the 'matter of trade' (i.e. software code), public ledgers introduce authentication thus scarcity into digital settings. Traceability of all actions on the ledger act as a deterrent from breaking the rules. So, blockchain move from 'carrots and rainbows' (von Krogh, Haefliger, Spaeth, & Wallin, 2012) as main incentives, to a 'gentle rivalry' (Ziolkowski, Parangi, Miscione, & Schwabe, 2018);

- Cryptocurrencies or other built-in blockchain rewarding schemes affect people's involvement not least because they trade and hoard tokens. This is not a feature of other FOSS projects, more reliant on reputation;

The uncertainty about tomorrow puts more pressure on what is done today because forking later on would be troublesome. In front of this condition, governance on-chain tries to put the future on the tracks that can be imagined today through allegedly complete smart-contracts. Consortia-based projects do not rely on these, but rely on arrangements according to which all partners are on the same boat and have 'skin in the game'. Durkheim argued that wherever a contract exists, it is subject to regulation, which is the work of society and not only of individuals;

- Derived from the previous points, blockchains manifest a level of mutually dependent interest, thus organizational togetherness, that the bazaar metaphor does not capture. While we maintain that digital modes of governance present substantial differences from previous ones like markets and hierarchies, we find the bazaar emphasis on software reductive. The focus on FOSS as main reference for the bazaar governance is limiting because it overemphasizes the production and development of software over its deployments, actual usages and drifts in practice, and undeniable influence that maintainers like miners exercise. Because of their function as long-term immutable ledgers, blockchains cannot be designed,

deployed, maintained, and certainly not understood without considering their actual use and the tensions they generate in real-life settings.

More concretely, like any other FOSS project, the source code of most blockchain software is publicly available for anyone to check, use, develop and redistribute it. In spite of these apparent similarities, there are remarkable differences between open-source applications like web browsers or word processors and blockchains, which makes them organizational technologies. Cryptocurrencies, by authenticating some tokens against the rest, introduce exclusivity into the digital environment, which has always been characterized by infinite replicability, thus plentitude. Records on distributed ledgers even when run by pseudonymous actors, are more trustworthy and reliable than what can be published on pseudonymous blogs. In short, before the blockchain, all copies were the same. With blockchain it has become possible to differentiate something from something else (like who owns a bitcoin) without relying on external authorities.

On open networks like the internet, both innovations and deviance come from the fringes. Since there is no way to seal boundaries to define who is in and who is out of open infrastructures, then to control them, the permissionless blockchains of our cases are constantly exposed to malicious actors and undesired outcomes. So, openness is generative both of innovations and misconducts (Zittrain, 2006).

It has to be reminded that an increased shared interest and togetherness does not come without tensions. Rather the opposite: conflicts in FOSS appear to be among tree-huggers compared to all possible means deployed in Bitcoin conflicts. The radicalization and even dishonesty that developed among involved Bitcoin factions led to incomplete or discordant forks. First, the evident loss of network effects that inherently accompanies these splits has to be noted: since Bitcoins attached to one chain cannot be traded any longer on the other. So, its overall use value depends on smaller mining capacity, trade volume, and user base. Beyond

that, the overall credibility of immutable ledgers has been severely undermined. In sum, Bitcoin block size and DAO conflicts illustrate the other side of trust and togetherness. In sum, it is essential not only not to overlook the role of trust in blockchains, but also not to overlook that trust building is not necessarily an idyllic process. What comes up clearly is that there can be no self-governance or self-sustainability solely relying on technology. Blockchains remain socio-technical systems, which are embedded into a broader institutional context even when they invent novel organizational forms.[47]

7.1. Hanseatic League

Hirschman (1970) articulated the three choices actors have to respond to declining organizations: loyalty, voice, or exit. Loyalty has been greatly diminished by the (allure of) wealth of opportunities that open networks prospect. Voice, i.e. the possibility of expressing diverging views, has also been enhanced by the wide availability of publishing tools to reach a potentially global audience. Changes in the possibility of exit, i.e. fork in these cases, is essential when comparing the bazaar to the mode of governance that blockchains enact. Referring to this threefold conceptualization and closing up to the details of a comparison between bazaar and our cases, one can see that loyalty is very low in FOSS, which tends to be promiscuous ("release early, release often, delegate everything you can, be open to the point of promiscuity" (Raymond, 1999)), whereas both permissionless and permissioned blockchains tend to be more 'sticky'. Probably because of a higher pressure to stay together in blockchains, voices tend to be much louder. Hardly ever a spat about Linux kernel technicalities hit the general press headlines, even if it runs billion of devices. The drama of crypto is often depicted as a never-ending saga for the global audience. Exit/fork and the disruption it entails for distributed ledgers, as argued above, mark the main difference

---

[47] https://policyreview.info/node/427/pdf

between bazaar organizing and the cases considered here. The following table summarizes the differences.

	Bazaar	**Blockchains**
Loyalty	Very low, to the level of promiscuity	Defined by its architecture
Voice	Community maintenance is important but dissent is hardly threatening	Very animated because interests are shared
Exit	Easy forks	Quite detrimental internally, generate a drop in credibility

Referring back to the DAO offers a good illustration of blockchains 'stickiness'. DAO miners were 'willing to sacrifice a week's mining revenue should [they] prove to be on the wrong side of the fork'[48] and thus were to follow outcomes that contradicted their preferences. This togetherness is peculiar of this case and blockchain applications. Ultimately, the Ethereum community remained relatively tight despite Ethereum Classic fork and the dissent that was voiced before and after it. It has to be noted that the voting process was not democratic in the sense of 'one head, one vote'. Only miners had the right to vote, which one user saw as evidence that 'Ethereum [would] never be free of miner consensus'. This clarifies the violation of FOSS characteristic 'separation of governance from property', thus blockchain's distinction from CBPP. What was at stake, and probably not very evident to these inward-looking communities, is that the totem of immutability, in which blockchains find their *raison d'être*, is rooted in the taboo of not forking. By deciding to fork to counteract

---

[48] https://www.reddit.com/r/ethereum/comments/4ot3z8/dao_is_under_attack_again/

an unintended use of their smart contact, the Ethereum community broke the foundational value they themselves had put at the core of their own technology. This is how they lost their innocence.

These reasons prompted us to name this peculiar governance mode. After considering several alternatives, we decided to name the mode of governance emerging from blockchain domain 'hanseatic', in reference to the Hanseatic League of the 13th to 16th century, before the consolidation of modern nation-states in Europe. Then, trade guilds across many cities spanning from nowadays Holland to the Baltic countries formed an alliance that proved hegemonic in Northern Europe trade through the North and Baltic seas. We find this analogy appropriate to suit our cases for three main reasons that correspond to three distinct disciplinary backgrounds:

1. It is an historic period that falls the constant fights of feudalism and pre-dates the establishment of the Rule of Law. Trust and alliances had a prominent role in regulating organizations and society even if rudimentary parliamentary assembly met sporadically:

2. During that centuries-long window, rival cities agreed to cooperate in order to foster their own commerce against other trade powers thought the established tariffs and trade rules;

3. Over those centuries, this alliance provided aids for safe navigation (including lighthouses and safe harbors), and defended its members from the constant threats of pirates. It even had its own army, albeit rarely deployed.

The Hanseatic League's favor for orderly trade over conflicts resulted in a long period of prosperity and peace. It is suitable to underline that this coalition was relatively fluid both because of members joining and leaving over time, and because of resemblances and common interests between member cities were not undermining their independence.

Reasons for referring to the Hanseatic League are that it used to have its own mode of governance which was heavily relying on trust rather than defined by an overall constitutional framework like modern national democracies. Also, its territory of influence was not set once for all, so exit was an option that some cities exercised sometimes over the centuries. Another reason to adopt this metaphor is the role of the guilds, professional associations that influenced the league's decisions, similarly to expert organizations having a more prominent role in consortia-based blockchains. Needless to say, compromised or just unreliable records because left to particular self-interests would turn highly problematic for example when land property authentication rely on them. In short, trust needs to be built far beyond software itself and its code availability. Within state jurisdictions, notaries and state officers are in charge of guaranteeing reliability. When the Rule of Law applies patchily, like in the Bitcoin and Ethereum cases, the questions of liability raise up: if there are no clear accountability lines, who is liable when something goes wrong? The awareness of those risks manifests indirectly also in the other cases above. For instance, the Georgia case sees a blockchain linked to Bitcoin -by far the most reliable blockchain because its size and track record- and state records. However, this induces conflicts between modes of governance: trust in the Hansa may not align with trust in the state (or hierarchy). If in 20 years an immutable blockchain records a different owner for a piece of land than an old paper certificate, what would a judge trust? What has legal standing? This remain open questions for the time being. What matters to stress here is that our reference to the Hanseatic League remains at a metaphorical rather than a blueprint.

7.2. Blockchains as organizational technologies

Information technologies have been changing how things get organized for a while now. Peer-to-peer networks, cloud computing, just to name a few waves of digital innovation, are instances of a mode of organizing which has been: a) circumventing the structures and conventions of formal organizations, and b) changing and disrupting markets while opening

new ones. Those changes are well epitomized by FOSS, its bazaar organizing and commons-based peer production. The most recent trend of digital innovation is blockchain, and comes from the same cultural milieu. However, it embeds functions that used to be domain of organizations: consensus and authentication. Cryptocurrencies proved at scale the feasibility of an architecture that certifies each token on a network and differentiates it from all others. All copies are the same no more. This newly created scarcity originates both cooperation to keep the system running reliably, and rivalry between actors longing for a finite number of tokens. Thus, blockchain mode of governance is peculiar, which we likened to the Hanseatic League for the prominence given to trust within an alliance rather than stringent hierarchies, where blockchains would be useless, or widely fluctuating markets, where cryptocurrencies governance showed all its shortcomings. Application domains like second-hand cars markets and land registries showed how this technology is not just about transmitting information, but it embeds organizational functions that redefine the possibilities for loyalty, voice, and exit. Thus, the overall organizational behavior.

Looking forward, it is impossible to avoid some level of speculation. Still, speculation about the future may say something about how things are perceived today. When money – or any kind of certain record for that matter – was not available, online organizing could be based on a gift economy like FOSS or Wikipedia, or had to rely on credit money that commercial banks keep pegged to fiat (i.e. state) money. Natively digital reliable records prospect an alternative that, for the time being, has been mainly tested for illegal trades. This is not new, major digital innovations, from videorecorders to digital music, found their origins in the gray area between legality and deviance. Indeed, social and organizational changes originate before this distinction crystallize.

In any case we should not be deterministic in assuming what behaviors and institutional context decentralized architectures imply and require. Agre (2003), referring to

the previous wave of peer-to-peer architectures originated with file sharing, instils the reasonable doubt that decentralized architectures do not necessarily match with decentralized institutions and vice versa. Especially, decentralization may not necessarily lead to equality in practice. In fact, most open projects (like the Web, Wikipedia, P2P, FOSS) showed remarkable tendencies to centralization over time (for instance (O'Mahony and Ferraro 2007). This is certainly possible for blockchain and, for instance, Bitcoin mining shows a clear centralization in China where estimates place 2/3 of computing power. Consortia-based blockchain may follow the same route but at least, since not all governance tools are inscribed on-chain a priori, partners can still decide the fate of their own partnership.

Long-term consequences in governance remain largely unpredictable, especially where state authorities cannot be taken for granted. In prospect, reliable records are promising in low trust environments, like where states are weak or absent. This means that, if successful, blockchains and states may be on a collision trajectory unless they partner. The modes this may happen would promising research avenues.

References

Aaltonen, A., & Lanzara, G. F. (2015). Building governance capability in online social production: Insights from Wikipedia. *Organization Studies, 36*(12), 1649-1673.

Agre, P. E. (2003). P2p and the promise of internet equality. *Communications of the ACM, 46*(2), 39-42.

Akerlof, G. A. (1978). The market for "lemons": Quality uncertainty and the market mechanism. In *Uncertainty in Economics* (pp. 235-251): Elsevier.

Atzori, M. (2015). Blockchain technology and decentralized governance: Is the state still necessary?

Benkler, Y. (2006). *The wealth of networks: How social production transforms markets and freedom*: Yale Univ Pr.

Benkler, Y. (2016). Peer production and cooperation. *Handbook on the Economics of the Internet, 91*.

Briggs, R. O., & Schwabe, G. (2011, 2011/05/05/). *On Expanding the Scope of Design Science in IS Research.* Paper presented at the International Conference on Design Science Research in Information Systems.

Brown, C. V. (1997). Examining the emergence of hybrid IS governance solutions: Evidence from a single case site. *Information Systems Research, 8*(1), 69.

Chesbrough, H. W. (2003). *Open innovation: The new imperative for creating and profiting from technology*: Harvard Business Press.

Ciborra, C. a. a. (2000). *From control to drift: the dynamics of corporate information infastructures*: Oxford University Press, USA.

Coleman, E. G. (2012). *Coding Freedom: The Ethics and Aesthetics of Hacking*: Princeton University Press.

Constantinides, P., & Barrett, M. (2014). Information infrastructure development and governance as collective action. *Information Systems Research, 26*(1), 40-56.

Czarniawska, B. (2014). *A theory of organizing*: Edward Elgar Publishing.

De', R. (2005). E-government systems in developing countries: stakeholders and conflict. *Electronic Government*, 26-37.

De', R., & Sen, C. (2004). The complex nature of e-Government projects: A case study of Bhoomi, an initiative in Karnataka, India. *Electronic Government*, 556-557.

Demil, B., & Lecocq, X. (2006). Neither market nor hierarchy nor network: The emergence of bazaar governance. *Organization Studies, 27*(10), 1447-1466.

Dodd, N. (2018). The social life of Bitcoin. *Theory, Culture & Society, 35*(3), 35-56.

Du, W. D., Pan, S. L., Leidner, D. E., & Ying, W. (2018). Affordances, experimentation and actualization of FinTech: A blockchain implementation study. *The Journal of Strategic Information Systems*.

Ekblaw, A., Azaria, A., Halamka, J. D., & Lippman, A. (2016). *A Case Study for Blockchain in Healthcare:"MedRec" prototype for electronic health records and medical research data.* Paper presented at the Proceedings of IEEE open & big data conference.

Grover, P., Kar, A. K., & Ilavarasan, P. V. (2018). *Blockchain for Businesses: A Systematic Literature Review.* Paper presented at the Conference on e-Business, e-Services and e-Society.

Henderson, J. C., & Venkatraman, N. (1993). Strategic alignment: Leveraging information technology for transforming organizations. *IBM systems Journal, 32*(1), 4-16.

Herbert, J., & Litchfield, A. (2015). *A novel method for decentralised peer-to-peer software license validation using cryptocurrency blockchain technology.* Paper presented at the Proceedings of the 38th Australasian Computer Science Conference (ACSC 2015).

Hirschman, A. O. (1970). *Exit, voice, and loyalty: Responses to decline in firms, organizations, and states* (Vol. 25): Cambridge, Mass.: Harvard University Press.

Hutt, R. (2016). *Beyond bitcoin: 4 surprising uses for blockchain.* Paper presented at the World Economic Forum.

Jemielniak, D. (2014). *Common knowledge?: An ethnography of Wikipedia*: Stanford University Press.

Karame, G. O., Androulaki, E., Roeschlin, M., Gervais, A., & Čapkun, S. (2015). Misbehavior in bitcoin: A study of double-spending and accountability. *ACM Transactions on Information and System Security (TISSEC), 18*(1), 2.

Kshetri, N. (2017). Will blockchain emerge as a tool to break the poverty chain in the Global South? *Third World Quarterly, 38*(8), 1710-1732.

Langley, A. (1999). Strategies for theorizing from process data. *Academy of Management Review*, 691-710.

Lustig, C., & Nardi, B. (2015a). *Algorithmic authority: The case of Bitcoin.* Paper presented at the 2015 48th Hawaii International Conference on System Sciences (HICSS).

Lustig, C., & Nardi, B. (2015b). *Algorithmic authority: The case of Bitcoin.* Paper presented at the System Sciences (HICSS), 2015 48th Hawaii International Conference on.

Lyytinen, K., & King, J. (2006). Standard making: a critical research frontier for information systems research. *MANAGEMENT INFORMATION SYSTEMS QUARTERLY, 30*(I), 405.

MacDonald, T. J., Allen, D. W., & Potts, J. (2016). Blockchains and the boundaries of self-organized economies: Predictions for the future of banking. In *Banking Beyond Banks and Money* (pp. 279-296): Springer.

Malone, T. W., Yates, J., & Benjamin, R. I. (1987). Electronic markets and electronic hierarchies. *Communications of the ACM, 30*(6), 484-497.

Maurer, W., & DuPont, Q. (2015). Ledgers and Law in the Blockchain.

Moloney, A. (2010). Unclear Land Rights Hinder Haiti's Reconstruction. *News.Trust.Org*. Retrieved from http://news.trust.org/item/20100705105000-axvt3/

Morabito, V. (2017). Business Innovation Through Blockchain. *Cham: Springer International Publishing*.

Morisse, M. (2015). Cryptocurrencies and bitcoin: Charting the research landscape.

Musiani, F., Cogburn, D. L., DeNardis, L., & Levinson, N. S. (2016). *The turn to infrastructure in Internet governance*: Springer.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Consulted, 1*, 2012.

Parker, G., Van Alstyne, M., & Jiang, X. (2016). Platform ecosystems: How developers invert the firm.

Powell, W. (2003). Neither market nor hierarchy: Network forms of organization. *The sociology of organizations: classic, contemporary, and critical readings*, 315.

Powell, W. W. (1990). Neither market nor hierarchy - Network forms of organization. *Research in Organizational Behavior, 12*, 295-336.

Provan, K. G., & Kenis, P. (2008). Modes of network governance: Structure, management, and effectiveness. *Journal of public administration research and theory, 18*(2), 229-252.

Raymond, E. (1999). The cathedral and the bazaar. *Knowledge, Technology & Policy, 12*(3), 23-49.

Riemer, K., Gogolin, M., & Klein, S. (2005). Introduction to Organizational Networks: Emergence, motives, classification and types. *Universitaet Muenster*, 35.

Sambamurthy, V., & Zmud, R. W. (1999). Arrangements for information technology governance: A theory of multiple contingencies. *Mis Quarterly*, 261-290.

Scholz, T., & Stein, V. (2018). The Architecture of Blockchain Organization.

Shaikh, M., & Henfridsson, O. (2017). Governing open source software through coordination processes. *Information and Organization, 27*(2), 116-135.

Stallman, R. (2002). *Free software, free society: Selected essays of Richard M. Stallman*: Lulu. com.

Stebbins, R. A. (2001). *Exploratory Research in the Social Sciences*: SAGE.

Surowiecki, J. (2005). *The wisdom of crowds*: Random House Digital, Inc.

Swan, M. (2015). *Blockchain: Blueprint for a new economy*: " O'Reilly Media, Inc.".

von Krogh, G., Haefliger, S., Spaeth, S., & Wallin, M. W. (2012). Carrots and rainbows: Motivation and social practice in open source software development. *MIS Quarterly-Management Information Systems, 36*(2), 649.

Walsh, C., OReilly, P., Gleasure, R., Feller, J., Li, S., & Cristoforo, J. (2016). New kid on the block: a strategic archetypes approach to understanding the Blockchain.

Weill, P., & Broadbent, M. (1998). *Leveraging the new infrastructure: how market leaders capitalize on information technology*: Harvard Business Press.

Weill, P., & Ross, J. W. (2004). *IT governance: How top performers manage IT decision rights for superior results*: Harvard Business Press.

Williamson, O. E. (1975). Markets and hierarchies. *New York, 2630*.

Ziolkowski, R., Parangi, G., Miscione, G., & Schwabe, G. (2018). *Examining Gentle Rivalry: Decision-Making in Blockchain Systems.* Paper presented at the Accepted with revisions for 52nd Hawaii International Conference on System Sciences, Maui, Hawaii.

Zittrain, J. L. (2006). The generative internet. *Harvard Law Review*, 1974-2040.