An Institutional Survival Guide for Open Blockchain systems: secondary rules as a solution to the governance of blockchains.

Abstract: Blockchain governance is hard, this paper explores this thorny issue. First, it provides a methodological framework to analyze different blockchain systems. Then, it outlines how the governance problem has unfolded in two major blockchains, namely, Bitcoin and Ethereum. Moreover, this essay shows how the governance of blockchains may limit their ability to comply with new regulation by focusing on blockchain digital immutability and art. 17 (Right to be forgotten) of the GDPR. Finally, it suggests a solution based on the establishment of secondary rules of change for blockchains, this notion draws from the work of legal philosopher, namely Hart and Pagallo. The goal of this analysis is to show how, by implementing secondary rules of change to govern protocol modifications and improvement proposals, blockchains could improve legitimacy, prevent hard-forks, better comply with regulations, and truly manifest their technological potential.

1. Introduction

This article studies blockchain [sic] governance. As is well known Nakamoto proposed the blockchain in 2008 as the underlining data structure of the Bitcoin system (Nakamoto, 2008, p. 306). Blockchains solve two longstanding problems in the field of digital cash: double spending and Byzantine fault tolerance (Narayanan & Clark, 2017; Wattenhofer, 2016). Blockchain technology is one of the last development in peer-to-peer (P2P) architectures; in fact, blockchains enable the "short route" typical of P2P systems in, among others, the online payment market (Pagallo and Durante, 2009).

Since then, the interest in blockchain technology has grown exponentially. While a comprehensive survey of the possible applications of the blockchain technology lies beyond the scope of this paper, I assume that the reader is aware of some of the several purported applications of this emerging technology, as suggested by some authors (Swan, 2015, 2017; D. Tapscott & Tapscott, 2016; D. T. a. A. Tapscott, 2017; Yermack, 2017).

The terminology around blockchain technology is developing continuously (Walch, 2017). Glaser and Bezzenger proposed a persuasive taxonomy that this study adopts as a starting point (Glaser & Bezzenberger, 2015); chiefly, they introduced a distinction between cryptocurrencies and decentralized consensus systems. More precisely, such systems are better understood as distributed and, then, decentralized. In distributed networks each point is neither a central hub nor a satellite node, whereas a decentralized network has multiple central hosts (Galloway, 2004, p. 10); hence the object of this study are distributed consensus systems, hereinafter "DCS". DCS are based on "peer-to-peer principles rather that central authority and rely on cryptography for network-wide verification (by consensus) of systems states" (Glaser & Bezzenberger, 2015, p. 2). Generally, DCS enable the transfer of digital (or tokenized) assets; moreover, DCS do not necessarily implement a cryptocurrency (e.g. the Corda platform) nor a data structure wherein data is organized in blocks[1] (e.g. IOTA and Hashgraph). Consequently, cryptocurrencies and blockchains are species of the genus DCS. This terminology allows the present study to move beyond cryptocurrencies and to deal with other consensus-based P2P systems. On a more granular level, this article adopts a methodology based on epistemological levelism to precisely define the object and the variables of the phenomena at hand.

Floridi has provided the refined version of epistemological levelism that grounds the methodological basis for this essay in the form of the method of levels of abstraction (Floridi, 2008, 2011). Floridi defines a level of abstraction (onward, also "LoA") as "*a finite but non-empty set of observables. No order is assigned to the observables, which are expected to be the building blocks in a theory characterized by their very definition*" (Floridi, 2008, p. 309).Moreover, "*an observable is an interpreted typed variable*[2]*, that is, a typed variable together with a statement of what feature of the systems under consideration it represents*" (Floridi, 2008, p. 306). By applying this method to the DCS landscape, one is in a better position to address the governance problem. While some have argued that the technology is "general purpose" (Davidson, De Filippi, & Potts, 2016), it seems evident that a better-informed discussion on DCS ought to tie normative claims to specific architectures. In other words, most aspects of a DCS are related to its architecture and, architectures differ widely from system to system. Thus, this methodology allows for a more precise definition that, in turn, enables a better understanding of the problem.

LoA(1) encompasses two observables, namely: the degree of openness concerning participation to a particular DCS and computational complexity. At LoA(1) systems are either open or closed[3] and Turing-complete or Turing-incomplete. In other words, closed systems implement a centralized identity layer, that is, only selected parties (nodes) may be granted permission to perform specific network functions. For example, only specific parties may be allowed to join the network or verify transactions. In contrast, in open DCS any node participating in the network has (in principle) the same degree of access to the network functions than any other node. In the vocabulary jungle of DCS, this distinction is also referred to as permissionless (open) or permissioned (closed) systems, for an explanation see (Xu et al., 2017). For example, the platform Corda built by the R3 consortium is an example of a closed DCS while most

[1] Hence the term blockchain

[2] That is, a placeholder qualified to hold only a declared kind of data.

[3] I am aware that some systems do not fall squarely in this categorization, think, for instance, of the EOS blockchain where, on one hand, anyone can use it (or contribute to the development of it) while on the other hand, the nodes in charge of validating the transactions (known as block producers) have been selected in the development phase. That said, I still hold that the open/closed nature of a system provides a much-needed starting point for scholarly analysis on the topic.

(if not all) cryptocurrencies are open DCS. This first distinction is of utmost relevance. The second observable defines what kind of computations a DCS can execute. Computational systems split between Turing-complete and Turing-incomplete[4], the latter execute only particular operations (e.g. Cardano or Bitcoin) while the former execute any computation, think of a world computer. Ethereum and EOS are examples of Turing-complete DCS.

This article uses a second – nested- LoA: LoA(2). LoA(2) has two observables: (i) the presence or lack thereof an influential figure in the systems and (ii) the presence or lack thereof a legal entity whose task is to maintain the network. According to LoA(2), Ethereum has both; namely, it has an influential figure (Mr. Vitalik Buterin) and a legal entity whose mission is to maintain the network (the Ethereum foundation[5]). Conversely, Bitcoin used to have an influential figure (Satoshi Nakamoto) and a legal entity in charge of maintaining the network (The Bitcoin foundation); at the time of writing Satoshi is still missing and the Bitcoin Foundation has ceased operations; therefore at LoA(2) Bitcoin is the opposite of Ethereum. LoA(2) helps us to shed some light on the governance structures of DCS; consequently, it will come in handy in section 5. By now, it should be clear that several types of blockchains exist according to the proposed classification, hence, the usefulness of the method of the levels of abstraction; thanks explicitly to LoA(1) we can exclude permissioned systems from our inquiry for the following reasons.

In fact, the governance of systems where there are a limited number of known-parties negotiating the terms and conditions for participation as in, for example, the SWIFT consortium need not concern us. While it represents an interesting area of study, it differs widely from the governance structure of P2P and open-source systems where anyone (again, in principle) can contribute to the governance of the system. Therefore, the most interesting aspect of DCS is the way in which open networks are governed especially if one is to believe the claims about their potential to re-arrange the way society is structured with DCS[6]. Hence, this articles focuses on open DCS as defined using LoA(1). It is now time to clarify at which level of abstraction we confront the concept of governance as it relates to DCS.

On one hand, the concepts of on-chain governance versus off-chain governance are defined as follows. The former refers to the implementation of governance rules at the system level (i.e. on the blockchain); in other words, governance structures are endemic to the architecture. Tezos and EOS are examples of DCS that implement on-chain governance. The latter refers to systems where the governance structures lie outside the architecture; that is, where governance rules are not *coded* into the system. At the time of writing, most DCS do not implement on-chain governance rules and they, often, do not explicitly adopt off-chain governance structures. This is not to say that most systems do not have governance; in

[4] This distinction is often reflected on the programming language of the system. In this sense, Turing-complete systems implement a Turing-complete language (e.g. Serpent and Solidity are Turing-complete programming languages used in the Ethereum system) and vice versa. Moreover, DCS may have their own programming language, support other programming languages, or both.

[5] A no-profit legal entity resident in Switzerland.

[6] For a rather amusing outline see (Jun, 2018).

fact they do, but, and this is crucial for our thesis, such governance structures are often opaque and hidden behind technicalities.

On the other hand, Malcom Campbell-Verduyn introduced a useful classification of governance of DCS. More specifically, the Author distinguishes between governance by blockchains, governance with blockchains and governance of blockchains (Campbell-Verduyn, 2018, p. 186). While it is evident that these three forms of governance mutually influence one another, this article deals with the governance of DCS for multiple motives. First, I am convinced that the governance of DCS is the most influential aspect in determining the future trajectory of the development of the technology. That is, in the interplay of the three facets of governance, the governance of DCS shapes the other two. Second, the governance of DCS is better able to outline the politics hidden behind the technology, because politics has artifacts (Joerges, 1999). Lastly, I believe that the level of governance of DCS is the most appropriate to implement an infraethics, that is, an *ethical infrastructure,* to ensure that the social experimentation and the development brought about by the technology evolves in a way that is conducive to human flourishing, enriches human interactions by opening ways of sound collaboration, and facilitates, among other things, what is morally right (Floridi, 2017; Pagallo, 2008).

This paper is organized as follows. Section 2 provides an overview of the existing literature on DCS governance; section 3 highlights how the problems of governance of DCS unfolds, focusing on the evolution of the regulatory environment. Section 4 examines the landscape of ideas embedded in DCS; section 5 provides a possible solution to the problem of governance of DCS, section 6 outlines some design principles to address the governance problem; section 7 concludes.

2. The DCS Governance in the literature

The subject of DCS lies at the intersection of several disciplines such as distributed computing, cryptography, game theory, sociology, economics, and law. Moreover, as with any complicated sociotechnical topic, discipline-hopping is a necessity (Galloway, 2004). Hence, it is unsurprising that several disciplines touched on the issue of governance of DCS, mostly using the more popular but less precise term blockchain governance. Notably, most relevant literature focuses on the topic of governance with or by blockchains, while less attention is generally reserved to the core focus of this work, namely, governance of blockchains. Besides, most scholars naturally focus on specific implementations of DCS, generally Bitcoin and Ethereum. I argue that a more proficuous approach lies in abstracting the general components of DCS (as provided by using the LoAs mentioned above) in order to address the governance of DCS more broadly. With these clarifications in mind, I examine some of the existing literature on the governance of DCS.

Sclavounis rightly distinguishes from governance by the network from the concept of governance of the network; this is the same distinction adopted in this work. The author also notes that "*The promise of governance by the network – a techno-institutional solution to solving the problems of cooperation and coordination – can only work if the governance of the network is robust, fair and predictable*" (Sclavounis, 2017).

Lehdonvirta argues that thinking about blockchain in terms of its potential to change the very way economies are organized turns out to be a naïve understanding of the technology since the real issue lies in who sets the rules that the network enforces. Therefore, blockchain technologies cannot escape the problem of governance; in his own words "*you can't engineer away governance as such*" (Lehdonvirta, 2016). The author, thus, established the blockchain governance paradox, according to which once one addresses the problem of governance one no longer needs blockchains.

Atzori shows the pitfalls in the decentralized governance narrative about blockchains by demonstrating the pre-political nature of the technology, "*contrary to the claims of some blockchain advocates, the final outcome would be the general disempowerment of individuals, the "deification of the market and the triumph of anti-politics*" (Atzori, 2015, p. 25). While she focuses on the issue of governance by the network, she concludes by showing that the real issue is, indeed, the problem of governance of the network.

On the quasi-evangelical side, Davidson et al. argue that blockchain technology is better understood as a revolutionary new institutional technology of governance (Davidson et al., 2016; Davidson, De Filippi, & Potts, 2017). They contend that blockchain technology is a "*new mode of governance that competes with other economic institutions of capitalism, namely firms, markets, networks, relational contracting and governments*" (Davidson et al., 2016, p. 24).

De Filippi and Loveluck examine the governance by and of the Bitcoin system finding that the latter exhibits a highly technocratic power structure[7] (De Filippi & Loveluck, 2016). They also address the opportunity to establish a body similar to ICANN and reject it: "*A centralized governance body […] would obviously fail to obtain any kind of legitimacy from within the Bitcoin community […] since eliminating the need for a fiduciary institutions, or other centralized authorities was very purpose of the Bitcoin network*" (De Filippi & Loveluck, 2016, p. 19). In the end, the authors argue for a governance structure using the underlying technology but fail to outline who should design such rules.

Reijers et al. study how DCS can produce models of governance and how these models are accepted. More precisely, the authors analyze the justification of political principles offered by technologist on the bases of an agreement made in an initial situation (e.g., social contract) (Reijers, O'Brolcháin, & Haynes, 2016).

Hacker applies complexity theory to DCS before suggesting an institutional approach based on a comply or explain approach drawn from the field of corporate governance (Hacker, 2017). He argues for

[7] This is consistent with a recent quantitative study that also find the same to be true for the Ethereum and Bitcoin systems (Azouvi, Maller, & Meiklejohn, 2018).

the application of corporate governance rules to blockchain applications through legal intervention. On this basis, Hacker suggests that an "ICANN for blockchains" may eventually arise if *"permissionless blockchains, and the cryptocurrencies and token-based ventures they give rise to, become more interconnected*" (Hacker, 2017, p. 35). This latter point is, however, controversial.

The establishment of an ICAAN for blockchains suggests the equation of internet and DCS governance; I see one major issue against it. ICAAN arose from the implementation of a centralized layer (the DNS system) on top of distributed architecture (TCP/IP), hence, unless a similar occurrence ensues in the DCS landscape I hold the equation to be unwarranted. For the time being, DCS lack a common centralized layer akin to the DNS systems that prompted the establishment of ICAAN.

Finally, Abramaowicz introduces the concept of cryptocurrency-based law, that is, a P2P decision-making method based on tacit coordination games, he suggests that such a method might be used to "*determine whether to make changes to the Bitcoin reference code*" (Abramaowicz, 2016, p. 368). Moreover, he correctly notes that Bitcoin uses P2P (governance by and with the network) for transactions and not for changes to the rules themselves (governance of the network). This solution still relies on a pre-existing set of rules, namely the ones establishing such governance framework. Thus, it is fair to observe that Abramowicz's perspective does not solve the actual problem of establishing the rules according to which the governance of the DCS operate.

It seems fair to argue that the issue of governance of these systems deserves more attention. Also, the differences between these ecosystems are usually underestimated or disregarded. I will now explore some relevant events in the two primary DCS (Bitcoin and Ethereum) to show how the governance issue has unfolded, and how it relates to an ever-changing regulatory environment as exemplified by the General Data Protection Regulation (onward, also GDPR) enacted in the European Union. The next section aims to clarify how the unsolved issue of the governance of the network impacts the landscape of DCS, possibly amounting to an existential (legal) risk.

3. The governance of DCS: case studies and real-world implications.

Let us begin by examining how the lack of governance (of the network) played out in crucial events in the DCS landscape. Namely, I focus on significant events in the Bitcoin and Ethereum systems as pathological examples of the absence of sound governance structures. One must note that the two systems have different governance modes (recall both LoA(1) and LoA(2)).

a) Update of the Bitcoin Core software from version 0.7 to 0.8.

March 2013, the Bitcoin core developers rolled out an update to the Bitcoin core software in order to fix some issues and vulnerabilities: ordinary maintenance work. Due to a bug in the update the new version of the software was incompatible with the older one, thus a *hard fork*[8] occurred. The price of Bitcoin plummeted, immediate action was needed. The core developers persuaded two of the biggest mining operators to roll back to the previous version of the software for the sake of Bitcoin's integrity (Popper, 2015). In a matter of hours, the blockchain running the version 0.7 caught up the one running the new software thus solving the issue. Surprisingly, the lack of any norms or guidelines for such an event did not produce any major inconvenience; pure technocracy proved successful. In this instance, the informal and opaque mode of governance manifested itself; a few people resolved the issue by coordinating without informing the community. Arguably, this event confronted the ecosystem with the problem of unpredictable off-chain events.

b) The Bitcoin block size debate.

Most DCS systems[9] have scalability issues, for instance the throughput of the Bitcoin network is in the order of 6-7 (TPS, transaction per second)[10]; moreover, by design, the size of each block in Bitcoin is limited to 1mb. Some members of the community along with some core developers (namely, Gavin Andreessen and Mike Hearn) proposed to expand the block size to accommodate more transactions per block thereby increasing throughput, others disagreed. The controversy culminated with the launch of Bitcoin Cash and Bitcoin Gold in 2017, different versions of Bitcoin where the block size is not limited to 1mb. This process unfolded in internet chatrooms, mailing lists, Reddit, and forums. Interestingly both sides claimed to represent the true vision of Nakamoto (Hearn, 2015). This controversy highlighted the lack of sound governance structures of Bitcoin (Campbell-Verduyn, 2018). Arguably, the block-size debate resulted in a loss of trust in Bitcoin's ability to adapt, to the advantage of other systems that are run by a legal entity or directed by an influential figure.

c) The DAO

The DAO[11] was a *"failed experiment in algorithmic governance"* (Campbell-Verduyn, 2018). The DAO was intended to act as a decentralized crowdsourced investment funding vehicle. In the funding phase the

[8] A hard fork is the split of the blockchain into two incompatible strands, for an overview of forking mechanisms and see (A. Zamyatin, 2018)
[9] With some notable exemptions in the likes of IOTA, EOS, Algorand, Hashgraph, Cardano, and Vechain.
[10] Several orders of magnitude below global payment networks such as VISA and Mastercard.
[11] Decentralized Autonomous Organization, for an incomplete terminological guide see (Buterin, 2014)

DAO collected 150 million dollars in ether[12]. A few weeks after the launch a hacker drained more than 30% of the funds exploiting a vulnerability in the code. A vivid debate arose in the Ethereum community, which, among several controversies, decided to rewrite the Ethereum blockchain to restore the funds. The much-heralded immutability of the blockchain was gone. Again, the decision process was opaque, and part of the community forked creating Ethereum Classic.

These examples show the lack of a consistent governance structure of the blockchain, so that a question naturally arises: how can one expect a general-purpose technology (Davidson et al., 2016) that could allegedly reshape society (Atzori & Ulieru, 2017; Jun, 2018; Swan, 2015, 2017) to operate in such an unpredictable way? I contend that one ought not to accept that. However, there is more.

Governance structures arguably determines the ability of systems to comply with existing or new regulations. To clarify how the lack of governance structures influences compliance one prominent example may suffice; enter the GDPR.

The GDPR came in effect on the 25th of May 2018, art. 17 (right to be forgotten) states that "*the data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay* […]" if specific grounds apply. Let us assume that the ground rules (a) and (b) of art. 17 apply and that art. 17.3 does not. Therefore, under the GDPR, a data subject whose personal data have been stored on a DCS has the right to obtain the erasure of such data. Putting aside several issues in determining the controller(s) and the processors(s) or personal data[13], current DCS are inherently incompatible with the regulatory framework of the European Union as represented by art. 17 of the GDPR[14]. This is not a hypothetical issue. Some research has shown that the Bitcoin blockchain already stores 1600 arbitrary files, some of which, surely qualify as personal data (Matzutt et al., 2018; Sward, Vecna, & Stonedahl, 2018). Prima facie, *immutable*[15] digital systems are bound to make the erasure of data impossible, this aspect is, in fact, one of the leading selling points of DCS. Now the question becomes how to address this problem.

Let us assume that technical solutions exist, as suggested by some relevant research (Ateniese, Magri, Venturi, & Andrade, 2017; Puddu, Dmitrienko, & Capkun, 2017) and that compliance with European Legislation is desirable for DCS. I contend that blockchains need a governance framework if they stand any chance of compliance with the GDPR. Supplementary, the establishment of a procedural system of

[12] Ether (ETH) is the currency of the Ethereum network.
13 For an overview of several legal issues related to DCS and the GDPR see (Ramsay, 2018)
[14] We leave aside some interpretation issues such as identifying the controller of the data for the sake of brevity, moreover such an assessment depends on the architecture of the DCS where the personal data has been inserted.
[15] In the sense specified by Walch (Walch, 2017).

governance of DCS is likely to pave the way to widespread adoption of DCS and, to improve the legitimacy of such systems in the eyes of regulators. Although this issue is not the focus of this paper it is possible to argue that failure to ensure the ability to comply with the GDPR could have dramatic effects on DCS in the EU. It may not be unwarranted to think that EU regulators could go as far as ban *non-complaint* DCS. After all, data protection is a fundamental right in the EU[16].

Lastly, this example shows how the lack of governance structures of the network could manifest itself in the form of exogenous (off-chain) events such as newly enacted regulations.

The next section deals with the sometimes hidden politics of DCS, highlights some common misconceptions and, by leveraging the LoAs introduced in the first section provides a tool for analyzing different implementations which will be relevant in section 5.

4. Hidden ideas in DCS

Anyone who is familiar with the crypto ecosystem knows what kind of narrative often permeates the discourse. The ideology of most early adopters and enthusiast of DCS has been qualified as anarcho-capitalistic (Bogost, 2017). There is, indeed, a certain aversion against authority and a celebration of the individual, that is, the celebration of the homo economicus known to sociologist as the anthropological monster (Atzori, 2015). Hidden behind a celebration of egalitarian principles lies a push toward a technocratic society managed by an elite of tech-savvy individuals.

Several authors have explored the politics of DCS (Baldwin, 2018; DuPont, 2014; Golumbia, 2016; Scott, 2015). The latter correctly notes that the dream of technological escape that informs some adopters of the technology (cyberpunks and libertarian alike) is essentially an ideology of the already-empowered and that DCS contain a latent potential for encouraging technocracy (Scott, 2015, p. 4). Golumbia shows how, in the DCS narrative, political opinions (often stemming from the right wing of the political spectrum) turn into facts; technical problems herald political solutions while being disguised as technicalities[17] (Golumbia, 2016, p. 48). The outlook given by those authors provides an essential backdrop for the discourse on governance of DCS.

One must also remember that artifacts have politics (Winner, 1980). Also, conversely, that politics have artifacts (Joerges, 1999). Galloway showed how protocol (in the form of the architecture of the internet) enabled the shift to a control society; analogously Manski and Manski conclude that "*recent history gives reason to expect that state interventions into the development of blockchain technology are more likely to lead in a totalitarian rather than democratizing direction*" (Galloway, 2004; Manski & Manski, 2018, p. 8). I see no reason not to argue that blockchain technology, and more generally, DCS may lead to a further transition into a

[16] Article 8(1) of the Charter of Fundamental Rights of the European Union
17 As an example, think of the proof of stake algorithm.

stricter control society. Therefore, any discourse on the present topic, especially when dealing with the issue of governance, must be wary of egalitarian claims and tales of empowerment.

Further, the narrative behind DCS assumes a natural technological progression of humanity toward decentralization (more appropriately, distribution) using technological means (Baldwin, 2018). This is not new. Agre pointed out the promise of equality brought about by the P2P movement and how it relates to well-established thinkers (Agre, 2003). P2P technology heralded a new era of egalitarian principles that culminated in the declaration of independence of cyberspace. The rest is history, *pace* John Perry Barlow. What seemed to be a technological drive toward the distribution of power and wealth turn out to empower more centralization of both, Lawrence Lessig worries that the same might happen to DCS architectures[18]. The issue of governance manifests the political aspect of DCS at many levels.

At the first level, the presence of an influential leader determines much of the power structures of some systems; think, as an example, of the role of Mr. Vitalik Buterin in Ethereum. The same applies to other DCS such as Litecoin (LTC) and Bitcoin before the leader of the former stepped down, and the leader of the latter disappeared. On the same line, the presence of an institutionalized entity in charge of the development of a DCS entails a different political outlook than a system without it, such a difference is found – among others – between Bitcoin and Ethereum. Simply put, benevolent dictatorships run these systems.

Second, the size of the network and the data structure used by DCS also has some relevance in the discourse about governance. Therefore, a network where possible validators are selected (e.g., EOS) must be treated differently than one where there is little or no hierarchy (e.g., Monero). More precisely the governance of a DCS necessarily presupposes a thorough analysis of the network structure, that is, of the governance by and with the DCS (see section 6).

Third, to avoid circularity or an infinite regress one must also acknowledge that DCS are mostly created without clear procedural governance external to the system. While it is true that some systems try to implement on-chain rules for the governance *of* the system itself[19] these rules already presuppose a framework wherein the rules have been designed before being implemented (see next section). So far, on-chain governance of DCS has been proven problematic. Tezos faced disputes between the founders and the first director of the foundation overseeing the $243 million fund. Further, EOS is experiencing a governance crisis at the time of writing[20]. Blockchain governance is hard, some argue it is too soon for

[18] Thinking Through Law and Code, Again - Lawrence Lessig - COALA's Blockchain Workshops - Sydney 2015, available here: https://www.youtube.com/watch?v=pcYJTIbhYF0

[19] Such as Tezos and EOS.

[20] As reported in https://www.coindesk.com/eos-arbitrator-problem-crypto-governance-breakdown-explained/

on-chain governance[21]; I disagree. The point is not that it is too soon, instead what is holding back the development of on-chain governance is the lack of off-chain rules on how to make on-chain rules.

The aim of this article, to which I now turn, is to show that the DCS ecosystem would benefit from adopting a constitutional order of *secondary rules*[22].

5. The Way Forward

The concept of primary and secondary rules of law is of paramount importance to address the governance problem of DCS. Hart introduced the classical distinctions between primary and secondary rules of law (Hart & Green, 2012). The former aim to govern social and individual behavior, the latter are rules of recognition, adjudication, and change. Rules of change regulate the creation, modification, and suppression of primary rules. As explained by Pagallo secondary rules are "*meta-rules by which all other rules of the system are identified and understood as valid, ie, that which counts as valid law within that system*" (Pagallo, 2017, p. 42). At one level, secondary rules include meta-rules of procedural regularity to ascertain whether a decisional process conforms to a given value (i.e. fairness, justice, nondiscrimination) (Kroll et al., 2016). Some argue that procedural regularity determines the legitimacy of a legal system (Barnett, 2003). Following this line of reasoning, we may say that secondary rules determine the governance *of* the network whilst primary rules determine the governance *with* and *by* the network. Consequently, the establishment of secondary rules heralds the proposed solution to the governance problem.

Thus, at our LoA a constitution dictates rules on how to make rules, and rules according to which other rules count as valid within the system. As Barnett argues the presence of secondary rules that foster the pursue of a given value give legitimacy to the system. With that in mind, in the DCS space, most implementations do not provide secondary rules. Consequently, a DCS that does not explicitly state the rules according to which the other rules are issued or amended may implement changes to the protocols that might be deemed illegitimate, as many examples in the DCS space have shown (see section 3). It is precisely the lack of such a structure that contributes to governance problems and hard-forks. After all, hard-forks are symptomatic of a lack of legitimacy in the forked system.

More precisely, when a DCS implements rules to govern the interactions on the network (in the shape of: "if the hash of block *x* with height *y* is less than t, then *y* is a valid block"[23]), one deals with the

---

[21] For example, see Micheal J. Casey in https://www.coindesk.com/soon-chain-governance/

[22] While it is true that some systems have adopted a *constitution* (EOS has one available here https://github.com/EOSIO/eos/blob/37ce45c0b60d2710569c2d1a9229945cc0e855a9/governance/constitution.md) the concept of constitution defended in this article is different and grounds another approach to DCS governance. One may, in fact, argue that the EOS constitution does not resemble a constitution in the legal sense.

[23] This type of norm (among others) determines the conditions of validity of the newly mined blocks in most DCS that implement the proof of work (PoW) consensus algorithm, also known as Nakamoto consensus, see (Cachin & Vukolić, 2017).

governance with the network. Conversely, when a DCS uses rules to prevent behaviors in the system (such as: "If a user sends some coins to an address, then the user cannot send the same coins to another address"), one finds governance by the network. Both these examples embody the primary rules of DCS.

What is missing are rules that govern how such rules are formed and enacted; what is missing is a constitution of DCS, that is, governance of the network. My point is that, no matter what fancy governance mechanism one implements on-chain, a DCS that lacks off-chain rules on how to make on-chain rules (a) does not escape the blockchain governance paradox, since any implementation of on-chain rules presupposes a deliberation on what those rules are and how they should be coded, (b) remains a pre-political tool, (c) makes complying with new regulation virtually impossible, and (d) fails to deliver on the old promise of the P2P movement by fostering an opaque, techno-hierarchical power structure unbounded by anyone's control. Moreover, such a DCS hides the value(s) that secondary rules should strive to foster, thus harming the legitimacy of the system itself (Barnett, 2003). Hence, I hold that the establishment of secondary rules might address the governance problem. I am aware that this line of reasoning might be subject to some objections, to which I now turn before showing how this solution differs from the ones mentioned in section 2.

i. There is no need for it.

The first objection that comes to mind is that there is no need for establishing secondary rules in the DCS landscape. This objection is quickly dismissed. First, there are already some quasi-constitutional principles embedded in some systems; e.g., the 21-million-coin cap in Bitcoin. Second, arguably many of the controversies result from the lack of a procedural framework according to which decisions are made. Finally, the lack of secondary rules of change undermines the wide-spread adoption of DCS since it increases risk and unpredictability while also possibly leading to fragmentation. Moreover, such rules would establish checks on core developers of DCS which, up until now, are unchecked safe for the possibility of forking the system (thereby electing another - unchecked - group of core developers). One can easily imagine a scenario where the benevolent dictatorship of a DCS loses the benevolent part; in this instance, the presence of clear secondary rules would swiftly highlight the event and prompt the ecosystem to react.

ii. Consensus on secondary rules would be impossible; thus, systems will fork.

This objection has some merit. Indeed, it is possible that in some DCS some users will refuse, or fail to agree, on the secondary rules; if this were the case, then probably a hard-fork will occur. Nonetheless, I argue that such an occurrence will be beneficial to the DCS space. After the original disagreement, systems which implement secondary rules will thrive and out-compete others, much in the same way as constitutional legal systems prevail in modern societies. More importantly, such systems are, arguably, more legitimate, just, and fair. Moreover, the presence of a clear governance structure of the network is likely to attract more investments and users given the lower risk factor. Lastly, governments will likely ban DCS systems that fail to comply with existing (or new) regulations.

iii. Secondary rules would hamper the ability of a DCS to evolve.

This objection is empirical. While it is possible that bad-designed systems of secondary rules will fail to perform at an acceptable level, if we assume that many different DCS will adopt different sets of rules, then one must concede that competition is likely to select the more efficient ones. That said, this objection also stands for current DCS, think, for example, of the block-size debate in the Bitcoin ecosystem. Nonetheless, even if the establishment of secondary rules would amount to an efficiency lost, it is still desirable for the respective gains in legitimacy, fairness, and predictability.

iv. On-chain governance rules are sufficient.

This objection is easily dismissed. On-chain rules exist only in so far as they presuppose higher, off-chain, rules. In other words, on-chain governance rules are merely an implementation of pre-supposed secondary rules that must to exist off-chain. As an example, Tezos implements on-chain governance rules in the form of allowing users to vote on changes to the protocol as well as the on-chain rules (Goodman, 2014); nevertheless, this design was adopted by the founder of the platform without off-chain secondary rules[24]. Moreover, by their nature, these rules would be difficult to implement in binary language, much in the same way as smart contracts fail to account for the complexities of natural language (Mik, 2017). Lastly, I argue that implementing complex governance structures on systems that are struggling to scale is an unnecessary overhead.

v. The establishment of an institutional body overseeing DCS is more desirable.

I disagree with this objection because it will not allow the DCS community to experiment with new and different modes of network governance. One exciting and promising aspect of this new technology is its ability to shape and enforce institutional arrangements by algorithmic rules (Wright & De Filippi,

[24] To be fair Tezos states the values according to which the system should operate, but it fails to design secondary rules to foster such values. Tezos values statement is available here https://medium.com/tezos/tezos-philosophy-and-values-9297f308ae21

2015). I hold that the establishment of an international body would prevent the flourishing of radical new solutions, after all, we should "*let them be peers*" (Pagallo, 2008). Additionally, such a display of political power would probably result in a rejection of the institutional body by much of the DCS communities.

vi. The blockchain is (already) a constitutional system.

Some authors informally argue that "*blockchains are constitutional orders – rule-systems in which individuals (or firms or algorithms) can make economic and political exchanges*" (Berg, Davidson, & Potts, 2018). They contend that "*blockchains look a lot like countries" and that "*[t]*he protocol (the constitution) resolves this problem* [consensus] *by incentivizing nodes to prefer the chain with the most work.*". The main problem I see in this account lies in the fact that virtually no DCS system has on-chain secondary rules. Consequently, blockchains lack one of the necessary conditions for a constitutional ordering: rules on how to make rules (see supra). At best, blockchains are clusters of primary rules enacted with no legitimacy nor regard to fundamental human values, that is, pre-political tools (Atzori, 2015; Atzori & Ulieru, 2017).

The approach of this study differs from the ones mentioned in section 2. I argue for the establishment of secondary rules, nothing else. This perspective leaves open the possibility of several modes of governance, be it one inspired by the corporate governance framework (Hacker, 2017), or on blind coordination games (Abramaowicz, 2016), radical markets (Posner & Weyl, 2018) direct democracy[25] or else. This is the crucial argument I put forward: whatever the conception of governance one holds the adoption of clear, and explicit secondary rules would benefit the whole DCS landscape. It would (among other things) prevent hard-forks that stem from ex-post solution to unforeseen problems as occurred, for example, with the DAO case (Campbell-Verduyn, 2018). Moreover, DCS that implement secondary rules would be legitimate in so far as they design secondary rules that foster the value(s) that inspire each system.

While I am aware of the century-old debate regarding constitutional legitimacy, I ought not to indulge in it to show how some literature on the topic provides useful insights for addressing DCS governance. I have argued that DCS that implement secondary rules would be more legitimate, I draw this conclusion from the work of Barnett on the topic of constitutional legitimacy (Barnett, 2003). He shows how constitutional legitimacy does not depend on the consent of the governed, but it arises when a constitution "*provides sufficient procedures to assure that the law enacted pursuant to its procedures are just*" (Barnett, 2003, p. 146).

Barnett adopts justice as the guiding principle following Lysander Spooner's work, according to whom "*Justice is evidently the only principle that everybody can be presumed to agree to, in the formation of government*"

[25] In spite of the teaching of the federalist papers as described by Werbach and Cornell (Werbach & Cornell, 2017)

(Spooner 1860, cited in Barnett 2003, p. 136). However, Justice is not the only base-value that could or should ground the legitimacy of a legal system nor of a DCS. In fact, at this stage, the presence of a governance structure of the network seems to be the only principle that everybody in the DCS ecosystem can be presumed to agree in the development of the software. Therefore, a set of secondary rules that constitute the governance structure ought to be implemented in DCS to fully foster the development of the technology and addressing its shortcomings. As Floridi puts it: "[…] *the most consequential challenge we are facing* […] *is* […] *how we are going to design the infosphere and the mature information societies developing within it that matters most*" (Floridi, 2018, p. 1). Simply put, whatever the governance models one believes is the right one to govern DCS it is of outermost importance that secondary rules are established.

The time is now ripe to sketch some design principles to establish secondary rules in the DCS space. The method of the LoAs provides the starting point to assess the peculiarities of each system, which ought to shape their respective secondary rules.

6. Directions on the way forward

The first categorization provided by LoA(1) - the distinction between Open/Closed systems- proves, again, essential. As mentioned, closed systems already implement a set of secondary norms in the likes of the contractual arrangements that govern the relationship between the entities that form a permissioned DCS. That said, LoA(1) also provides us with a second categorization on the basis of the value of the observable identified as computational complexity. In this respect, Turing-complete systems should implement different secondary rules than Turing-incomplete ones. Think, for example, of a rule establishing the procedure for an emergency shutdown of the network due to a rogue decentralized autonomous organization (DAO), albeit this seems farfetched the combination of DCS and AI could lead to unforeseeable events. Conversely, Turing-incomplete systems tend to be more predictable due to their limited functionalities; therefore, a different set of rules is needed. In other words, the issues raised by DCS systems are closely correlated with their computational complexity.

LoA(2) provides another distinction that may be made explicit by secondary rules In fact, such rules could be designed as to account for the role of a prominent figure (e.g., the founder of the system) or to account for the role of an institution in charge of the network; or both. What is relevant for our discourse is that power structures ought to be made explicit by off-chain secondary rules, thereby contributing to advance the DCS landscape as outlined in the previous section. Again, making explicit the relevance of persons or institutions in the governance of DCS does not necessarily imply strictly defining the methods and procedure according to which those entities ought to function; although, that is surely possible. In fact, many bodies of secondary norms do so[26].

[26] See, for instance, art. 1 of the Italian Constitution which establishes the democratic principle.

Finally, other LoAs could be adopted to analyze DCS as to highlight fundamental values and core differences that ought to shape the design of secondary rules or to identify the core value(s) of each system. This more granular level of epistemological inquiry lies beyond the scope of this paper. It should be the subject of further, extensive research. As a suggestion, one might adopt a LoA whose observables are the consensus algorithm, the distribution of mining power, the geographical reach of the network. Such an inquiry may provide the foundations upon which the designers of the system could devise secondary rules that dictate the governance of the network.

7. Conclusion

In this essay, I have argued for the use of a version of epistemological levelism in the analysis of the DCS landscape to understand each implementation better and to move beyond a level of analysis that only considers Bitcoin and Ethereum (section 1). Later, I outlined the leading literature on the topic of governance as it relates to DCS; this short literature review highlighted how most of the academic discourse focuses on the governance with and by the network. Conversely, the governance of the network is prominent because it influences the governance with or by the network. Section 3 provided some examples of the failures of governance in the DCS space with a focus on how such issues may result in a fatal clash with new regulations such as the GDPR. Section 4 showed the presence of the often-hidden, ideologies in the discourse surrounding this new technology in order to show how these architectures could (and to some extent already have) enable anti-democratic forms of governance. In section 5, I argued for the establishment of secondary rules to address the shortcomings of the governance of DCS. That is, a quasi-constitutional order for DCS system. The drafting of these off-chain norms has many advantages, among which: legitimacy, fairness, and predictability; these advantages could pave the way for widespread adoption of DCS systems. If DCS systems represent a social innovation and an institutional technology, then they should build on top of the legal and political science tradition as it will allow their designers to implement the correct ethical infrastructure to sustain the project of human flourishing. In addition, it could prevent DCS architects to reinvent the wheel or to repeat some mistakes. The task of drafting rules should, therefore, bring together experts from many fields and not become (as it is often the case) an afterthought. There are many challenges to overcome; nonetheless, the task is worth enduring if one wants to harness the full potential of the technology. Arguably, the governance of DCS amounts to what constitutes a DCS, although I admit the details of such governance are still an open issue that, nevertheless, ought to be made explicit.

Acknowledgments: This paper is an outcome of the Ph.D. research performed inside of the Joint International Doctoral (Ph.D.) Degree in Law, Science, and Technology, coordinated by the University

of Bologna, CIRSFID in cooperation with the University of Turin, Universitat Autònoma de Barcelona, Tilburg University, Mykolas Romeris University, The University of Luxembourg.

8. Bibliography

A. Zamyatin, N. S., A. Judmayer, P. Schindler, E. Weippl and W.J. Knottenblet. (2018). A Wild Velvet Fork Appears! Inclusive Blockchain Protocol Changes in Practice.

Abramaowicz, M. (2016). Cryptocurrency-based law. *Arizona Law Review, 58*, 359.

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

Ateniese, G., Magri, B., Venturi, D., & Andrade, E. (2017). *Redactable blockchain–or–rewriting history in bitcoin and friends*. Paper presented at the Security and Privacy (EuroS&P), 2017 IEEE European Symposium on.

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

Atzori, M., & Ulieru, M. (2017). Architecting the eSociety on Blockchain: A Provocation to Human Nature.

Azouvi, S., Maller, M., & Meiklejohn, S. (2018). Egalitarian Society or Benevolent Dictatorship: The State of Cryptocurrency Governance.

Baldwin, J. (2018). In digital we trust: Bitcoin discourse, digital currencies, and decentralized network fetishism. *Palgrave Communications, 4*(1), 14. doi:10.1057/s41599-018-0065-0

Barnett, R. E. (2003). Constitutional legitimacy. *Columbia Law Review, 103*, 111.

Berg, C., Davidson, S., & Potts, J. (2018). Crypto Constitutionalism

Bogost, I. (2017). Cryptocurrency might be a path to authoritarianism. *The Atlantic, 30*.

Buterin, V. (2014). DAOs, DACs, DAs and More: An Incomplete Terminology Guide.

Cachin, C., & Vukolić, M. (2017). Blockchains Consensus Protocols in the Wild. In *arXiv preprint arXiv:1707.01873* (Vol. 31st International Symposium on Distributed Computing).

Campbell-Verduyn, M. (2018). *Bitcoin and Beyond Cryptocurrencies, Blockchains, and Global Governance* (M. Campbell-Verduyn Ed.). New York: Routledge.

Davidson, S., De Filippi, P., & Potts, J. (2016). Disrupting governance: The new institutional economics of distributed ledger technology.

Davidson, S., De Filippi, P., & Potts, J. (2017). Blockchains and the economics institutions of capitalism. *Journal of Institutional Economics*.

De Filippi, P., & Loveluck, B. (2016). The Invisible Politics of Bitcoin: Governance Crisis of a Decentralised Infrastructure. *Internet Policy Review, 5*(3). doi:10.14763/2016.3.427

DuPont, Q. (2014). The politics of cryptography: Bitcoin and the ordering machines. *Journal of Peer Production, 1*(4), 1-10.

Floridi, L. (2008). The method of levels of abstraction. *Minds and machines, 18*(3), 303-329.

Floridi, L. (2011). *The philosophy of information*: Oxford University Press.

Floridi, L. (2017). Infraethics–on the Conditions of Possibility of Morality. *Philosophy & Technology, 30*(4), 391-394. doi:10.1007/s13347-017-0291-1

Floridi, L. (2018). Soft Ethics and the Governance of the Digital. *Philosophy & Technology, 31*(1), 1-8.

Galloway, A. R. (2004). *Protocol: How control exists after decentralization*: MIT press.

Golumbia, D. (2016). *The politics of Bitcoin: software as right-wing extremism*: University of Minnesota Press.

Goodman, L. (2014). Tezos: A self-amending crypto-ledger position paper. In.

Hacker, P. (2017). Corporate Governance for Complex Cryptocurrencies? A Framework for Stability and Decision Making in Blockchain-Based Monetary Systems. *vailable at SSRN: https://ssrn.com/abstract=2998830 or http://dx.doi.org/10.2139/ssrn.2998830*.

Hart, H. L. A., & Green, L. (2012). *The concept of law*: Oxford University Press.

Hearn, M. (2015). Why is Bitcoin forking. Available here: https://medium.com/faith-and-future/why-is-bitcoin-forking-d647312d22c1

Joerges, B. (1999). Do Politics Have Artefacts? *Social Studies of Science, 29*(3), 411-431.

Jun, M. (2018). Blockchain government - a next form of infrastructure for the twenty-first century. *Journal of Open Innovation: Technology, Market, and Complexity, 4*(1), 7. doi:10.1186/s40852-018-0086-3

Kroll, J. A., Barocas, S., Felten, E. W., Reidenberg, J. R., Robinson, D. G., & Yu, H. (2016). Accountable algorithms. *U. Pa. L. Rev., 165*, 633.

Lehdonvirta, V. (2016). The blockchain paradox: Why distributed ledger technologies may do little to transform the economy.

Manski, S., & Manski, B. (2018). No Gods, No Masters, No Coders? The Future of Sovereignty in a Blockchain World. *Law and Critique*. doi:10.1007/s10978-018-9225-z

Matzutt, R., Hiller, J., Henze, M., Ziegeldorf, J. H., Müllmann, D., Hohlfeld, O., & Wehrle, K. (2018). *A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin.* Paper presented at the Proceedings of the 22nd International Conference on Financial Cryptography and Data Security (FC). Springer.

Mik, E. (2017). Smart contracts: terminology, technical limitations and real world complexity. *Law, Innovation and Technology*, 1-32.

Pagallo, U. (2008). Let them be peers: the future of p2p systems and their impact on contemporary legal networks. *Eur. J. Legal Stud., 2*, 234.

Pagallo, U. (2017). The legal challenges of big data: putting secondary rules first in the field of EU data protection. *Eur. Data Prot. L. Rev., 3*, 36.

Pagallo, U., & Durante, M. (2009). Three Roads to P2P Systems and Their Impact on Business Practices and Ethics. Journal of Business Ethics, 90(4), 551-564. doi:10.1007/s10551-010-0606-y

Popper, N. (2015). *Digital gold: Bitcoin and the inside story of the misfits and millionaires trying to reinvent money*: Harper New York.

Posner, E. A., & Weyl, E. G. (2018). *Radical Markets: Uprooting Capitalism and Democracy for a Just Society*: Princeton University Press.

Puddu, I., Dmitrienko, A., & Capkun, S. (2017). μchain: How to Forget without Hard Forks. *IACR Cryptology ePrint Archive, 2017*, 106.

Ramsay, S. (2018). The General Data ProtectionRegulation vs. The Blockchain: A legal study on the compatibility between blockchain technology and the GDPR. Stockholm University.

Reijers, W., O'Brolcháin, F., & Haynes, P. (2016). Governance in Blockchain Technologies & Social Contract Theories. *Ledger, 1*, 134-151.

Sclavounis, O. (2017). Understanding Public Blockchain Governance.

Scott, B. (2015). Visions of a Techno-Leviathan: The Politics of the Bitcoin Blockchain.

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

Swan, M. (2017). Anticipating the Economic Benefits of Blockchain. *Technology Innovation Management Review, 7*(10), 6.

Sward, A., Vecna, I., & Stonedahl, F. (2018). Data Insertion in Bitcoin's Blockchain. *2018, 3*. doi:10.5195/ledger.2018.101

Walch, A. (2017). The path of the blockchain lexicon (and the law).

Werbach, K. D., & Cornell, N. (2017). Contracts Ex Machina.

Winner, L. (1980). Do Artifacts Have Politics? *Daedalus, 109*(1), 121-136.

Wright, A., & De Filippi, P. (2015). Decentralized blockchain technology and the rise of lex cryptographia.

Xu, X., Weber, I., Staples, M., Zhu, L., Bosch, J., Bass, L., . . . Rimba, P. (2017). *A Taxonomy of Blockchain-Based Systems for Architecture Design.* Paper presented at the Software Architecture (ICSA), 2017 IEEE International Conference on.