Alma Mater Studiorum – Università di Bologna
in cotutela con Université du Luxembourg

DOTTORATO DI RICERCA IN LAW, SCIENCE, AND TECHNOLOGY – LAST-JD

Ciclo XXXII

Settore Concorsuale: IUS/20

Settore Scientifico Disciplinare: 12/H3

The Authority of Distributed Consensus Systems: Trust, Governance, and Normative Perspectives on Blockchains and Distributed Ledgers

Presentata da: ***Crepaldi Marco***

Coordinatore Dottorato

Prof. Monica Palmirani

Supervisore

Prof. Ugo Pagallo

Co-supervisore

Prof. Sjouke Mauw

Esame finale anno 2020

ABSTRACT

The subjects of this dissertation are distributed consensus systems (DCS). These systems gained prominence with the implementation of cryptocurrencies, such as Bitcoin. This work aims at understanding the drivers and motives behind the adoption of this class of technologies, and to – consequently – evaluate the social and normative implications of blockchains and distributed ledgers. To do so, a phenomenological account of the field of distributed consensus systems is offered, then the core claims for the adoption of systems are taken into consideration. Accordingly, the relevance of these technologies on trust and governance is examined. It will be argued that the effects on these two elements do not justify the adoption of distributed consensus systems satisfactorily. Against this backdrop, it will be held that blockchains and similar technologies are being adopted because they are regarded as having a valid claim to authority as specified by Max Weber, i.e., *herrschaft*. Consequently, it will be discussed whether current implementations fall – and to what extent – within the legitimate types of traditional, charismatic, and rational-legal authority. The conclusion is that the conceptualization developed by Weber does not capture the core ideas that appear to establish the belief in the legitimacy of distributed consensus systems. Therefore, this dissertation describes the *herrschaft* of systems such as blockchains by conceptualizing a computational extension of the pure type of rational-legal authority, qualified as algorithmic authority. The foundational elements of algorithmic authority are then discussed. Particular attention is focused on the idea of normativity cultivated in systems of algorithmic rules as well as the concept of decentralization. Practical suggestions conclude the following dissertation.

CONTENTS

1.Introduction

The subjects of this dissertation are blockchains and distributed ledgers (aka distributed consensus systems). I first encounter a blockchain, like many others, when studying the cryptocurrency Bitcoin. It is not rare for one to start looking at cryptocurrencies out of academic curiosity and then exhibit the symptoms of the so-called blockchain fever. The severity of this condition varies, and it may increase with the publishing of books and articles concerned with explaining how this class of technologies will, sooner rather than later, disrupt entire sectors of the economy, eradicate corruption and, finally, dispose of intermediaries (Swan, 2015; Tapscott & Tapscott, 2016; Vigna & Casey, 2018). The argument goes something like this. Fist premise, Bitcoin uses a data structure named, blockchain or block chain. The Bitcoin's blockchain enables it to maintain a single ledger of transactions that (a) is accessible to every participant in the network (b) contains all the transactions ever occurred in the system (c) uses cryptography to secure the data and provide integrity (d) is maintained by members of the network on a voluntary basis and (e) is not administered by a single entity. Second premise: Bitcoin is decentralized money because it uses a blockchain. Conclusion: a blockchain with the same properties of the Bitcoin one does for x what Bitcoin did for money. With some simplification, this appears to be the underlying logic of the blockchain revolution. Of course, holders of this view will not hesitate to add several further arguments as to why blockchains will, indeed, be revolutionary. Perhaps by pointing to the importance of double-entry bookkeeping or to the method to ensure the reliability information in ancient Mesopotamia (C. Berg, 2017; Vigna & Casey, 2018). It should be noted that the further away a system is from the original Bitcoin design, the less experience and understanding there is regarding its viability and plausibility.

In this work, I examine the arguments for the blockchain revolution by answering the following question. Why do people, firms, governments and institutions adopt blockchains and distributed ledgers? In other words, why, given a choice to blockchain or not to blockchain, a significant number of agents

are considering the former? To answer this, it is first necessary to examine if the most prominent claims about the properties of blockchains and distributed ledgers suffice to explain why people 'do' blockchain. Accordingly, the first part of this work deals with the effects of this class of technology on the issues of trust and governance. Moreover, the research question of this work entails examining the first premise of the argument by studying what makes Bitcoin decentralized money in the first place. Recently, the prospect of doing things with blockchains and similar data structures that are often described as distributed ledger technologies has moved beyond the cyber-libertarian origin of Bitcoin. Interestingly, there is a significant engagement of the public sector with these new technologies (Ølnes & Jansen, 2018; Shahaab, Lidgey, Hewage, & Khan, 2019).

Reports from public institutions appear to support the adoption of the technology at some level, and several initiatives are either underway or planned in many countries (OECD, 2019). Recent developments add to the relevance of an in-depth analysis of 'why to blockchain.' Think, for example, as the Libra initiative that is making headlines around the world and suscitating opposite reactions from policymakers worldwide (Khan & Goodell, 2019). Libra aims to be a global currency and financial infrastructure built on a blockchain, backed by a basket of fiat currencies and governed by the Libra association whose most prominent member is Facebook Inc. (Libra Association, 2019). In a joint statement, France and Germany agreed to block Libra's project, by stating that "no private entity can claim monetary power, which is inherent to the sovereignty of nations" said French Finance Minister Bruno Le Maire.[1] It is an open question if the Libra association would have been born without the innovation brought about blockchains. Nonetheless, it adds relevance to understanding what the fuss is about in the context of blockchains and distributed ledgers.

[1] https://www.reuters.com/article/us-facebook-cryptocurrency-france-german-idUSKCN1VY1XU

On this basis, it is relevant to point out the following distinction. To blockchain does not mean to use or develop a system for the transfer of value over the internet, e.g., a cryptocurrency. While cryptocurrencies generally presuppose a blockchain architecture, blockchains may exist without cryptocurrencies as a method to manage information. Therefore, the x in the basic argument for the blockchain revolution might be anything provided it is based on the need for trustworthy information. To take distance from shady cryptocurrencies, government reports usually adopt the term of distributed ledger technology (or DLT). DLT include blockchains and belong to the category of distributed consensus system (see chapter 2). There are several reasons as to why public bodies - along with other institutions - attempt to distinguish their engagement with the technology from dubious methods of payments based on peer-to-peer networks and cryptography.

First, cryptocurrencies may facilitate money-laundering, terrorist financing, and tax evasion (De Vido, 2019; Marian, 2013). Second, it is known that cryptocurrencies are widely used to purchase illegal goods and services from the dark web. Throughout the next pages, the terminology of blockchains and distributed ledgers will be adopted to represent the broader area of distributed consensus systems (Glaser & Bezzenberger, 2015). For most of the current and proposed implementations, make use of a distributed ledger often organized as a blockchain. It is important to note that I will not deal with the aforementioned legal concerns related to cryptocurrency in this work[2].

This introductory chapter deals first with the methodology of this work. A significant challenge of interdisciplinarity is to preserve methodological rigor while hopping - out of necessity - to other disciplines other than one's own. This is necessary because the subject at hand demands an interdisciplinary approach, for it blends notions from several disciplines so that a mono-disciplinary account would likely be unsatisfactory (van Klink & Taekema, 2008). Then, the section 1.2 summarizes

[2] See the following sources for a thorough legal analysis of the issues associated with cryptocurrencies (Finck, 2019; Fulmer, 2019; Gilcrest & Carvalho, 2018; Girasa, 2018; Herian, 2018b; Ibáñez, O'Hara, & Simperl, 2018; Low & Mik, 2019; Naves et al., 2019; Pagallo, Bassi, Crepaldi, & Durante, 2018; Pflaum & Hateley, 2013)

each of the following chapter to provide the reader with a map for navigating and understanding this work.

1.1 Notes on methodology

The field of legal philosophy provides the methodological foundation for this work. However, specific chapters may borrow other methodological techniques. This section first discusses the overarching methodology of this dissertation, later it mentions other methods of investigation adopted in single chapters.

Legal scholars engaged in philosophical inquiry made insightful contribution to the understanding of systems of rules. The set of all the rules - explicit or implicit - studied by legal philosophers within a jurisdiction is the law of that jurisdiction, or, more broadly the normative environment of a given polis[3]. Regardless of the ontological status of laws, it is possible to conceptualize legal norms as logical propositions, think, for example, to the consequentialist formula of Hermann Cohen and Hans Kelsen: "If A, then B ought to follow" (Kelsen, 1967). Other normative structures relevant from the perspective of the legal philosopher are co-regulation and self-regulation (Pagallo, Casanovas, & Madelin, 2019). Against this backdrop, this section defines the type of interdisciplinary research developed throughout this work.

There are four types of interdisciplinary legal research, divided into two groups: basic and advanced. According to the taxonomy of interdisciplinary legal research put forward by Siems, this work belongs to the type 1 of advanced interdisciplinary research (Siems, 2009). In other words, the perspective adopted allows me to deal with problems and issues that are not strictly legal. I chose this perspective

[3] In the sense of a body of citizens, (Estella de Noriega, 2002)

because the technological phenomena at hand demands a broader viewpoint. In particular, the implications of blockchains and distributed ledgers would arguably be either exaggerated or underrated if the focus was only put on legal matters with little regard to the technical aspects or sociological implications. More specifically, this perspective is conducive to study blockchains and distributed ledgers as system of rules and to explore their legal, that is *de lege ferenda,* implications. Concerning our subject, philosophical, sociological, and policy considerations - as well as technical innovation from the field of cryptography and distributed computing - ought to be taken into account. This is not to say that legal questions will not be considered when appropriate or that legal scholarship will not be foundational to this work. However, the sources and the problems discussed in the following pages may not be considered legal, strictly speaking. The same can be said about the overreaching research question of this work, namely, why do people, institutions, and companies use or engage with blockchains and similar technologies. Note that the previous question is relevant even if these actors are merely considering entering the blockchain arena. In fact, the research question is not *prima facie* legal, yet it has legal implications.

Another reason to adopt the type 1 perspective is that blockchains and distributed ledgers are systems of logical rules. Chiefly, the medium in which blockchains' rules are expressed is computer code, while legal norms are often expressed with natural language or, sometimes, symbols. Think, for example, as the speed limit, which is generally displayed symbolically when one enters a jurisdiction. Then, it is interesting to examine how different ways of expressing logical rules affect the operation of each system. And, perhaps if the thrust behind blockchains and distributed ledgers has something to do with the increasing reliance on algorithmic system of techno-regulation (Brownsword & Yeung, 2008; Goodwin, Koops, & Leenes, 2010).

The methodological perspective adopted, also, enables us to establish a shared vocabulary to study the technical aspects of blockchains and distributed ledgers along with their social and legal implications. Establishing a common terminology is essential when terms have distinct meanings across disciplines as

the next example makes clear. Let us consider a term that is all-pervasive in the context of these technologies: decentralization. Lawyers have a model of the concept of decentralization, which arguably differs from the perspective of software engineers. For the latter, it describes the structure of a network and how different tasks are partitioned. Software engineers might regard decentralization in the context of blockchains, as the fact that no single entity has control over all the processing. Alternatively, decentralization might just be understood as a metric in the context of engineering specifications, i.e., "[w]e use centralization level to formally define decentralization of blockchains. A blockchain is N(e) centralized if the top N nodes performed more than 1- (e) fraction of transactions" (Wu, Peng, Xie, & Huang, 2019, p. 2). For the formers, instead, it does not describe networks; rather, lawyers might think of decentralization as a "common and variable practice in most countries to achieve primarily a diverse array of governance and public sector management reform objectives"(UNDP, 1999, p. 1). Conversely, it is evident how problems might occur if differences in terminology are not leveled; this is possible by adopting the type 1 interdisciplinary legal viewpoint.

However, a single methodology would not suffice. Hence, different chapters adopt – when needed - other methodological techniques to properly assess why blockchains are relevant and are being implemented across many sectors. The task of describing each method is postponed to the beginning of the chapter wherein it will be adopted, for now, a brief overview of the techniques adopted is enough. Chapter 2 borrows the phenomenological method as elaborated by Heidegger in the masterpiece Time and Being (Heidegger, 1996). Chapter 3 examines different notions of trusts found in the philosophy of technology literature as well as in the sociological work of Niklas Luhmann (Luhmann, 1979). Chapter 4 uses the method of the levels of abstraction as developed by Floridi (Floridi, 2008, 2011) while chapters 6 and 7 engage in a sociological analysis of the authority of blockchains and distributed ledgers and, consequently, draw upon the method of investigation adopted by Max Weber (M. Weber, 2012).

Lastly, a few words on the type of sources referenced in this study are in order. Sources from the grey literature are included out of necessity to account for the multitude of technological solutions developed

for blockchains and distributed ledgers. In particular, among the research produced by organizations outside traditional commercial or academic publishing, white papers are worth mentioning. This is because, since the inception of Bitcoin, important developments have been announced in white papers. Therefore, this type of grey source is referenced throughout this work when appropriate. Occasionally, sources from blog posts and web pages will be cited to provide the reader with a better understanding of the debates within the communities that are developing blockchains and distributed ledgers. Such sources will be more prevalent when dealing with issues such as governance and forks while almost absent in the chapters dealing with other questions. The inclusion of such materials is essential to better understand the ideas that support the adoption and development of blockchains and distributed ledgers. On this basis, the next section maps this dissertation by summarizing each of the ensuing chapters.

1.2 Outlook

When considering possible explanations for why agents use or engage with blockchains and distributed ledgers, several options come to mind. On the one hand, one could make the case that these technologies improve the current situation incrementally. That is, they enable agents to achieve the same goals more efficiently (Catalini, 2017). While this might hold in limited contexts, the narrative that pushes blockchains and distributed ledgers forward appears different. Proponents of the technology often consider it revolutionary or - at a minimum - capable of disrupting several economic sectors. But what exactly is regarded as revolutionary? Or, which is equivalent, what are distributed consensus systems? Before developing any argument, it is necessary to make clear what this work is about. To do so, chapter 2 defines the object of this study. Then, the first argument as to why people and institutions are engaging with distributed consensus systems is examined in the next chapter. Accordingly, chapter 3 examines the influence of blockchains and distributed ledgers on trust. The claim is that these technologies remove or drastically reduce the need for trust to carry out transactions, i.e., that they enable trustless trust (Werbach,

2017). After all, it is argued that Bitcoin is a payment system with no trust. On this basis, chapter 3 examines different accounts of trust before evaluating under which conditions - and to what extent - blockchains and distributed ledgers reduce or even eliminate trust. More importantly, the cost of reducing the need for trust by trusting computations will be considered. It is possible to anticipate that important distinctions ought to be made concerning the type of assets, the design of each network, and how users access each system. Particular attention will be directed toward the relation among trust, reliability, and control under the framework established by Niklas Luhmann (Luhmann, 1979). Chapter 3 concludes by arguing that the adoption of blockchains and distributed ledgers is not justified solely on their effects on trust. These effects are limited to specific instances and are not a consequence of the adoption of the technology per se. Additionally, the eventual reduction in the level of trust is granted by control.

Chapter 4 then examines the second main argument as to why agents should engage with distributed consensus systems. The argument is that blockchains and distributed ledgers enable new modes of governance. To examine the previous claim, chapter 4 begins by distinguishing three distinct aspects related to governance, namely governance by, with or of blockchains and distributed ledgers. Then, it examines how popular systems function at the different levels of governance and describes their limitations by analyzing real-world episodes in which the governance of these networks broke down. On this basis, chapter 4 describes the limitation of blockchains and distributed ledgers from the governance perspective by pointing out a crucial difference with another co-ordination system of rules, namely, the law. It argues that blockchains and distributed ledgers are, in the current state, incomplete system of rules because they lack what has been described in legal philosophy as secondary rules (Crepaldi, 2019). Based on the conceptual incompleteness of blockchains and distributed ledgers, chapter 4 concludes that the adoption of this class of technologies is not justified based on their ability to establish new modes of cooperation. The real issue does not lie in which rules are hard-coded into these networks, rather, it depends on how such rules are agreed upon, and amended.

In light of the previous findings, chapter 5 asks what other factors might explain the engagement with blockchains and distributed ledgers. It argues that these technologies are being used or adopted because they are believed to have a valid claim to legitimacy. In other words, what might explain blockchains' adoption is that (a) they are perceived as the proper means to specific ends and (b) they are considered a better alternative to other competing mechanisms. The introduction of the notion of legitimacy demands some clarifications. Therefore, chapter 5 untangles the notion of legitimacy by studying it at three different perspectives: the philosophical, the legal, and the sociological. Once the meaning of legitimacy has been clarified, chapter 5 defends the choice of adopting the sociological account to answer the main research question. Then, it introduces the methodology of Max Weber and sets the stage for the next chapters (M. Weber, 2012).

Later, chapter 6 applies Weber's methodology to current distributed consensus systems. It describes each of the pure types of imperative co-ordination developed by the German sociologist and evaluates if they explain the adoption and use of blockchains and distributed ledgers satisfactorily. Consequently, it first describes the pure type of traditional authority and examines the Bitcoin system. It describes its social and technical characteristics that can be accounted for on the basis of traditional authority.

Then, it deals with the pure type of charismatic authority considering the Ethereum and TRON systems before turning its attention to the pure type of rational-legal authority, and two other systems, namely, EOSIO and Decreed. In this context, it describes the social and technical arrangements of each of these four systems and describes how their salient elements can be explained readily if their authority is established on elements proper of the Weberian pure types. Chapter 6 concludes that other reasons appear to establish the belief in the legitimacy of blockchains and distributed ledgers beyond the elements described by Max Weber.

Building upon the aforementioned discussion, chapter 7 studies the elements upon which the authority of blockchains and distributed ledgers is established. That is, it explores the salient characteristics that are put forward as reasons for the engagement with blockchains and distributed ledgers. It finds that the

belief in the following ideas appears to establish the legitimacy of distributed consensus systems in their ideal state. These ideas are transparency, openness, decentralization, security, deterministic operations, absence of a bureaucratic staff, and voluntarily subjection. This chapter concludes that an extension of the Weberian pure type of rational-legal authority, qualified as algorithmic authority, is needed to explain the engagements with blockchains and distributed ledgers. In other words, it argues that the ideas on which systems such as blockchains and distributed ledgers operate are distinct form the ones that grant authority to systems of rules based on tradition, charisma, or the impersonal legal order. So that, the basis on which the authority of distributed consensus system is cultivated escapes the Weberian classification. On this basis, it describes the ideas that establish the authority of the systems subject of this work.

Then, chapter 8, engages with examining the consequences of the belief in the authority of algorithms from the perspective of the normative operations of blockchains and distributed ledgers (aka cryptolaw). It describes crucial elements of cryptolaw by comparing it to the law of nation states in the western tradition. Chapter 8 also recovers the issue of decentralization to deepen the analysis. It first provides a more precise definition from the one offered in section 7.3.1. Then, it touches upon the relevance of this notion, albeit briefly, before examining how systems such as blockchains and distributed ledgers could decentralize effectively. Lastly, the conclusion summarizes the main findings of each chapter and ends this dissertation.

2.The Phenomenology of Distributed Consensus Systems

The landscape of distributed consensus systems is evolving in rapidly. One struggles to make sense of the different terms adopted in the discourse surrounding this nascent field. For example, the concept of blocks of data linked together by cryptographic means is sometimes described to as blockchain, block chain, Blockchain, or distributed ledger. The field is driven by the recent boom of cryptocurrencies, both in value and numbers, at the moment of writing, there are 3041 cryptocurrencies[4], with a total market capitalization of 205 billion USD. The link between the rise of cryptocurrencies and the interests in distributed consensus systems stems from the fact that virtually every cryptocurrency implements a version of a blockchain, or block chain, or distributed ledger. While various implementations may differ in relevant ways (such as money supply schemes, issuance policy, messaging protocol, and so on), virtually everyone implements a distributed data structure to reach consensus on system states (Bano et al., 2017, p. 356). This chapter aims to make sense of the concepts beyond the buzzwords and to provide a conceptual framework for the rest of this work. At the onset, it must be noted that blockchains are a species of the genus of distributed ledger technologies, that, together with directed acyclic graphs (hereinafter, also, DAGs) are a species of the genus of distributed consensus systems (Glaser & Bezzenberger, 2015).

The great innovation of distributed consensus systems is their ability to reach consensus on a particular state without relying on a trusted third party or central authority. In other words, blockchains and distributed ledgers enable mutually distrusting parties to reach agreement on a single record of the state machine of the network, in a way that prevents information to be managed by a single entity. The

[4] Data retrieved from https://coinmarketcap.com/ on the 25th of October 2019.

excitement around this field has produced substantial literature at many different levels, including, academia, institutions, governments, and industry (Casino, Dasaklis, & Patsakis, 2018; Oshodin, Molla, & Ong, 2016). The result of such a rapid interest is fragmentation and lack of consistency at almost every level of discourse (Walch, 2017). Additionally, because this field lies at the intersection of several disciplines such as cryptography, distributed computing, game theory, economics, sociology and law, terminology is, no doubt, a challenge to address. On this basis, this chapter adopts a philosophical method of investigation to shed light on the building blocks of these technologies and to expose the clogs in the distributed consensus machinery. The goal is to describe precisely the most relevant components of distributed consensus networks as well as their logical structure.

This chapter, then, deals with the understandable misunderstandings that arise when different disciplines interact using different concepts, and vocabularies. Consistency demands it. No agreed-upon definition of the critical components of a distributed consensus system exists; concepts change their meaning depending on the context. Hence an analytical approach is put forward to examine these systems from the perspective of experience. Accordingly, a phenomenology of the distributed consensus systems is offered. Martin Heidegger devised the phenomenological method of investigation that informs the current analysis (Heidegger, 1996). The next paragraphs describe the method developed by the German philosopher.

Heidegger's methodology employs three levels of analysis. At the first level, the method analyses the phenomenon, that is, "what shows itself in itself, what is manifest" (*ibidem,* p. 25). The task is to define what the object of analysis is by way of its manifestation. In other words, this methodology starts by answering the following question: What is the phenomenon? Then, at the second level, the phenomenological method deals with the logos of the phenomenon. According to Heidegger the logos is the ratio, the meaning of relation and relationship. Consequently, the second methodological step exposes the ratio of the phenomenon under investigation. The investigation of the logos, thus, answers the following question: what is the phenomenon for? The logos is the purpose of the object under

investigation, which – in the present case – are distributed consensus systems. Lastly, the third level of this methodology examines the conditions of possibility of the phenomenon, that is, what enables the phenomenon to exist. Simply put, the conditions of possibility describe the elements that enable the phenomenon under consideration to manifest itself, i.e. to exist. By leveraging this methodology this dissertation attempts to analyse the basic concepts of distributed consensus architectures in order to highlight differences and commonalities. Architectures matter, blockchains and distributed ledgers are no exception (Winner, 1980).

Another methodological note is necessary. This work adopts a bottom-up approach; it examines the software stack of DC systems by moving from the level of data structures to the one of smart contracts. The phenomena under scrutiny carry normative implications for development and designs of these systems. For example, the choice of a Turing-complete scripting language influences the functionality of the system, therefore the phenomena of scripting languages is selected. Consequently, not every single component of, for example, the Bitcoin software stack, is considered in the following analysis. Yet, enough components are examined and discussed through the phenomenological lenses to provide the reader with a thourgouh understanding of the many implementations in the DCS landscape. This chapter lies the foundation to build up our analysis concerning why blockchains and similar systems are being used and on what grounds their adoption is advocated. It is important to note that no such thing as the blockchain, or the distributed ledger technology exists, rather different systems and designs borrow common principles to achieve different, yet sometimes similar objectives. Consequently, it is necessary to meet with skepticism sources that deal with the blockchain technology as it is likely an indicator of a categorical mistake.

This chapter evolves as follows; section 2.1 addresses the phenomena of data structures; section 2.2 describes other relevant components of the DCS stack such as network structure, nodes, and scripting language. Section 2.3 analyses the consensus algorithms, while section 2.4 examines the so-called smart contracts.

2.1 The Structures of Data

In information systems, the choice of how to manage and structure information often leads to distinct data structures, i.e. a blockchain might be adopted when there is a need for a tamper-evident, append only data structure as opposed to a traditional database (Dinh et al., 2017). This section deals with the distinct data structures developed to organize information among distributed consensus systems.

At a given level, information is considered information about reality in terms of data space; more narrowly, information can be though as the object around which an information system is designed (Floridi, 2010, 2011). Therefore, different choices in the management of information result in correspondingly different data structures. In the field of distributed consensus systems, there are three types of data structures, namely, blockchains, distributed ledgers, and directed acyclic graphs. It must be noted that, at the time of writing, the majority of distributed consensus systems organizes information with blockchains. This is not surprising if one considers the following two factors. First, Bitcoin – the original cryptocurrency uses a blockchain to manage and distributed information. Second, most of the later implementations heavily borrowed from Bitcoin's original design. However, the presence of other mechanisms to manage information should not be disregarded if a complete analysis of the technological landscape is attempted. In the following pages, a reference architecture is selected to perform the phenomenological account.

Accordingly, the Bitcoin system is considered as the archetype of blockchains (Nakamoto, 2008). Corda, instead, is chosen as an example of a distributed ledgers data structure (DL) for it was among the first proposal of leveraging the benefits of this new class of technology in a closed system, and its lead engineer is a former Bitcoin core developer (Brown, Carlyle, Grigg, & Hearn, 2016). Lastly, IOTA will be considered as an example for DAG, because it has the largest market capitalization among DAGs and for the precise documentation it offers compared to other implementations such as Hedera (Baird, 2016; Popov, 2018). Let us examines each data structures in turn.

The first way to manage information is via a blockchain. Because most cryptocurrencies are adaptations of the original Bitcoin design most of the subsequent remarks extends to them (Tschorsch & Scheuermann, 2016). The phenomena grouped under the term blockchain are data structures in which information is stored in blocks that are cryptographically linked together, hence the terminology. That is, a data structure wherein the information is (a) organized in blocks (b) replicated across nodes (c) linked together such that any alteration of the information stored in block n requires the modification of all subsequent blocks (n+1, n+2, n+3 and so on). Blocks are added to the blockchain by means of a consensus algorithm, which will be discussed later. If all the above conditions hold when observing a phenomenon then it is a blockchain.

The logos of a blockchain is controversial as it depends on the possible uses of blockchain-based systems. Some authors claim that the blockchain is a general-purpose technology while others disagree. Sinclair et al., for example, consider blockchains as a general purpose technology, they write: "[o]ur argument is that blockchain – or distributed ledger technology [sic] – is neither a production nor an exchange technology per se […] but it is better understood from the economic perspective as an institutional technology" (Davidson, De Filippi, & Potts, 2017, p. 2). Others, such as Swan even go as far as to regard the affordances enabled by blockchains as blueprint for a new economy (Swan, 2015). On the other side of the argument, authors such as Gerard do not consider blockchains useful even in the context of cryptocurrencies (Gerard, 2017). For the moment, it is still unclear which side will end up being right. However, it is likely that the correct position lies somewhere in the middle. Concerning our purposes, the logos of the original Bitcoin blockchain is the focus of this phenomenological account. This is because the current investigation is concerned with what blockchains are used at this moment in time.

First and foremost, the Bitcoin blockchain enables electronic cash, that is, it was invented as the data structure of a peer-to-peer electronic cash system (Nakamoto, 2008). Consequently, the logos of blockchains is to record systems states for enabling P2P transactions. In the case of Bitcoin, system states are the transactions; metaphorically a blockchain is a massive spreadsheet that stores transactional entries

between the participant i.e. Alice send 5 unit to Bob, Bob sends 3 units to Charlie and so on (Wattenhofer, 2016). In systems that adopt this data structure, blockchains are the output of the consensus algorithm and they are the only authoritative source for the nodes in the network with regard to important parameters such as the balance of accounts (Narayanan, Bonneau, Felten, Miller, & Goldfeder, 2016).

Second, the Bitcoin blockchain tracks the bitcoin[5] in circulation. Additionally, it increases the supply of the bitcoins in the system with the so-called coinbase transactions[6]. In Bitcoin the node which is entitled to add a new block to the blockchain will add a transaction to itself, thus minting new bitcoins. The logos of the blockchain is also to provide integrity to the system. That is, it addresses the single point of failure (SPoF) problem of distributed computing by replicating itself across all the nodes; the blockchain achieve resiliency through redundancy (Yli-Huumo, Ko, Choi, Park, & Smolander, 2016). Finally, the Bitcoin blockchain addresses the hard problem of double-spending in the context of digital cash by establishing a digital original, namely each bitcoin is a unique sequence of digital signatures stored in the blockchain (Narayanan et al., 2016). Interestingly, bitcoins do not exist outside their own blockchain.

Often, some emergent properties of blockchains are mistakenly believed to be their logos. While this conceptual step might be unwarranted, it is the underlying assumption that drives blockchains projects beyond cryptocurrencies. Among such properties, one finds transparency, tamper-proofness, persistency, and traceability (Conte de Leon et al., 2017; Iansiti & Lakhani, 2017). While these properties can, and do, arise in some blockchain-based systems, they ought not to be regarded as the logos of this data structure, at least strictly speaking. Primarily, such properties are a by-product of enabling a peer-to-peer electronic cash system by means of an open distributed network which addresses the problem of double spending. One, therefore, should think of such properties as emergent rather than inherent. This

[5] I use the term Bitcoin with the capital B to refer as the system as a whole while the one with the lower-case b to refer to single coins (or fractions thereof).

[6] The coins in the system can also be *pre-loaded* and assigned at the moment the blockchain is created, in this case some coins (or all of them in some cases) are added to the system in the genesis block, that is, the first block in the blockchain.

conceptual shift explains why in ten years no one has found a use case for a blockchain as prominent as the transfer of cryptocurrencies. Once the purpose of the blockchains has been established, the next step of Heidegger's methodology is to examine the condition of possibility of blockchains. That is, how are blockchains possible?

There are some obvious conditions of possibility of blockchains, namely, electricity, computers, a network of networks, cryptography, a transport protocol and so on. However, this section focuses on the conditions of possibility at a higher level, so that blockchains can be distinguished from other ICT. For example, a blockchain needs several nodes to represent a viable solution. Clearly, a blockchain with two nodes makes little sense, and would not be perceived as such. On the contrary, lack of hierarchy at the architectural level is not necessarily a condition of possibility of blockchains[7]. This means that the presence of validating nodes as in the case of systems based on the delegated proof-of-stake family of algorithms, does not exclude the presence of a blockchain in the phenomenological sense developed in this chapter (Cachin & Vukolić, 2017). Pace Bitcoin maximalist[8].

Another condition of possibility of blockchains is a shared intention between the participants. Namely, given that blockchains require a certain number of nodes to operate, cooperation among them (or of a significant fraction) is necessary. In other words, a shared intention for what the purpose of the blockchain is a condition of possibility in itself (Bratman, 2013). This shared intention varies from system to system, and when it crumbles systems and communities split. Without the cooperation of at least the majority of the nodes (the famous 51% threshold), blockchains cannot operate at the conceptual level because it is not possible to prevent double spending if the majority on the nodes is behaving maliciously. This conditions also explains the sheer number of different blockchains out in the wild. On a technical

[7] A prominent example of blockchain where only selected nodes perform specific network functions is EOS (Xu, Luthra, Cole, & Blakely, 2018).

[8] The term refers to a philosophical position identified by the belief that the only real block chain (the term is used with a space because this is how it was first written by Bitcoin's creator) ought to be praised and supported. Accordingly, maximalist believe that other solutions should not be supported.

level, this shared intention is reflected by the specification of the data that the blockchain is designed to store. In practice, it ranges from unspent transactions outputs (Bitcoin) to computational results (Ethereum).

Finally, at a different level of abstraction several technical conditions of possibility exist that may not be obvious. For example, a sound set of cryptographic algorithms to link blocks together, a communication protocol and so on. These elements do not deserve much attention due to their lack of implications in the present theoretical framework, but there is an exception. The mechanism according to which nodes determine how new information is appended to the blockchain, namely the consensus algorithm. All consensus algorithms must tolerate Byzantine behavior of a subset of nodes. This implies that a viable algorithm to solve the Byzantine Generals problem is another condition of possibility of blockchains (Cachin, Schubert, & Vukolić, 2016; Lamport, Shostak, & Pease, 1982). Interestingly, the choice of the consensus algorithm influences the shared intentionality such that different algorithms result in different blockchains (see section 2.3) A more pronounced difference in intentionality leads us to the second data structure of this phenomenology, that is distributed ledger technologies.

The second method for organizing information in distributed consensus systems is the distributed ledger (DL) data structure. These systems share some of the same properties of blockchains albeit with significant differences. Generally, DL systems are private or permissioned as opposed to open, or permissionless blockchains (Androulaki et al., 2018). Hence, if one allows only selected parties to perform specific network functions or participate in the network, one may implement a different consensus algorithm thereby achieving a higher transactions output. This is due to a change in the adversarial assumptions. More precisely, 51% attacks and Sybil attacks are not a source of concern if access to the system is restricted to known nodes. Examples of these different consensus algorithms are Proof of Elapsed Time (PoE), Practical Byzantine Fault Tolerance (PBFT), Honeybadger, and Paxos. As the example of DL data structures this section selects the Corda platform, developed by the R3 consortium. Corda is a prominent DL system developed for industrial applications.

The phenomena of DL exhibit a high degree of variety, consequently, the following definition is wide enough to account for most implementations. A distributed ledger is a method of managing information that exhibits some properties of a blockchain-type data structure but may not have blocks and requires the identification of some of the nodes in the network. In other words, a distributed ledger is permissioned systems that does not linked system's data in blocks. The closed nature of many DL stands in unambiguous contrast with blockchains, so that within the crypto community private or permissioned systems are considered to be 'just' distributed databases. One need not weight on this objection, because to a relevant extent even open blockchains are distributed databases (Maiyya, Zakhary, Amiri, Agrawal, & El Abbadi, 2019). Permissioned systems still share some of the properties of blockchains albeit not all.

The main distinction between blockchains and distributed ledgers is the presence of an identity layer and the different type of data structure, which is not necessarily composed of chunks of data linked together by hashing functions (aka blocks in blockchains). Yet, some DL providers market themselves as blockchains to benefit from the hype surrounding open blockchains, which adds to the terminological confusion in this field. For example, the Corda website defines the platform as the open source blockchain for business even if the data structure implemented cannot be considered a blockchain (Brown et al., 2016). The next section describes the purpose of such systems, i.e. the logos of distributed ledgers.

One might argue that the purpose of these systems is to mitigate some of the problems that open blockchains have. It comes to no surprise, therefore, that DLs are marketed to business and institutions, that established companies run them or that no regulators banned this technology[9]. Distributed ledgers are a better solution than blockchains in term of transactions privacy, transactions finality, transactions throughput (TPS), compliance and so on. Therefore, one may conclude that their logos is to overcome the shortcomings of open blockchains. Yet, the technical advantages of DL are not exclusive, thus their logos ought to be found elsewhere for definitional purposes. In fact, the logos of DL is to address the

[9] In contrast with cryptocurrencies that have been banned in several jurisdictions (Xie, 2019)

regulatory and governance challenges of open systems. This is because, DLs aim to dispose of the ideals of open systems and establish sound governance structures (Velasco, 2017). The condition of possibility of these types of systems are the subject of the next paragraphs.

The conditions of possibility of distributed ledgers mostly overlap the ones of blockchains, but not in full. On the one hand, DLs implement an identity layer to manage the identities and privileges of the parties involved in the system. The management of identities is a condition of possibility of DL. Moreover, the identification of the parties is what allows distributed ledgers to achieve some technical advantages when compared to open solutions. That is, some known attack vectors as the so-called 51% attack, Sybil-attacks, that are sources of concerns for open blockchains do not affect DL systems because of the identification of the parties. A further condition of possibility of DLs within the ongoing framework, is the presence of a legal entity (usually, but not necessarily, a for-profit organization) in charge of maintaining and developing the network. DLs have the legal representation that most blockchain systems wish to forgo. Additionally, this legal entity provides the contractual agreement that regulates its operations along with the governance mechanism. Therefore, governance crisis and hard-forks are not a concern in DL-based systems. The previous remark is often the reason why distributed ledgers are considered centralized rather than decentralized, of course this position entails a specific idea on the meaning of decentralization which will be discussed later in this work (see chapter 7).

The third and final way to organize information in a distributed consensus system is the directed acyclic graph method also known as DAG (Benčić & Žarko, 2018). This type of data structure differs significantly from blockchains and distributed ledgers, IOTA implements a DAG data strucuture named the TANGLE. Other examples include Hedera Hashgraph, and Algorand (Baird, 2016). The phenomenon is based on the mathematical concept of DAGs. A DAG is a finite directed graph that has a topological ordering of the vertices such that every edge is directed in a sequence. Simply put, a DAG is a mathematical model of information. Therefore, IOTA's TANGLE is a stream of interlinked transactions wherein each transaction is a vertex in the graph while each edge is an approval (Popov, 2018). It is worth

noting that the TANGLE adopts a proof of work algorithm for spam prevention and resilience as well as consensus on vertexes. This means that consensus algorithms do not strictly depend on the type of data structure of the distributed consensus system. The TANGLE is akin to blockchains but differs significantly in its architecture. The TANGLE has no blocks, no miners, and no ledger.

The logos of the TANGLE is to improve on the technical limitations of blockchain systems but to maintain the openness of system. It provides a distributed system to transact at a higher TPS. As for the conditions of possibility of the TANGLE, all the system tokens ought to be included while bootstrapping the system, so no issuing scheme is provided in this instance. The issuance scheme of IOTA leads to a necessary increase in the trust required to bootstrap the system, simply put, one ought to trust the funders of the systems in the bootstrapping phase.

In conclusion, the foundational part of distributed consensus systems has been analyzed through the phenomenological method of investigation. The three data structures used to build decentralized consensus system (blockchains, distributed ledger and directed acyclic graphs) have been considered to establish a clear distinction and a common terminological ground. The analysis now moves upward the distributed consensus system stack to examine other components of these systems that are relevant for this dissertation.

2.2 Relevant Components of Distributed Consensus Systems

The second layer of the consensus stack is built on top of the data structures discussed above. The analysis will continue with a bottom-up approach to identify the main components of the consensus stack. These elements will be discussed to allow the reader to acquire a thorough understanding of the most important parts necessary to build a distributed consensus system. Furthermore, each component may be designed in ways that influence the system's behavior and characteristics, both at the technical and social level.

The methodological approach is maintained from the previous section, therefore for each component the discourse will address the following questions: what is it? What is it for? What are its conditions of possibility? The aim of this section, having regard to the highly interdisciplinary nature of the discourse is to establish a shared understanding of technical concepts and building blocks in terms that are understandable and sharable to both technically trained and non-technically trained readers. Such an understanding is of paramount importance to advance the discourse on the technologies at hand and to fully grasp its implications that span across several different domains. Considering the nature of the phenomena discipline hopping is in part a necessity in building the following phenomenological account (Galloway, 2004).

The complexity of the software stack is such that many components contribute to the functioning of the system, the next sections only consider the most fundamental ones. The selected fundamental components are the network structure, functions of nodes, scripting languages, and consensus algorithms. While much of the literature focuses on distributed consensus systems as a unitary concept, the purpose of this section is to show the startling differences between architectures of blockchains, thereby showing the need for a more granular approach; no system is created equal, architectures matter and distinct ideologies shape different solutions (Joerges, 1999). The next paragraphs describe the phenomenological assessment of these components.

The first component of the second layer of distributed consensus systems stack is the network structure. Most systems implement a peer-to-peer-network (P2P). The concept of a P2P network is well known in the literature, both from the legal perspective and a technical one (Agre, 2003; Pagallo, 2008; Pagallo & Durante, 2009). At the phenomenon level a P2P network is a distributed application architecture that partitions tasks or workload between peers. Peers are equally privileged and equipotent participants in the system, albeit different peers may perform different network function. At the core of any DDC lies a P2P network, this explains why some clashes were, after all, foretold (Pagallo et al., 2018).

The logos of a P2P network is arguably synthetized with dynamic-duo of decentralization and disintermediation, both technical and political. A P2P network enables distribution and decentralization of the system, it goes without saying that if one were to implement a distributed consensus system with a server in charge of managing the system's interactions little room would be left to the concept of decentralization and the concept of distribution. However, technical mechanisms go only as far as to dictate specific arrangements of power, centralized control might, in fact, exists after decentralization (Galloway, 2004).

The discourse on the condition of possibility of a P2P network bears some difficulties; its nature is twofold. On the one hand, part of the condition of possibility may be qualified as geographical, that is it requires a given geographical distribution and a critical mass of nodes to function effectively. On the other hand, the condition of possibility is sociological, in the sense that it depends on the presence of a given number of agents willing to commit their resources to participate in the network. This is because, if only a few entities run the nodes of a P2P network, then one is outside the realm of distributed consensus systems. Of course, from a technical perspective one can implement a P2P network that lacks the abovementioned condition of possibility, but from the current perspective, it seems that these are necessary conditions for the phenomena of distributed consensus systems. Interestingly, even permissioned systems such as Corda are P2P networks, the main difference from permissionless ones is the presence of a root authority whose task is to issue identity certificates[10] to the nodes. All in all, the network structure of almost all distributed consensus systems, regardeless of their data structures is P2P.

The impetus behind blockchains and distributed ledgers appears as another instance of libertarian attempts to implement a specific ideology on cyber P2P networks, however Pagallo noted in 2008 that P2P "are not the key to a new egalitarian paradigm" (Pagallo, 2008, p. 2). This is likely to be the case with this class of technologies, regardless of their flat and anti-hierarchical network structure these

[10] In Corda, these certificates are issued using TLS.

systems do not appear to pave the way toward an egalitarian paradigm. Yet, blockchains and distributed ledgers as a new generation of decentralized and encrypted P2P architectures are actually producing new challenges (*ibidem, p.* 9). So that, as in the case of *old* P2P network they are "transforming key concepts of current legal and political debate" (*ibidem*, p. 9), this is uncontroversial in the context of digital currencies and financing of start-up companies. To a relevant extent, the newfound attention to these P2P networks harbingers a clash with existing normative structures that is not surprising, case in point the issues in squaring data protection regulations with some blockchains (Pagallo et al., 2018). With that in mind, let us continue the phenomenological analysis of our subject.

The second component of a distributed consensus system built upon a P2P network is the messaging layer. The phenomenon of the messaging layer is a set of software instructions. The logos of the messaging protocol is the exchange of information between nodes, whereas its conditions of possibility coincides with the ones of the network structure. The exchange of information between nodes is key to several functions, some of the most important ones are discovery of other peers (addr command in the Bitcoin network), connection to other peers (version and verack command), verifying network status and alerts and disseminating transactions and information in general among the network. Rather than being a purely technical matter, an important distinction needs to be made with regard to the reach of messages: global versus local broadcasting. In permissionless systems the information is generally broadcasted across all the network, while in permissioned one information may be broadcasted only to selected parties. This architectural choice corresponds to different assumptions about authority and the degree of trust in the players participating in each system. In fact, trust works differently when information about trustees and trustors is not (always) available to everyone. Moreover, the global transmission of information is a necessary condition for one of the most important ideas at the core of blockchains, namely, transparency. On the contrary, permissioned systems enable parties to hide some information to increase privacy and confidentiality.

Second, many legal norms are triggered by the geographical location of the information, i.e. where the nodes are in the world. To put this distinction in perspective, information in Bitcoin is global, both in a technical and geographical sense, on the contrary, information in Corda (and other permissioned systems) can be both technically and geographically confined. The implications from a legal perspective range from determining the competent jurisdiction, to the applicable law. Many more legal conundrums arise when information is globally broadcasted, therefore the choice of the messaging protocol is not a purely technical question when dealing with this class of technologies.

The third element of the phenomenology concerns the functions of the nodes. Nodes split into full ones, verifying ones and information providing nodes. In the Bitcoin system full nodes store the entire copy of the blockchain but rely on other nodes to verify the correctness of the records, while in Corda are named just nodes. The verifying nodes are called miners in Bitcoin while notaries in Corda, lastly, information providing nodes are commonly referred to as oracles (Teutsch & Estsblishment, 2017). Oracles are necessary when there is a need to provide information external to the system, so called off-chain. Full nodes store the entire copy of the ledger, that is, the entire history of system states as determined by the consensus algorithm. The logos of full nodes is to maintain and bootstrap new nodes with the entire ledger; they also check every transaction to assess its validity against their record before broadcasting it, and, lastly, provide resiliency of the information. One can conceptualize main nodes as the gatekeepers of the system; therefore, the system is decentralized in so far as a critical number of main nodes operates. Critically, main nodes must store a full, updated copy of the entire ledger or blockchain to function, this is their condition of possibility.

The second type of nodes are the verifying ones. These nodes update the ledger according to a set of pre-defined rules that are included in the consensus algorithm. Verifying nodes are computers that write new information to the ledger, that is, they add new blocks to the blockchain or append new information to the distributed ledger. These nodes verify and record all the modification of states that are propagated throughout the system. The logos of these nodes is to run the consensus algorithm, they are the clogs in

the “trust machine”. In some systems, such as Bitcoin, one - de facto - condition of possibility of verifying nodes is the deployment of computer system with specialized hardware: application specific integrated circuits (ASIC). The same applies to consensus algorithms that require specific hardware to operate such as proof-of-elapsed-time or TPoS[11]. On the contrary, in other systems verifying nodes do not required specific hardware as a condition of possibility (i.e. Corda). One must also note that the role of verifying nodes and their phenomenology is deeply entrenched with the consensus protocol implemented in the system.

The final type of nodes is information providing nodes, named, oracles. These nodes feed information to the systems by signing or not signing a transaction that depends upon off-chain conditions (Teutsch & Estsblishment, 2017). Therefore, oracles are the only sources of information outside the system. The logos of oracles is to interface distributed consensus systems with the outside word. The need for oracles hinges on the need to gather off-chain data. The presence or lack of oracles enables a further distinction among the systems; namely between internal and external systems. The former do not need to feed information that is found off-chain, while the latter do. Oracles ought to be included in the transactions structure to function properly, moreover they are at risk of becoming single point of failure (SPoF) if not implemented correctly. Lastly, oracles ought to deal with the non-deterministic nature of the off-chain world (Cachin et al., 2016). These are the conditions of possibility of oracles.

The fourth components of the DDC stack is the scripting language, that is, the domain specific language used to enable the programming of each system. The differences in scripting languages is of paramount importance. Simply put, the scripting language is the programming language of the system, thus, it enables the system to perform calculations. Differences at the level of programming languages reflect on the functionalities of each system. On one hand, Bitcoin uses a simple intentionally Turing

[11] This algorithm requires specific hardware components that have a trusted execution environment, i.e. a dedicated area in a central processing unit. Trusted execution environment guarantee confidentiality and integrity of the code and data used for calculations, see https://en.wikipedia.org/wiki/Trusted_execution_environment

incomplete, FORTH-like language with no loops. On the other hand, Corda adopts languages that target the execution of JVM bytecode, that is, any language that compiles into an executable JavaScript bytecode, examples of such languages are Whiley and Kotlin. This stark distinction allows us to stress, again, how architectural choices yield widely different normative conclusions. A Turing incomplete system, like Bitcoin, is more predictable and it is narrower in scope as it can only perform a known set of functions. Contrarily, a system that uses a Turing complete language is capable of executing any algorithm (in principle). Therefore, Turing complete systems requires a different regulatory approach. This distinction ought to be kept in mind when dealing with our subject; one should not conflate these two by, for example, not acknowledging this distinction when regulating distributed consensus system.

There are other components in the software stack, such as, cryptographic functions, digital signature algorithms, hash tables, hash trees and so on. Albeit these components are interesting areas of technical research they exhibit a high degree of fungibility. Accordingly, not much changes from the current perspective if one, for example, implements SHA-3 or a SHA-256. For this reason, our analysis concerns mainly the components which, in turn, influence the functionalities and affordances of each systems. That said, two main components of the distributed consensus systems stack deserve their own sections due to their inherent complexity and relevance to this work, namely consensus algorithms and smart contracts. Considering these remarks, this chapter moves to the phenomenology of consensus algorithm (next section) before concluding with a phenomenology of smart contracts (section 2.4).

2.3 Consensus Algorithms

The concept of consensus is elusive in the context of our phenomenology. Unsurprisingly, there is no agreed upon definition to start from, rather it depends on the level of discourse. Most likely, the confusion is due to the interdisciplinary nature of the subject matter and because each discipline has its own idea of consensus. From the computer science perspective, consensus can be defined as the agreement upon the validity of system states and their ordering (Narayanan et al., 2016; Narayanan & Clark, 2017; Wattenhofer, 2016). Conversely, from the legal perspective consensus can be defined as the outcome of a jurisdictional process. Interestingly, both definitions are capable of being expressed as the outcome of a set of logical rules, the former by several consensus algorithms; the latter by the set of prescriptions that form the body of procedural law.

In this sense, one may argue that a judicial decision that has no recourse against it may be considered as the consensus expressed by one legal system. In other words, if a Judge has ruled that Alice has to pay Bob a given sum of money, then the legal system in which the ruling has been issued, one can suggest, has reached consensus on the fact that Alice owes Bob a given sum of money. This example aims to show how the very notion of consensus varies widely from discipline to discipline. Consequently, a phenomenology of consensus within distributed consensus systems adopts two distinct perspectives. The first one is technical, and it belongs to the field of distributed computing. The second one, conversely, adopts a more general view on the notion of consensus, such that, social sciences can converge on the notion of consensus as applied to the present topic.

Historically, the problem of consensus in distributed systems has been subject to copious research, it suffices to remember the pioneering work of Lamport and the subsequent development of several algorithms that enables computer networks to achieve consensus in an eventually synchronous model (Lamport et al., 1982). In practice, several consensus algorithms have been deployed and continue to function in the real word (Bano et al., 2017; Cachin & Vukolić, 2017; Crain, Gramoli, Larrea, & Raynal, 2017; Sigrid Seibold, 2016). A thorough analysis of such algorithms lies beyond the scope of this work,

for now, what one must remember is that the field of distributed computing has been grappling with the problem of consensus for at least 30 years, long before the first blockchain was proposed in 2008 (Narayanan & Clark, 2017).

Consensus in distributed computing is a fundamental problem in control of multi-agent systems, the phenomenon of such problem can be defined as follows. Let there be n nodes, of which at most f might crash, i.e. at least n-f nodes are correct. Node i starts with an input value. The nodes must decide for one of those values that satisfies the following properties:

Agreements: all correct nodes decide for the same value;

Termination: all correct nodes terminate in a finite time;

Validity: the decision value must be the input value of a node[12].

Less formally, the phenomenon of consensus in distributed computing is a set of instructions that constitute a protocol. The logos of the consensus algorithm is to disseminate instructions (i.e. write instructions in the case of blockchains and distributed ledgers) among the nodes such that each node executes the same sequence of operations on its instance of the service performed. Simply put, consensus in distributed systems aims to guarantee that the information written on the systems is the same under a set of adversary circumstances.

The condition of possibility of consensus is a set of rules that enable nodes to cooperate and reach consensus on some relevant aspect of the system, usually the order of the computational steps to perform to achieve a determined result. The consensus models are designed following a set of assumptions, that is, the designers of the system fix the condition in which the system is expected to function. This leads to distinct consensus protocols, each one with specific characteristic and peculiarities, for example some

[12] Adapted from the science of blockchain and fundamentals in distributed computing (Wattenhofer, 2016)

protocols are designed to accommodate (only) network partitioning events, whereas other (such as the byzantine family of protocols) are designed to withstand arbitrary behavior of up to 1/3 of nodes. In this context arbitrary behavior means that nodes may crash, leave and join the network randomly, or engage in malicious behavior. It follows that for the phenomenology of consensus at the level of abstraction of distributed computing, the notion of consensus resolves itself in the set of instructions (i.e. the phenomenon) that enable machines to achieve agreement, termination, and validity. In the case of Bitcoin, the algorithm that enables the network to reach consensus on the order of transactions and on the ownership of each bitcoin is commonly referred to as Proof-of-Work (POW) or Nakamoto Consensus (NC). On the contrary, many distributed ledgers, such as Corda and Hyperledger, do not depend on a specific consensus algorithm but let their users implement different algorithms on the basis of their specific needs.

In light of the previous account, NC is a consensus algorithm designed within an eventually synchronous network to withstand byzantine behavior of f = (< 51%) of the computational resources present at any given time in the network. Thus, it should be clear from this perspective that consensus is bounded by the set of assumption under which its condition of possibility unfolds. However, the innovative potential of blockchains and similar systems is not related to advancements at the consensus level from the perspective of distributed computing. Rather, it depends on the fact that these systems are believed to grant agreement on a specific state without the need for a central authority on a single version of the truth within a given system (Vigna & Casey, 2018). This is how Bitcoin creates electronic cash without the need for an intermediary or trusted third party. The next paragraphs examine the concept of consensus from the legal perspective.

A good starting point to tackle the notion of consensus at the current level of abstraction is the Merriam-Webster legal dictionary; it defines consensus as (a) a general agreement: unanimity or (b) the judgment arrived at by most of those concerned. As we can see, definition (a) is the general definition of consensus, however, definition (b) seems to be best suited for our phenomenology in so far as it

implies a process to achieve it. According to this second definition the phenomenon of consensus can be described as follows: among different interpretations of a set of facts, consensus is a shared view on those facts that differs from at least one interpretation. In this sense, consensus in the legal sense is the agreement on some real-world facts in a legally meaningful way. As for the logos of consensus, it is possible to identify the following reasons for why a legal system tries to achieve consensus among its constituents. First, there is the need for coordination (Pagallo, 2016). Second, there is the need for agreement on which factual conditions entail which legal conclusions, for example following Kelsen's account of legal norms "If A, then B" clearly there must be a way to reach consensus on what A actually is before dealing with B (Kelsen, 1967). Thus, at a minimum consensus serves two different functions: it addresses the need for coordination among autonomous agent in a legal system and, second, enables agents to assess whether certain requirements are met or not. Another important aspect of the phenomenon of consensus in the legal sense is its procedural nature, that is, the law implements rules of procedural regularity in order to achieve its goals (Pagallo, 2017a, 2019).

Of course, there are easy cases and hard ones (Dworkin, 1986). In the former, consensus operates in the shadow because there is a general understanding about the facts, therefore no sensible different interpretations arise. The latter are more fascinating. In order to solve hard cases, the legal machinery is activated through the technology of procedural law. In most legal system there is plethora of consensus algorithms, some are known under the notion of dispute resolution mechanism, some are called arbitrage, but the most popular ones are Courts and Tribunals. Courts are the engines of consensus in legal systems; agents that follows a specific set of instruction, and meet specific requirements, can activate the legal machinery to reach consensus on a specific set of facts, often referred to as causa petendi in civil law systems. Thus, legal systems across the world entrust the judicial process with the power to establish consensus in the legal sense, and this is the condition of possibility of consensus at the level of abstraction of the law. This account shows that consensus has two different, context depending meanings. However,

there are some interesting peculiarities among the different interpretation of consensus as well as important differences. The rest of this section deals with such elements.

Consensus at the technical level is deterministic; while at the legal level it is not. Let us elaborate. In order to get computers to agree on the outputs of calculations one must be sure that the same calculation always return the same output if the input values do not change (Cachin et al., 2016). Otherwise, two different machines can – and will – reach two correct, but different, results. It is self-evident that, in this instance consensus would be impossible to achieve. This is why systems that use scripting languages with functions with random inputs (such as Javascript) warn the developers not to use specific functions (e.g. math.random() or new.date()). For the same reason, Bitcoin does not implement functions with pseudo-random (or difficult to predict) inputs and Corda compiles code to a deterministic Java Virtual Machine (JVM). The law is different. The consensus reached by the legal machinery is bound to be non-deterministic, different courts will eventually disagree on the conclusions to be drawn on the basis of similar premises. To cope with this non-deterministic nature legal system usually implement a central judicial authority, whose decision are often binding for lower level courts. Even when the decisions of the highest court are not binding, such as in most civil law systems, they still have a relevant degree of *autoritas* on lower level procedures. Thus, the law necessitates some degree of centralization for its inherent non-deterministic nature. This leads us to an important disclaimer. Any claim about one particular blockchain or DLT application ability to solve the age-old problem of coordination or to automate the legal system must be taken with a grain of salt (Low & Mik, 2019). This is because a fundamental contradiction arises when one tries to automate a process that is – by definition – non-deterministic. On this basis, this dissertation adopts the technical notion of consensus unless otherwise stated. When the term consensus is used it will refer to technical notion of coordinating computational steps in a byzantine context. An example clarifies the previous point.

Many technologists have evangelically preached the record-keeping capabilities of blockchains (Sicilia & Visvizi; Victoria Louise, 2016). The main assumption is the following: since the Bitcoin

blockchain keeps track of who owns how many bitcoins then it is capable to do the same for other assets. Therefore, one can build a blockchain to transfer real estate property and benefit from the emergent properties of the blockchain and get rid of the perceived inefficiencies of legacy systems. It sounds simple, and desirable but there is a catch. The Bitcoin blockchain deals only with bitcoins, i.e. tokens generated by the system, and not with digital representation of other assets. Therefore, bitcoins are endogenous to the Bitcoin blockchain. On this basis, proposals to transfer anything that is exogenous to a system must be met with a vein of skepticism. It suffices to say that such a system requires the recording of an asset in terms that are understandable to it, that is, it requires the so-called tokenization of the asset (Li, Wu, Pei, & Yao, 2019; Weingärtner, 2019). Therefore, the process of recording requires a recorder, someone of something that records the relevant information in the system. Of course, the tokenization of any asset should be robust enough as to not generate disputes and to improve on current systems for the transfer of that class of assets, for example, a property registry based on some version of a blockchain or a distributed ledger needs a sound mechanism to ascertain that the cryptographic token x actually represent real estate y. However, it is not clear how this can be attained without having a centralized entity recording the assets.

This section has highlighted one primary misconception about the distributed consensus system landscape by showing how a single concept carries two distinct meanings and how their conflation might lead to unrealistic claims about the technology. That said, some of these systems arguably innovate the way in which information is shared and managed between mutually distrusting parties in the absence of a central authority. This chapter now moves to a last element of our phenomenological analysis, namely, smart contracts.

2.4 Smart Contracts

Many smart contracts are neither smart nor contract (Mik, 2017). The source of misunderstanding is likely found in the technical origins of the term smart contracts and it is exacerbated by the clash of many disciplines. Nick Szabo introduced the concept of smart contracts back in 1997 when he compared smart contracts to a vending machine (Szabo, 1997). After more than 20 years the concept has evolved into a buzzword that is often misused. The following section explore the concept of smart contracts using the same methodology adopted throughout this chapter, its objective is to bridge the terminological and technical gap between the law and the narrative within the crypto space. This section provides an overview of the technical definition(s) of smart contracts before attempting a phenomenological account of the concept; then it aims at providing a legal account of the phenomenon before its concluding remarks.

As expected, there is no standard definition of smart contracts from a technical perspective, different designers define them in different ways. Others, on the contrary, take the notion for granted, for instance, Ethereum's yellow paper does not define smart contracts, rather it considers their characteristics. First, it references an entry on the Bitcoin wiki that refers to "contracts" by saying that smart contracts contain a set or arbitrary rules that control a digital asset implemented in code. A look at the Bitcoin Wikipedia comforts us by stating that contracts on a blockchain "don't make anything possible that was previously impossible"[13]. Second, Ethereum regards smart contracts as "cryptographic 'boxes' that contain value and only unlock it if certain conditions are met" (Wood, 2014). Wikipedia defines smart contracts as "computer protocols intended [..] to facilitate, verify, or enforce the negotiation or performance of contracts"[14]. In Bitcoin contracts are not smart and are regarded as: "a method to form agreement with people via the block chain". There are other definitions of smart contracts provided by industry, academia and other institutions that I will not consider in this section.

[13] https://en.bitcoin.it/wiki/Contract

[14] https://en.wikipedia.org/wiki/Smart_contract

In elaborating a phenomenology of smart contracts from the technical perspective, the analysis will try to establish a minimum common denominator that should encompass what smart contracts are without being concerned about what they can (maybe) do. The following approach may seem minimalistic to some, but rigor requires to take such an approach in defining this term, after all even Ethereum's co-founder Mr. Vitalik Buterin acknowledged that the term smart contracts could be confusing, but it was kept for reasons of continuity[15]. In the difficult task of describe a phenomenology of an elusive and confused concept such as the one of smart contracts, Heidegger's methodology guides us toward clarity. The phenomenon of a smart contract in distributed consensus systems is a set of instructions that are executed on a decentralized, distributed network of computers. This definition of the phenomena is consistent with others in the technical literature (Bartoletti & Pompianu, 2017; Bhargavan et al., 2016; Gonzalez Rivas, Tsyganova, & Mik, 2018; Grigg, 2015). The logos of smart contracts is to enable the trusted and verifiable execution of instructions without relying on a central authority. As such, smart contracts are tamper-proof, censorship-resistant software programs whose execution does not depend on a single node in a network of computers. It is also important to add that smart contracts share the emergent properties of the system in which they run. For example, smart contracts in Ethereum are publicly visible, and stored in a decentralized fashion across many nodes.

The conditions of possibility of smart contracts are the following. The existence of a decentralized network of computers that can reach consensus on the state of the system, like a blockchain or distributed ledger architecture[16]. The presence of a scripting language that supports smart contracts. Lastly, smart contracts need to be deterministic for the same reason put forward earlier in this chapter; this may limit their abilities to interact with the real world unless some other mechanism is implemented[17]. This account

[15] https://insidebitcoins.com/news/vitalik-buterin-i-quite-regret-adopting-the-term-smart-contracts-for-ethereum/182844

[16] It is not clear at the time of writing if the third type of data structure (the TANGLE) can implement smart contracts as defined in this work.

[17] One possibility would be to pre-compute the operations of a smart contracts and broadcasting them to the network before the verification phase as a way to minimize the use of a non-deterministic programming language.

of smart contracts may seem to be overly simplistic and limited to the reader who has been exposed to the mainstream discourse on the technology (Cutts, 2019; Frantz & Nowostawski, 2016; Shermin, 2017), but it is consistent with the actual phenomena of smart contracts, that is, how smart contracts are experienced within systems such as blockchains and distributed ledgers. A further reason to adopt this conservative definition is that, at the time of writing, there are many smart contracts platforms, thus raising the complexity in establishing a richer definition capable of encompassing all different solutions. The present approach simplifies the discourse and fosters a bottom-up approach to understand the technology at hand and helps us to build up the terminological framework adopted in this dissertation. Concluding, smart contracts are software programs that execute on a distributed consensus system; however, the unfortunate terminology demands consideration of the phenomenon from the legal perspective.

The use of the term contract spurred the interest of many legal scholars; some have developed analysis from a contract law perspective (Alberini & Pfammatter, 2019; Brownsword, 2019; Cuccuru, 2017) some expanded the theme of execution (Unsworth, 2019). Others analyzed terminological issues and the legal impurities of transacting with some real-world goods on a blockchain (Mik, 2017). Much effort has been channeled (again) toward formalizing contractual law for smart contracts deployment, this tendency is well represented both at the industry and the academic level (Governatori et al., 2018; Grigg, 2015; Idelberger, Governatori, Riveret, & Sartor, 2016; Tai, 2017). Arguably, the legal viewpoint is more informative in respect to the technical one, likely because when laypeople read the term smart contracts, they tend to expect some more legal rather than something which belongs to the set of software protocols within the field of distributed computing.

The usual starting point for the phenomenological analysis is the phenomenon, from a legal perspective smart contracts are not (always) contracts. First, any meaningful discourse on the contractual nature of smart contracts presupposes a legal frame of reference; the following discourse develops under the Italian legal framework. Therefore, the following remarks may not hold in other legal systems. The

art. 1321 of the Italian civil code defines a contract as “the agreement between two or more parties, to constitute, regulate or extinguish among them a patrimonial juridical relation.” Art. 1325 dictates the requirements that any contract must meet; if a contract does not meet these requirements the sanction is nullity. The requirements are (a) the agreement of the parties (analogous to the meeting of minds doctrine form common law jurisdictions), (b) the cause (the economic and social function that the parties want to achieve with the contract), (c) the object and (d) the form if the law requires it. Let us assume that smart contracts do indeed constitute, regulate or extinguish a patrimonial relation. Next, we need to assess if smart contracts meet the requirements of art. 1325. It is uncontroversial that the agreements can be reached with the use of digital signatures or with ICT technologies and that, therefore, an agreement could be represented by signing the transactions that triggers a smart contract. However, it is by no means required that a smart contract involves different parties. For example, I could code a smart contract that transfers assets between two account that I have control over, thus that particular smart contract would not qualify as a contract under Italian law, for a contract with oneself is not a contract at all. Additionally, smart contracts might be deployed with the expectation that parties will later adhere to it, so that they would not be regarded as contracts but as offers to the public. Requirement (b) is also uncontroversial, because it can be argued that most smart contracts have a legitimate cause. Concordantly, smart contracts usually have an object thus requirement (c) is also met. The last requisite (d) may nullify smart contracts which constitute, regulate, or extinguish judicial relations for which a particular form is required under Italian law, while accordingly to the free-form principle every other relation could be legally represented in smart contract code without incurring in the sanction of nullity.

This short legal analysis of smart contracts under Italian law leaves many problems open for discussion but more importantly it shows how, with regard to smart contracts nothing is new under the Italian sun. What we can say is that smart contracts that constitute, regulate, or extinguish judicial relation for which a specific form is required under Italian law (so-called forma ab substantiam) have no legal effects (nullity). From the perspective of the qualification smart contracts do not pose legal

problems that have not been already discussed at length with respect to contracts concluded with electronic means (Scholz, 2016). Hence, not every smart contract in the technical sense is also a contract in the legal sense, much in the same way as not every software system implements a contractual relation.

From the legal perspective, the logos of smart legal contracts does not strongly differ from the logos of legal contracts in general. The main difference being the platform where the performance of the contract is executed, along with the lack of flexibility of smart contracts compared with other contracts (Sklaroff, 2017). Thus, in the narrow case in which a smart contract qualifies as a legal contract the logos of former coincides with the logos of the latter. That is, the reason for contracts is to create, to regulate, to modify or extinguish patrimonial relation between parties.

Lastly, the analysis moves to the condition of possibility of smart contracts in the legal sense. One can argue that this condition resolves itself in the mapping of each specific smart contract to the norms of contract law in each independent jurisdiction both at the national and international level. The technology of contract in the legal sense is platform agnostic and blockchains, and distributed ledgers are no exception. A contract can be formed orally, on paper, or on by signing a transaction in the Ethereum blockchains. Accordingly, the condition of possibility of smart contracts (a) depends on the jurisdiction through which the phenomenon is analyzed, and (b) implies a legal analysis of each smart contract implementations according to the frame of reference adopted.

Many interesting legal questions arise from the implementation of smart contracts that are, unfortunately, outside the scope of this dissertation because they do not concern the reason why agents engage with distributed consensus systems. For now, the reader must keep in mind that in the rest of this work the term smart contracts will be used in the technical sense unless otherwise stated. In fact, much of the excitement around smart contracts in the legal community seems to overlook some major technical difficulties (Low & Mik, 2019); considering the aspiration of this work the discourse will not deal with problems that may or may not arise from technical achievements but deals with the opportunity to use smart contracts as a set of instruction to program distributed networks.

2.5 Conclusion

This chapter explored the technologies of blockchain, distributed ledgers and directed acyclic graphs by considering their core components through the lenses of the phenomenological method proposed by Heidegger. Different perspectives have been adopted to grasp the terminological and conceptual gaps that often inform the academic discourse around these technologies. This chapter aimed to establish a terminological and conceptual base for the rest of this dissertation. The takeaway from this chapter is that nothing such as The Blockchain exists; what does exist is a class of technologies to manage data in a distributed environment. In the end what blockchains, DAGs or distributed ledgers can achieve is a matter of evaluation on a case-by-case scenario with regard to the specifics of the problem(s) one intends to address. The same applies to the subject of the next chapter, namely, trust. It has become common practice to associate blockchains and distributed ledgers with trust (Baldwin, 2018; Hawlitschek, Notheisen, & Teubner, 2018; Thurimella & Aahlad, 2018; Werbach, 2017, 2018). More precisely, many refer to blockchains architectures as trustless architectures, trusted computing systems, trust as a service or zero trust architectures. As such, the task of the next chapter is to expose the reader to the most prominent theories about trust in the cyberspace and to ascertain how they square with the consensus architectures described in this chapter. Again, one finds lack of consensus about fundamental concepts in the digital consensus space. On this basis, the following chapter explores the first reason that is often put forward to implement blockchains and similar technologies.

3. It’s not about trust: blockchains, control, and reliance

"We have proposed a system for electronic transactions without relying on trust" (Nakamoto, 2008, p. 8). The disappearance of trust marks the end of the Bitcoin white paper. Bitcoin, therefore, hinges on (dis)trust. Seven years later - in 2015 - the Economist referred to the underlying technology – blockchains - as the trust machine. It reads: "spread of blockchains is bad for anyone in the "trust business"—the centralized institutions and bureaucracies, such as banks, clearing houses and government authorities that are deemed sufficiently trustworthy to handle transactions." [18]. The assumption is that technologies like blockchains have an important impact on the "trust business", this chapter examines how this class of technologies relate to trust and what, if anything, changes when blockchains and similar solutions come into play (Werbach, 2018). Preliminarily, it is important to highlight the relevance of the subject matter.

If the Economist is right, the consequences are unimaginable. Arguably, trust is key to every human activity, so much so that without trust one would hardly justify getting out of bed (Luhmann, 1979). Moreover, major institutions are in the trust business along with - to a relevant extent – legal systems and legal technologies such as contracts and corporations. The issues of trust and its relation to distribute consensus systems is of paramount importance for the purpose of this dissertation as it is, arguably, the primary argument put forward to explain agents' engagement with blockchains and distributed ledgers. Consequently, this chapter deals with trust in/with distributed consensus systems. More precisely, it aims to understand and conceptualize how does the shift for zero-trust to the creation of trust occurs? Moreover, how did a technical solution designed for a zero-trust system such as Bitcoin transform into the trust machine? These are the questions that this chapter aims to address.

In order to answer these questions, this chapter develops as follows. The first section analyzes some relevant theories of trust and how they relate to the technological innovation of blockchains and

[18] https://www.economist.com/leaders/2015/10/31/the-trust-machine accessed on 10th September 2018.

distributed ledgers as described in the previous chapter. Then, section two deals with the subject of trust between human agents (HA→HA) mediated by distributed consensus technologies. Later, section three explores the impact of DC systems on the level of systemic trust; that is, the trust relation between HA and The Technology (HA→T) before turning its attention to the problematic relation between trust, control and reliance. It will be argued that blockchains, along with DL and DAGs increase control and, at best, replace trust with reliance.

3.1 Old and New Theories of Trust

Trust is relevant in many aspects of human interactions (HA → HA); therefore, it comes to no surprise that several fields dealt with it. This adds another layer to the interdisciplinarity of the subject of this dissertation. Consequently, this section evaluates several theories of trust from different scientific domains. Much of the literature on the topic of trust in the context of blockchains, seems to regard trust as a "I know it when I see it" type of concepts, so that its ontological nature is often cast aside (Werbach, 2017). For example, Hawlitschek et al., discuss trust and blockchains in the context of the sharing economy (Hawlitschek et al., 2018). They regard trust as "the intention to accept vulnerability based upon positive expectations" (*ibidem,* p. 52). They conclude that an essential issue is the ambiguous use of the terminology around trust. I agree with this perspective; accordingly, this section examines different accounts of the notion of trust. This is a necessary step to critically examine if blockchains and distributed ledgers should be adopted because of their effect on trust. Additionally, this section moves from old theories of trust to newer ones. And it examines both trust and e-trust as defined by Taddeo (Taddeo, 2009). Its purpose is to outline different views of trust and, therefore, take a position on the issue of trust before studying the interplay of trust and distributed consensus systems.

Niklas Luhmann laid the foundations for the modern understanding of trust; his work has been widely influential in the trust literature across many disciplines. As a functionalist, Luhmann considers trust as

an effective form of complexity reduction; he argues that "trust is required for the reduction of a future characterized by more or less indeterminate complexity." (Luhmann, 1979, p. 15) Trust, is the result of a decision process characterized by risk, or – to use Luhmann's word - a gamble. Further, trust requires expectations to make a difference in the decision process. Otherwise, one deals with hope, which is trust minus expectations. Luhmann introduced the risky nature of trust, represented by the possibility of betrayal which is a common denominator across the different accounts of trust taken into consideration in this section. Trust is, indeed, a risky business. Hence, without risk, there is no trust. This is a first important consideration, risk is a necessary, yet not sufficient condition for trust to arise in a given relationship. However, it is not clear how one would design a risky technology in the first place, so that it seems already possible to begin to question the possibility of trust in technology, an issue often taken for granted in popular narratives surrounding blockchains. Luhmann's view of trust as a decisional process has been elaborated by Gambetta in the context of economics and game theory.

Gambetta defines trust as "a particular level of the subjective probability with which an agent assesses that another agent or group of agents will perform a particular action" (Gambetta, 1988, p. 216). According to this view, if the probability exceeds a certain threshold trust is warranted, else agents refuse to trust. The calculation of the probability by the trustor is, therefore, of primary importance. Such calculation is grounded on the trustor's own beliefs about the trustee's behaviors and capabilities. Gambetta's view reduces trust to subjective probability held by the trustor on the trustee; this account represents trust as a risk assessment based on expected probabilities of future events. Notably, Gambetta modeled the goal of the trustor – and its expected utility – to assess the opportunity to trust. This leads us to another necessary condition for trust, namely its teleological element. The goal of the trustor is of primary importance in trust relations. A trustor may trust the trustee to achieve a given goal, as such, at a minimum trust is a tripartite relationship between the trustor, the trustee and the goal of the former. Against Gambetta's view, some authors argued that trust is not just a matter of subjective probabilities, but a cognitive process.

Castelfranchi and Falcone put forward the cognitive view of trust as a complex structure of beliefs and goals (Castelfranchi & Falcone, 2000, 2010). As a corollary to the view of trust as a cognitive process, the trustor must have a "theory of mind" of the trustee. Therefore, trust consists of three elements 1) a mental attitude 2) a decision to rely on the trustee and 3) a behavior, namely, the effective act of entrusting another agent (Castelfranchi & Falcone, 2000). These authors focus their analysis on formalizing the cognitive view of trust for multi-agent systems (Durante, 2010; Falcone & Castelfranchi, 2001).

Another account defines trust as a complex procedural process that allows the trustor to deliberate on whether to trust the trustee for a given goal. Within the notion of trust as a procedural process, Grodzinsky et al. described several steps to attain trust (Grodzinsky, Miller, & Wolf, 2011). First, trust is a relation between the trustor and the trustee. Second, they consider trust as a decision by the trustor to delegate to the trustee some aspect of importance to achieve a goal. Third, trust requires risk such that risk is proportional to trust, the higher the risk the more trust is required. Fourth, the trustor has the expectation of gain by trusting. Fifth, the trustee may or may not be aware of being trusted by the trustor. Lastly, they contend that trust is reflective, that is, effective trust relations begets more trust among the same agents (*ibidem*). Here, it is possible to find another important element of trust, that is, the continuity required to establish deep bonds of trust, this is often a result of multiple interactions across a significant timespan. With respect to technological artifacts this may mean that a given system could gain trust from its users by operating continuously in a manner that enables the trustors to achieve their goal, yet it is not clear that another concept appears better suited to explain the relationship between users and technological systems.

Pitt develops a different conception of interpersonal trust, that is, HA → HA trust relations (Pitt, 2010). According to his view trust is grounded on the cognitive mechanism of promising. Therefore, trust is limited to cognitive agents, and it is strictly interpersonal because it builds on promising. More precisely, in Pitt's own words trust is a relation where "[y]our promising and my taking your words

allows me the freedom to do something else, not worrying if the thing you promised to do will get done, for if it does not get done, then I would have had to do that instead of the other thing I was going to do" (*ibidem, p. 448*). Trust is built and amounts to promising between cognitive agents. Interestingly, promises are often described as the sociological foundations of contract so that legal systems are, also, deployed to make sure that promises that qualify as contracts are fulfilled (Werbach & Cornell, 2017).

The previous accounts exposed the notion of trust in social sciences as a decision process, a cognitive state, a mechanism for the reduction of complexity, and so on. While distributed consensus systems are often designed with the goal of enabling cooperation among HA, designers often conflate the social science notion of trust with a different one, namely a technical conception of trust, i.e. trusted computing. In this sense, trust is a collision of paradigm as shown by Camp et al., that is, purely technical systems to implement trust must assume a particular account of trust in the social sciences (Camp, Nissenbaum, & McGrath, 2002). Therefore, this chapter disambiguates the term trusted computing to avoid likely confusion with the overarching argument about the possibility of trusting the specific class technologies under consideration.

The term trusted computing has little to do with trust as a social concept. On the contrary, trusted computing refers to protocols and hardware developed by the Trusted Computing Group to ensure that computers are more secure for users and behave in an expected fashion. As it is evident, the initiatives of the trusted computing group need not concern this work for, as Richard Stallman eloquently put it "[w]ith a plan they call trusted computing, large media corporations, together with computer companies such as Microsoft and Intel, are planning to make your computer obey them instead of you."[19]

Notwithstanding the misuse of the term trusted computing, the technical literature abundantly uses terms such as, trusted systems, and trusted execution in a peculiar sense which does not coincide with the theories of trust examined in the previous paragraphs nor with the meaning of trusted computing

[19] https://www.cs.bham.ac.uk/~mdr/teaching/modules/security/lectures/TrustedComputingConcepts.html/ accessed on the 5th of May 2019

referenced above. In the areas of blockchains and distributed ledgers the concept of trust takes a specific declination that the next paragraphs aim to expose.

It is possible to sketch the contours of the understanding of trust within blockchains' communities and proponents starting from the Bitcoin whitepaper. First, the current state of affairs is considered undesirable for too much trust needs to be granted for money to function (Golumbia, 2016). This is because, there have been many instances in which trusted entities misbehaved. It is important to note that the Bitcoin system was release in the immediacy of the 2008 financial crisis, a point in history where trust in banks and regulatory institutions hit a low point. Second, crypto narratives appear to consider trust as a relation between the trustor and the trustee in which the trustee has some autonomy, so that, she can behave in a way that is not aligned with to the goal of the trustor. Therefore, the autonomy of the trustee is considered undesirable and costly. This is where software architectures like blockchains come into play. In relation to trust the core idea is to create a trusted system in the sense that the autonomy of the trustee is reduced to a set of known alternatives, thereby eliminating the possibility that the trustee could act against the goal of the trustor. However, this entails eliminating the risk element necessary for trust to exist, this explains why Nakamoto said that Bitcoin is a system without trust rather than a trusted system. More precisely, some instances of blockchains and distributed ledgers manipulate trust by eliminating the risk with software protocols. Then, we need to ask what notion of trust – if any – applies to these systems.

In other words, what type of interactions are we concerned with when dealing with blockchains and distributed ledgers? In the absence of face to face (f2f) interactions what notion of trust could be applied to computer systems? Taddeo studies the phenomenon of trust relations mediated by information communication technologies (ICT), namely, e-trust (Taddeo, 2010a, 2010b; Taddeo & Floridi, 2011). Two options arise. Either trust is not possible in the digital space for it needs something that is lacking in cyberspace (Nissenbaum, 2001, 2004). Or trust is possible in digital environments for it is not bounded by physical interactions, hence, e-trust refers to the trust that arises in the context of interactions mediated

by ICT. Taddeo identifies three main obstacles for e-trust (Taddeo, 2009). These obstacles presuppose that some conditions for the emergence of trust cannot be fulfilled in digital environments. More precisely, detractors of e-trust hold the following conditions to be strictly necessary for trust to occur:

a) direct physical interaction between agents;

b) the presence of shared norms and ethical values that regulate the interactions in the environment;

c) the identification of the parties involved.

These arguments have been examined by Taddeo, who concludes that those conditions are also possible in digital environments. However, it does not follow that the conditions for e-trust are present in the context of blockchains and distributed ledgers, so that, even if one assumes that e-trust is possible then it is an open question if it arises among interactions mediated by the class of technologies at hand.

Moreover, e-trust splits into two categories, interpersonal trust, and systemic trust. One can distinguish these modalities of e-trust on the basis of the parties involved in the trust relation. Hence, in the case of interpersonal trust, one finds interactions between autonomous agents (HA and AAA), while in the case of systemic trust one deals with interactions between agents and technology (AAA → T or HA →T).

Note that the first modality of trust does not strictly require human agents (HA), in fact, it also extends to interactions that involve artificial autonomous agents (AAA) albeit with some nuances in the latter case (Durante, 2015; Grodzinsky et al., 2011). While interactions between HA and AAA within DCS raises some interesting theoretical questions, it need not concern this chapter as the argument for the adoption of blockchains and distributed ledgers based on trust only considers the aspect of human to human (or institutions) interactions. Therefore, the account of trust in the context of blockchains and distributed ledgers moves on by analyzing, in the ensuing section, the subject of interpersonal trust before dealing, in section 3.3, with systemic trust.

3.2. Interpersonal Trust in Distributed Consensus Systems

Interpersonal trust in blockchain-type systems refers to the act of trusting someone through a DCS, as such it is a specific kind of e-trust. When considering e-trust more broadly, the architecture of the system and characteristics of the interactions are determinant. E-trust depends on the architecture on which the interactions take place, thus two models of e-trust are possible. One is centralized trust, i.e. (HA → TTP→ HA) in T, while the other is P2P trust (HA → HA in T) (Mallard, Méadel, & Musiani, 2014; Werbach, 2018). This distinction in part grounds the belief that blockchains or distributed ledgers should be deployed when trust is lacking, as, for example, in the context of land registries in developing countries (Victoria Louise, 2016). This is because, some assumed that decentralized and distributed systems dispose the need for trusted intermediaries, therefore a switch to the first architecture of trust to the second occurs. It is also believed that P2P trust is a superior method because it aims to relinquish intermediaries which might act against the goal of the trustors (Botsman, 2012).

Werbach describes the two archetypal architectures of e-trust in the context of blockchains (Werbach, 2017, 2018). The author traces back the centralized model of trust to the popular concept of Hobbes's Leviathan. In this instance, trust is delegated to powerful intermediaries that manage the relations between agents. On the contrary, P2P e-trust is characterized by atomic relations. This account of e-trust architectures appears too simplistic to be satisfactorily. In fact, most of the successful trusted intermediaries of e-trust, who brand themselves under the equivocal term of sharing-economy platforms, are a combination of both architectures (Hawlitschek et al., 2018). It is likely that one trusts the other users of the platform, namely the Uber drivers and the Airbnb hosts, more than one trusts the platform itself. This occurrence is consistent with most of the trust theories explored in the previous section, so that, trust architectures are simply not binary. More likely, a successful trust architecture adopts a mix of centralized trust and of peer-to-peer trust. One might then argue that following the popular narrative on blockchains (and other similar systems), e-trust relations belong to the peer-to-peer category because

no entity is formally in charge of most systems there should be no need to defer trust to a trusted third party. This line of reasoning is flawed.

Promoters of blockchains and other open systems argue that, with blockchains, there is no need for trust anymore. That is, blockchains enable trustless trust, an oxymoron according to which transactions that used to require trust to occur no longer need it, therefore – given the high cost of trust – more trustless transactions will occur thereby enabling an incredible array of benefits for the society and the economy (D. W. E. Allen, Berg, Lane, & Potts, 2018; Davidson, De Filippi, & Potts, 2016). Henceforth, the trust machine is a machine that does not create trust; rather it eliminates it.

This is because, according to the perspective adopted in this chapter, a technological system cannot be trusted but can only be relied upon (see section 3.3). In Luhmann's sense, blockchains and distributed ledger reduce complexity thus competing with trust in the reduction of all possible futures. However, the reduction is likely a result of the increased control enabled by such systems.

Should one then conclude that e-trust does not occur in these types of systems? As with other areas related to the technology at hand, the answer depends on the architecture of each system. For example, the trustless claim is only attributed to open or permissionless systems while in permissioned ones, the presence of a root authority that issues identity certificates is a trust leap in its own right (Botsman, 2012). Therefore, permissioned systems do not appear to raise significant challenges from the perspective of e-trust, as the literature on the topic of trust and technology seems sufficient to account for the presence, or absence of e-trust within these systems. The same does not hold with respect to permissionless systems, so that, the rest of this section focuses on HA→HA e-trust in the context of open systems such as, Bitcoin, Ethereum, Litecoin, Monero, and Z-Cash.

The process that drives the trustor to trust the trustee rests on an assessment of the trustworthiness of the latter. Among the elements that determine trustworthiness one finds familiarity, trustor's influence on the trustee, sanctions, and enduring structures (Luhmann, 1979). The nature of this assessment is controversial. Some argue that trustworthiness is a set of beliefs that the trustor holds on several aspects

of the trustee. In this sense, trust is a blend of knowledge – about the trustee – and ignorance. Since e-trust entails risk, the assessment of one's trustworthiness determines the amount of risk that the trustor is willing to take to achieve a given goal. If one should model such a relation, the outcome of the assessment of trustworthiness ought to be compared to a threshold determined by the amount of risk the trustor is willing to take to achieve a given goal. If, then, the trustworthiness crosses the risk threshold then the trustor chooses to trust. The claim of crypto systems is that e-trust is not needed for rational agents to execute transaction within the system, or, which is equivalent that one needs only to trust the protocols of each system. The following example examines the transfer of digital value to make clear how the process of elimination of trust unfolds courtesy of open distributed consensus systems.

Let us start by describing the process of transacting digital value via ICTs according to two extremes of trust architectures, that is, centralized trust and peer-to-peer trust. In this example, the action that the trustee is entrusted to perform is the transfer of value on behalf of the trustor. In the centralized model, the trustor evaluates the trustworthiness of an intermediary (I) based on both beliefs and objective facts. Thus, the relevant trust relation is HA→I. For example, if Alice is evaluating the trustworthiness of PayPal in order to transfer value to Bob, she would probably consider several elements. More precisely, she might evaluate the familiarity she has with the service provided by PayPal, her influence on it (also regarding regulatory guarantees), her possibility of sanctioning PayPal in the case of bad behavior and so on. In the end, she would probably decide that the trustworthiness of PayPal is enough to trust it to achieve her goal. This process comes at a cost: the percentage of the value of the transaction that PayPal retains either from her or from Bob. Notably, a third-party is required to carry out the exchange on the internet within the centralized model of e-trust. In this case, Alice need not trust Bob to execute the transaction but only the intermediary I.

Let us examine the transfer when taking into consideration blockchains and distributed ledgers architectures. The transfer of digital value can occur in two distinct ways. In the first case, let us assume

that Alice already owns some unit of her cryptocurrency of choice[20]. Provided she already possesses Bob's public address (and that Bob is willing to accept the cryptocurrency of her choice) she instructs her software wallet to broadcast a transaction to Bob. She then waits for the consensus process to unfold and then, presumably, for Bob's confirmation. *Prima facie* this process does not require an intermediary nor trust in Bob. In this case, the elimination of trust comes at a significant cost. If we consider the best-case scenario, Alice needs to invest time in learning about the system of her choice since she is technically savvy and therefore can reliably examine the repository of the system of her choice on GitHub. Then, she needs to install and maintain a full copy of the data structure on her machine where she also must install the software wallet. If she picks Bitcoin, that is some 210.000 megabytes of blockchain to store, along with the necessity to keep her computer powered and connected to the internet for 24/7/365. Ultimately, she also needs to safeguard her private key because if she loses it, she also loses control of her coins. The same holds for Bob, so that the cost buried by Alice must be multiplied by a factor of two. Yet, in this instance, it appears that the trust machine has performed as advertised, it eliminated the need to trust and intermediary to achieve the goal of transferring value over the internet. But this is not the whole story. If we relinquish some of the previous assumptions, the situation changes.

In this second case, the first assumption does not hold, therefore Alice is not technically savvy and does not already own crypto coins. It is important to stress that while the actual distribution of most crypto coins is a known unknown, one should be confident in the claim that most users of cryptocurrencies belong to this second scenario[21]. Therefore, Alice sign-up with an exchange (E) in order to obtain some coins, as she agrees to the terms and conditions on the exchange's website the claim of a

[20] Either she obtained them from a previous transaction or by participating in the consensus algorithm therefore obtain some coins as a reward for her efforts.

[21] The real distribution of coins in an open system is difficult to assess. In fact, the relation with public addresses and individual is sketchy at best because anyone can create and arbitrary number of address to store some coins. Yet, if we take the case of Bitcoin, a savvy user would probably run a full node instead of an SVP one for many reasons. If this assumption holds there are around 10.000 full nodes in the Bitcoin network while a popular bitcoin exchange (Coinbase) has served more than 20 million customers. Hence, it is safe to conclude that the vast majority of people who transact with bitcoins belong in this second scenario.

trustless exchange begins to fade. In this scenario, Alice trusts the exchange to perform her transaction to Bob much in the same way as she would have trusted another intermediary had she gone the old way. Consequently, if one considers the trustworthiness of crypto coins exchanges, in this scenario Alice makes a more significant trust leap. In this latter case, the trust relation is HA→E, which is equivalent to HA→I. Arguably, no advantage arises if the trust machine shifts the trustee from I to E. This leads to a paradox. In order to avoid trusting established intermediaries, most users are asked to trust a new, emerging, class of entities for a perceived gain in trustless transactions. In these instances, the trust machine requires more trust than it eliminates.

The higher need for trust is apparent if one evaluates the trustworthiness of exchanges (E). The first element is familiarity; unsurprisingly, exchanges are not familiar to new users as they have only existed for a limited amount of time. Then one finds trustor's influence on the trustee, which in this case, is rather limited in scope with regard to legal mechanisms, case in point the Mt. Gox incident and – more recently – the QuadrigaCX debacle. The same applies to enduring structures, the possibility of sanctions, seals of approval, brands and other variables that a trustors usually evaluates in the assessment of trustworthiness (Camp, 2003). This section shows that, indeed, the trust machine works for HA→HA e-trust, but with a critical caveat. Trustless interactions occur if and only if agents can directly access open distributed consensus systems and if they have the necessary competencies to do so. In most cases, the trust machine requires more trust than it eliminates in the case of transfer of units of value across the internet. However, this is not the only caveat.

The previous example dealt with the case of e-trust relations that involve the transfer of endogenous assets on open distributed consensus system, i.e. the case in which two agents exchange bitcoins by running two full nodes. However, much of the discourse around these systems involves claims about their ability to also enable the transfer of other types of assets. Many examples are to be found in the literature, ranging from land transfer systems to intellectual property licensing, identity management, diamonds, and so on. The common denominator of these proposals is that they claim to enable the

trustless transfer of assets other than endogenous assets, that is, cryptographic tokens. This section ends by showing how these claims fall short in enabling trustless interactions at a conceptual level.

Preliminary, a few words are necessary on the distinction introduced above between native or endogenous assets and non-native or exogenous ones. The former are assets created and stored only in the system that transfers them, i.e. this types of assets have no correspondent in the real world. All crypto coins are examples of endogenous assets, they are inextricably linked to the data structure that transfers them, one cannot take any bitcoin away from its blockchain. The latter, instead, are assets that have a correspondent in the real world such that their transfer using DC technologies requires their representation at the software level, hence their exogenous nature. The process of representing exogenous assets on a DC system is referred to tokenization (Li et al., 2019; Weingärtner, 2019). Tokenization is a mechanism for linking the real-world object to a digital representation on the system, i.e. the token. From the perspective of trust the problem is manifest.

In order to enable the trustless transfer of exogenous assets, one needs, at a minimum, to trust the mechanism of recordation since distributed consensus systems cannot provide any guarantees for it (Lemieux, 2017; Victoria Louise, 2016). Richard Feynman put it eloquently when investigating the incident of the Challenger; he wrote: "You know the danger of computers, it's called GIGO: garbage in, garbage out" (Feynman & Leighton, 2001, p. 107). Blockchains and distributed ledgers are no exception. Thus, the trustless exchange of real-world assets on such systems is a non sequitur for it appears to require trust in the representation of the real-world asset. And, more importantly on the institutional mechanism that allows for the representation of the external assets. Consequently, the current, well-understood mechanisms to foster trust would apply to the perspective mechanisms of representing real-world assets in these systems.

However, it is often said that trust in blockchains and similar architectures does not reside with other autonomous agents, rather that trust is needed in the software and algorithms of each system so that, what is argued for, appears to be that one of the major innovation of blockchains is to transfer trust to

the protocols. On this basis, this chapter now turns to assess whether trust in technology is possible and, then, what changes – if anything - when distributed consensus systems come into the picture.

3.3 Trust in Distributed Consensus Systems

Can one trust technology? What does it mean that trust on the blockchain does not rest with organizations, but rather with the security and auditability of the underlying code (Wright & De Filippi, 2015)? Does it make sense to say that one trusts technology at all? These issues are not limited to the field of DCS technologies, rather they affect our current state of affairs due to the dissemination of ICTs and the subsequent information revolution (Taddeo, 2010a, 2010b). It turns out that the answer to these questions hinges on whether trust applies to technological systems or not, which in turn, depends on one's notion of both trust and technology.

Logically, one's conception of technology comes first. The pervasiveness of technologies across human societies is an essential element of the human condition. As it has been eloquently put "the laws of technology allow us to find the logic of human evolution: starting from the hero of the ape-like tribe of early humans grasping how a bone could be used as a weapon, down to the orbital satellite in Kubrick's famous match cut in 2001: A Space Odyssey" (Pagallo, 2013, p. 20). Such an account falls into the instrumental view of technology, in that, the technological device bone is a mean to an end, namely, obtain control of a scarce resource. The instrumental view of technology is found in Heidegger's work. This Author starts from the clear definition of technology that everyone knows, that, to the question "What is technology" answers with two statements: "Technology is a means to an end [and] a human activity" (Heidegger & Lovitt, 1977, p. 4). While one can find other accounts of the nature of technology, this dissertation adopts this "instrumental and anthropological definition of technology" (*ibidem,* p. 5). With this definition of technology this section now aims to assess the possibility of trusting technological artefacts.

In line with Heidegger's account, Pitt argues that technology is humanity at work (Pitt, 2010). Consequently, he offers a critical clarification with regard to trust in technology. In fact, the simple question can we trust technology requires the addition of the purpose for which a specific technology is trusted. Thus, this question becomes "can we trust our technologies to perform as promised?" (*ibidem*, p. 449). He argues that this question makes sense only if there is a prior negative assumption the technology ought not to be trusted, he then grounds it on three further assumptions. First, that technology has an ideological stance. Second, that the law of unintended consequences is at play and, third, that designers and builders of new technologies are after their personal gain and not for the betterment of humanity. Pitt adds an important corollary to our initial question. Chiefly, as it stands, the questions can you trust a blockchain or a distributed ledger are unanswerable for they deal with something that does not exist. As this dissertation showed in the previous chapter there is no such thing as The Blockchain, A distributed Ledger or A Directed Acyclic Graph. Analogously, "it is a category mistake to ask questions about Technology" (*ibidem*, p. 453). Regardless, in the literature on DC systems many authors take for granted the possibility of trusting The Technology, for example, Catalini and Gans write that "[t]rust in the intermediary is replaced with trust in the underlying code and consensus rules" (Catalini, 2017, p. 8).

The next paragraphs deal with the possibility to trusting blockchains and distributed ledgers from the general attitude of trust in technological artefacts. Nickel et al. distinguish between a rational-choice view of trust and motivation-attributing accounts of trust (Nickel, Franssen, & Kroes, 2010). The former considers trust as a risk-assessment judgment the trustor makes in terms of the subjective probability that exceeds a certain threshold for trusting. The latter, instead, holds trust as in the cognitive-process wherein the trustor also considers objective attributes of the trustee. The rational-choice account of trust dates back to Coleman but has been the subject of numerous critiques for it lacks a theory of mind of the trustee (Coleman, 1997). Regardless, even this account of trust is unfit to support the argument that it is indeed possible to trust a technology for performing a specific function. The authors conclude that "the

extension of rational-choice account of trust to technical artifacts does not lead to a genuine notion of trust in technical artifacts, different from reliability" (Nickel et al., 2010, p. 435)

Moreover, they conclude that motivation-attributing accounts of trust cannot be adapted to technology because these accounts assume that trustees possess mental states valuable from the perspective of the trustor, and interests of his own. They also hold that "in the case of socio-technical systems, which involve humans as operators, trust in system's operators cannot be transferred straightforwardly to the system as a whole" (*ibidem,* p. 443). I agree with this perspective. So that, narratives about trust in the protocols of blockchains and distributed ledgers conflate the notion of trust with reliability (Auinger & Riedl, 2018).

Therefore, it is possible to conclude that trust in the particular technology at hand to perform the tasks they are designed to execute is, in fact, reliance. Consequently, one relies on the Bitcoin system to execute transactions as its specifications demand, because Bitcoin's software has no alternative than executing as programmed. The inability of deviating from specifications of software system eliminates risk, which is an essential condition for trust relationships. This entails that were a transaction in bitcoin to disappear for a bug in the code one would not feel betrayal but disappointment. Analogously one would not feel betrayal toward one's alarm clock were it to fail to execute the task of playing a given sound at the desired time.

Yet, one finds many examples in the literature where the words trust, trustless, and trustworthiness are applied to the technology itself. For example, a prominent advocate of Bitcoin explains in the following way, trust in the network is ensured by requiring participants to demonstrate proof-of-work, by solving a computationally difficult problem. The cumulative computing power of thousands of participants, accumulated over time in a chain of increasingly-difficulty proofs, ensures that no actor or even a collection of actors can cheat, as they lack the computation to override trust (Antonopoulos, 2014). This is held in spite of the fact that most of the mining nodes are controlled by a small number of Chinese actors.

It appears that one is left with a choice. Either one adopts a Wittengsteinian stand and concludes that trust has a different meaning than the one argued in the previous pages. Or one must conclude that in the distributed consensus space one finds reliance on technological artifacts disguised as trust (algorithms, code, and so on). The latter option is correct. This section, therefore, ought to conclude by explaining why this conceptual shift – from reliance to trust – is highly consequential. First, the reasons that appear to account for the conflation of trust and reliance are discussed.

The culprit of the conceptual shift from trust to reliance is multifold. Different vocabularies among discrete disciplines are responsible. If one reads the blockchain literature in the system science domain, one easily finds contributions that consider blockchains as trust-free transaction systems (Notheisen, Cholewa, & Shanmugam, 2017). The separation of academic disciplines proves, again, unproductive with regard to complex subjects that have no regard for such boundaries (Galloway, 2004). Consequently, this works aims to partially address this issue by adopting an interdisciplinary approach.

Another reason is the belief that trust is persistent. It seems that blockchain proponents and technologist believe that once, as Nakamoto said, one removes the need for a trusted intermediary that trust, somehow, persists in the algorithms and in the code. This stance is tantamount to identify trust as entropy such that, as the second law of thermodynamics dictates in all spontaneous processes the total entropy increases and the process is irreversible. Trust is not entropy. If, as it seems the case, distributed consensus systems can – in some cases – remove trust, trust itself does not persists making the underlying code trusted or trustworthy. Still, the shift from trust to reliance is highly consequential.

Another motive to preserve the idea that blockchains and distributed ledgers enable trustless trust is marketing. Trust sells well. The recent success of initial coin offering (hereinafter, also, ICO) seems to support the previous claim (Hoffman, 2018; Oren, 2018). Yet, in order to separate hype from reality, one ought to be precise and recognize that the core innovation of blockchains and similar systems is the shift from trust to reliance, with the important caveat outlined in the previous section, i.e. direct access to endogenous assets on open networks. This section argued that it is not possible to devise a meaningful

notion of trust in technology within the dominant understanding of trust. Hence, one does not trust distributed consensus systems, but he relies on them to achieve a given goal. This also explains why the discourse on systemic trust does not apply to our subject matter.

Systemic trust is the trust in institutions[22], that is, trust in legal systems, markets, and the player operating within society (Mutti, 2004). The presence of systemic trust is critical for the successful development of economies and societies. The first blockchain implementation was developed at a time when systemic trust stood at an historical low amid the 2008 financial crisis (Hayes, 2019). Before dealing with the effects of blockchains and distributed ledgers on systemic trust, this notion has to be explored further.

If one applies the previous accounts of trust, both the rational-choice account and the cognitive one it is possible to understand how systemic trust is, indeed, possible. For one, institutions possess discretion in the sense that they can influence their behavior without any input from other agents. Institutions do have objectives and goals of their own that may or may not be transparent to the outside and could be misaligned with the ones of the agents trusting them. Hence, institutional trust is possible and amounts to systemic trust in the interplay of different institutions across societies. It is interesting to note how, in respect to the subject of money, Luhmann noted how systemic trust and interpersonal trust are intertwined. More precisely, he argued that systemic trust acts as a distributed reduction of complexity and, consequently, that system trust displaces interpersonal trust (Luhmann, 1979). Systemic trust requires explicit and built-in control from society to function appropriately, this lack of control contributed to the failure of systemic trust in 2008.

If one pairs this view of systemic trust with a specific account of trust the relation between systemic trust, blockchains, reliance, and innovation becomes apparent. Durante argues that trust is, also, "a twofold relation between two relations: with control on one hand, and lack of control of the other hand,

[22] Institutions is intended in the sense specified by Searle (Searle, 2005)

at the same time" (Durante, 2010, p. 356). Through these theoretical lenses one starts to grasp the innovation potential of distributed consensus systems. Let us compare the difference between a relation on the basis on institutional trust and one based on reliance on a given technology by considering the same example of transfer of digital value. In the first instance, when trustors trust institutions to transfer value they lose control over their assets for the gain in the reduction of complexity, that is, the ability to complete the transaction. In the second case, if we hold the goal constant trustors need not trust a distributed consensus system rather, they merely rely on it. Hence, trustors still enjoy the reduction in complexity (being able to achieve their goal) with a significant decrease in the risk involved. Blockchains and distributed ledgers appear to reduce complexity with less risk. However, a critical disclaimer is in order.

The previous argument holds under the following assumptions. First, agents must interact directly with the technological apparatus, that is, without intermediaries such as exchanges, wallet providers and so on. Second, the benefits of shifting from trust to reliance for transacting applies only to endogenous assets, while, on the contrary, exogenous ones still require an institutional structure, hence systemic trust. Third, this argument stands solely for the set of relations that are possible under the current technological paradigm, which, as it stands, amount to the limited domain of payments over the internet with dubious currencies.

These remarks also entail that when agents interact with these technologies in a mediated fashion, the level of trust required increases. Also, this analysis shows how drawing general claims from specific implementations of the technological landscape of DC may lead one astray as it is a category mistake. In fact, much has been written about distributed consensus systems ignoring the reality that many of the daily interactions occur on exchanges so that a higher degree of systemic trust is present. Another critical aspect is that analysis at the level of one system – usually Bitcoin or Ethereum – are continuously taken as general claims on this class of technologies. For example, Auinger & Riedl argue that "[W]hile we have chosen Bitcoin as our study context […] we are currently not aware of arguments why our

conclusions should not be generally applicable to other blockchain application" (Auinger & Riedl, 2018, 7). Even if induction, i.e. inference based on many observations is a dubious logical process. The aim of this section – and in no small part of the previous chapter – was to show how induction with regard to distributed consensus systems is an undesirable method of investigation.

Finally, this section only dealt with open systems as permissioned ones do not claim the same degree of trustlessness, and because most of the arguments that support the adoption of this class of technologies appear to not apply to permissioned systems. However, there are significant implications that also apply to the latter case when it comes to the interplay of trust, control and reliance. On this basis, the next section deals with trust in the context of permissioned distributed consensus systems.

3.4 Trust in Permissioned Systems.

Some authors split permissioned systems in two categories: consortium and private (Chu & Wang, 2018). According to this classification, consortium systems allow only known participants to join the network while private ones have a single participant in the consensus process. It is clear that this distinction needs to be dismissed for a distributed, decentralized system must have more than one participant to represent a significant innovation, otherwise one is dealing with a distributed database. Consequently, this section deals with permissioned systems of the consortium-type. That is, where multiple known entities participate and maintain a shared data structure, be it a blockchain, a distributed ledger or a DAG.

The critical element of these systems is the presence of a root-authority that issues identity certificates. The root authority is a SPoF (Single Point of Failure), and a trusted third party (TTP). In the literature, these systems receive much less attention under the assumption that they are just glorified distributed databases. In contrast, commercial efforts are actively pushing toward this type of systems. In fact, established players in the likes of IBM, Microsoft, and Oracle are engaging with permissioned

architectures. In recent times, several products have been taken to market that implement this type of data structure, prominent examples are found in the food supply chain as well as in international trade. As an example, the Ethereum foundation – a legal person incorporated in Switzerland – in charge of maintaining the world 2nd permissionless distributed consensus system (Ethereum) established the Ethereum Enterprise Alliance (EEA) with the aim of accelerating the adoption of the enterprise version of Ethereum (EE). The initiative aims to establish open standards for industrial applications. Additionally, state-led initiatives in the field are likely to make use of the same design (OECD, 2019; Ølnes & Jansen, 2018). There are different reasons as to why established players may opt for a permissioned system, these reasons are both legal and technical. As for the technical part, permissioned systems do not require a consensus algorithm that exploits the use of a scarce resource (i.e. PoW or PoS), because when one deals with known parties Sybil and 51% attacks[23] are not possible. The artificial commitment of a scarce resource has been proposed in the computer science literature to deter spam in e-mail communications and in other areas as well, the assumption is that it renders the spammers business model unprofitable by requiring the commitment some amount of a scarce resource. Consequently, this different adversarial model allows permissioned systems to implement other BFT consensus algorithms (i.e., PBFT, Honeybadger, etc.) that enable these architectures to scale much more efficiently regarding TPS. This is also reduces the environmental concerns associated with the energy required to run permissionless networks (Chapron, 2017).

Legal reasons play an important role as well. More precisely, the adoption of an identity layer does not challenge established legal modes of regulation and enforcement in the cyberspace. Think, for example, of know-your-customer (KYC) and anti-money-laundering (AML) regulations. The possibility of identifying the transacting parties makes regulators more comfortable; it does not disrupt enforcement

[23] A sybil attack is an attack vector that requires the attacker to create numerous *fake* nodes to then flood the network in the case of denial of service attacks (DoS) or to isolate one or more other nodes to perform a double-spending by feeding the targets with a different version of the DC data structure.

of legal norms as the permissionless data structures do. Another compelling legal reason to opt for permissioned systems lies in the interplay of blockchain technology and data protection regulation. Think, for example, to the practical difficulty of enforcing art. 17 of the GDPR on public blockchains due to their immutability (Pagallo et al. 2018). Lastly, permissioned systems operate under the aegis of a contractual agreement between parties that – presumably – regulates the governance aspect as well as possible controversies that may arise during the operations of the system. Thus, it comes to no surprise that permissioned systems are more favored by regulators and established institutions while being slanted by proponents of permissionless solutions. Against this backdrop, the next paragraphs examine the implications for trust, control and reliance in the context of permissioned architectures, which – it is important to stress – are being developed by industry and by the public bodies. A recent example of this is the announcement of the European Blockchain Service Infrastructure[24].

The previous section showed how permissionless systems enable the shift from trust to reliance in the case of direct transactions with endogenous assets. The same does not hold true for permissioned systems. In fact, these systems are designed to streamline and clear business (or government) relations that are already required trust. Therefore, in most cases, these systems deal with the transfer, clearing, and traceability of exogenous assets or rights. However, it is possible in principle to establish permissioned systems that will deal with endogenous assets as the recent Libra initiative is set out to achieve.

For example, an implementation of a permissioned DC system gain prominence when the retail giant Carrefour partnered with IBM to allow customers to trace the origin of food across the supply chain. The system went live in September 2018, when the first asset reached the market with a QR code sticker on its packaging that enables customers to get information about its supply chain with the courtesy of a permissioned blockchain. This first asset was a chicken. In particular, the Carrefour-IBM system

[24] https://ec.europa.eu/digital-single-market/en/news/european-countries-join-blockchain-partnership for an overview of the project. Accessed on the 10th of September 2019.

aggregates data from 29 farms, 2 feed mills, and 1 slaughterhouse allowing customers to access the complete history of the chicken from birth to purchase. Chickens are not born and live on blockchains. Yet, the reason to deploy similar solutions is arguably found by looking at the effect of this system on trust.

In particular, and this is the crucial point, trust is reduced to just one transaction and a single entity, namely, the entry point transaction (EPT). In the previous example, provided that the system is open, transparent and that the digital representation of the asset is secure, consumers need not trust the whole supply chain but just the first representation of the asset on the system. Consequently, the risks of the misrepresentation, mistreatment, and incorrect information about the asset are reduced to the EPT. The relation is less risky, and, therefore, requires less trust. This argument holds for any other system that transacts with exogenous assets as well with the representation of other rights on distributed consensus systems.

One can infer that, in a more complex scenario, after the exogenous assets undergo a critical number of transactions between different parties the trust required for subsequent transactions would drastically be reduced. In the long term, this may also lead to a shift from trust to reliance; but this is speculative. Many issues need to be addressed for such a shift to occur, for the time being, the perceived gain in the implementation of a permissioned system lies in the reduction of trust from n transactions to one, namely the EPT. Trust in permissioned systems is required at the level of the EPT transactions. This is the situation with regard to the assets, however a few words on the entities that develop such systems are in order.

A certain level of trust is necessary in permissioned distributed consensus systems. More precisely, trust in the developers, and the institutions that build and maintain the technical infrastructure where the transactions occur seems required. In the previous example, one must trust IBM as the provider of the technical system that tracks, records, and displays the history of one’s chickens. It is possible to argue that such trust could and should be reduced via the openness of the source code as is already the case in

many permissionless systems. Chiefly, these systems ought to operate transparently to make a significant impact on the issue of trust. If, as it seems, the beliefs that individual users could review and understand the source code by themselves is purely aspirational, the integrity of these systems may be granted by a new set of institutions devoted to auditing the code of permissioned systems or by other mechanisms such as standards and pre-approval. If one considers the decrease in trust the main driver toward the adoption of these systems, one ought to be wary of not allowing for the establishment of trusted systems as black boxes. In this sense, the likely characteristics of a desirable permissioned systems partly overlap with the core properties that appear to drive blockchains' adoption.

The previous remarks shed light on how trust is affected within permissioned DC systems. It is now time to address another aspect of this technology that relates to trust, namely, control. As Durante concluded, "trust is not only a relation between interactive agents but, primarily, a cognitive relation with what remains out of control within what we believe to hold control over" (Durante, 2010, p. 365). This leads the last paragraphs of this chapter to explore the relation between trust and control and to assess their interplay in the context of distributed consensus systems.

Castelfranchi and Falcone recognized the presence of a dialectic relation between trust and control. They conclude that "control is antagonistic of this strict form of trust [interpersonal], but that it also competes and complements it for arriving at global trust [systemic]" (Castelfranchi & Falcone, 2000, p. 821). Further, they showed how control could create trust making the trustee more willing or effective. This account of control's influence over trust fits within the theoretical framework of Luhmann's work. More precisely, some of the mechanisms identified by the German sociologist to establish trustworthiness resemble a form of control. Think for example, of sanctions and control of the trustor over the trustee. Therefore, it appears that control can, indeed, foster trust under some circumstances. However, too much control, and trust vanishes because risk is eliminated, which has been established earlier as a necessary condition for trust relationships.

Moreover, the topic of control by technological means of ICTs demands a brief digression. Many scholars recognize the social nature of technology, crucially, "technology is social before it is technical" (Galloway, 2004, p. 80; Winner, 1980). Galloway also showed how control exists after – architectural – decentralization in the forms of protocols, "control is the outcome of the developments in networked communications […] the founding principle of the net is control, not freedom" (*ibidem,* p. 142). Hence, if control is an enabler of trust and protocols control society, our closing question is critical. Are permissioned systems enabling the shift from trust to reliance by introducing control in their architecture?

Despite the interplay of trust, control and communication networks much of the literature on the topic of distributed ledgers hardly covers the issue of control, with a few exceptions. Jannice Kall argues that "blockchain [sic], as a technology, offers the possibility to code property control into the property objects themselves" (Käll, 2018, p. 137). She further argues that the mechanism by which blockchains and distributed ledgers enable a further level of control is analogous to the mechanism of digital right management (DRM), this development is seen through the lens of the shift from a disciplinary to a control society following the work of Deleuze and Haraway (Deleuze, 1988). While Kall manages to strike a critical characteristic of the technology, namely, the higher degree of control that it enables, she falls short in depicting the interplay between control and trust.

Conversely, Meijer and Ubacht highlight the tension between trust and control. They show how the narrative around blockchain and distributed ledgers speaks about trust but means control. They conclude that "Blockchain [sic] technology is empirically often related to trust, but should rather be related to control. The empirical data suggests that if complete control is possible in blockchains, then no trust is needed" (Meijer & Ubacht, 2018, p. 4). Problematically, they adopt Nooteboom account of trust and control, according to which the term reliance includes both trust and control (*ibidem*). For the purpose of this work, it seems necessary to maintain the distinction between trust and reliance because it grounds the argument that the technologies at hand enable a shift from trust to reliance under some circumstance.

Therefore, this chapter adopts a different account of reliance and control. Chiefly, reliance differs from control in that the latter requires the possibility of intervention upon the controlled set of actions (Castelfranchi & Falcone, 2000). Reliance does not entail the possibility of intervention. Also, Meijer & Ubacht assume that complete control is possible in blockchains, hence the shift from trust to control, however, they fail to recognize that this shift occurs only with regard to direct engagement with exogenous assets in open systems and not as a de facto consequence of implementing a blockchain-type system. In other words, reliance displaces the need for trust while control reduces it. In the extreme case, control is capable of eliminating trust as in the well-known case of the Panopticon.

Consequently, one relies on systems where one transacts directly with endogenous assets while one needs to trust when transacting with exogenous assets on both open and closed systems. Most importantly, in this second case, the amount of trust required is significantly less because these systems enable control through cryptography, transparency, irreversibility and the other properties highlighted in the previous chapter.

Finally, the tension between trust and control in closed systems that enable the transfer of exogenous assets results in a decrease of trust and a corresponding increase in control on the tokenized assets. The assumptions that drive the adoptions of such systems, therefore, demand careful consideration of the new modalities of control enabled by this new class of technologies.

3.5 Conclusion

Trust is a complex issue; this chapter explored the narrative on trust that permeates the literature of many fields starting from the general level up to the few contributions focused on distributed consensus systems. Chiefly, the innovation of these systems lies in the possible shift from trust to reliance. Thus, if one holds that the presence of trust in x is less desirable than reliance on x, then this technology has

the potential to unlock an array of untapped benefits across many areas. For example, to transfer value across the globe with ICT one moves from trusting banks and institutions to rely on the software of a computer system. However, it is necessary to consider if the change is desirable and what is the cost associated with it.

Other relevant conclusions of the previous analysis are the following. For the shift from trust to reliance – the famous design of a system that do not requires trust – to occur three conditions must hold. First, the trustors must interact directly with the computer system without the presence of an intermediary. Consequently, trustors must possess the necessary technical skills to vet to source code and invest enough time to manage their access credential and store the whole copy of the data structure of the system – this is the state of affairs at the time of writing. Second, the information systems must be open and transparent so that agents can witness the systems' operations. Third and final, transactions ought to involve only endogenous assets – i.e. cryptocurrencies. Because the tokenization of exogenous assets requires a trust leap. That is, agents must trust the process of tokenization not to misrepresents the assets and to provide specific guarantees against fraud, the so-called entry point transaction problem.

On this basis, one might entertain the conclusion that systems which fall outside the permissionless/endogenous assets categorization are not relevant. On the contrary, section 3.4 made clear that systems which deal with exogenous assets can decrease the need for trust, albeit never getting to the point of displacing it in favor of reliance as in the case explored in section III.III. The reduction to trusting multiple parties to trust only the ETP and the root-authority is, indeed, an improvement over existing structures. Thus, one can explain the growing interests in solutions aimed at supply chains and other economic areas where trust is of paramount importance.

Permissioned systems require less trust to execute transactions or computations by enabling control through software architectures, thereby reducing the action space of the entities involved. For example, a party cannot tamper with the information stored on a blockchain for a supply chain, thus the action space of the party is reduced. The reduction is achieved via technical solutions such as hashing

algorithms that provide a distributed control over the information. That is, every participant in the system can control the other's actions, and – in this case – the state of the information. Permissioned DC systems decrease trust through distributed control.

In conclusion, it seems that the effects of distributed consensus systems on trust does not justify their engagements. Accordingly, the next chapter deals with another proposition often put forward to justify the adoption of distributed consensus systems, namely, that these systems enable a new mode of governance, thereby competing with or perhaps even substituting other co-ordination mechanisms such as, the law, market, and firms.

4. Governance and Distributed Consensus Systems

The proposition that blockchains and distributed ledgers will eventually lead to new forms of social organizations is bold and pervasive. While this is not the first time that technology has been considered capable to foster some social arrangement other than others (McKnight, 2012; Pagallo, 2008), it appears that one of the core arguments to foster the adoption of distributed consensus systems is linked with their

alleged ability to enable agents to organize in novel ways. Due to the low level of systemic trust in western societies, the blockchain movement has gathered an unexpected amount of support. Accordingly, this chapter examines the claim that blockchains and distributed ledgers are a new mode of governance, or according to some strong proponents of the technology systems of rules where nobody makes the rules! The goal of this analysis is to show that, similarly to the case of trust examined in the previous chapter, an in depth analysis of the previous claim leads to the conclusion that, as it stands, blockchains and the like might do little to compete with other governance mechanisms. As it will be argued in the following pages, this is mostly because there is an unspoken element of rules that is unlikely susceptible of being programmed. To use John Rawls words: "as with any set of rules there is understood a background of circumstances under which it is expected to be applied and which need not - indeed which cannot - be fully stated." (Rawls, 1955, p. 17) Additionally, blockchains and distributed ledgers are, in their current implementation incomplete system of rules because they lack secondary rules.

Some regard blockchains as a system of rules capable of competing with other modalities of regulation, such as norms and markets (Davidson et al., 2016, 2017; De Filippi, 2018). Other authors echo similar claims, namely, the possibility that blockchains could unlock new and uncharted ways of cooperation and collaboration (Galen et al., 2018). In other words, some regard distributed consensus systems as a new mode of governance. While the notion of governance tends to be fuzzy, it is possible to argue that the different mechanisms, artifacts, technologies, and institutions designed to achieve coordination in a given system can be conceptualized under a broad notion of governance[25]. Therefore, this chapter deals with the notion of blockchains and distributed ledger governance in order to critically examine the claim that such artifacts are systems of rules capable of organizing and coordinating the human affair in a novel fashion.

[25] For an overview of the relevant understandings of governance from the legal perspectives concerning new technological developments see (Pagallo et al., 2019)

Arguably, the goal of distributed consensus systems has always been achieving coordination in a multi-agent system characterized by specific assumptions. Since the birth of Bitcoin, blockchains enabled coordination of mutually-distrusting parties to transfer a scarce resource over the internet without relying on a trusted third party. Other projects, then, set out to achieve coordination by blockchains in other fields beyond online payments. To a relevant extent, the promise of this class of technologies is to bring the short-route proper of P2P systems to countless sectors, as such, it is evident how blockchains and distributed ledgers must – to achieve their stated objective – enable a new way of governance (Pagallo & Durante, 2009).

A critical characteristic of distributed consensus systems as a coordination mechanism is their alleged decentralized and disintermediated nature. It seems that, in the discourse around blockchain governance, a false dichotomy is present. More precisely, both the literature on the topic and technologists seem to split governance structures into two, opposite, categories. On the one hand, governance is centralized, concentrated in the hands of an institution or a powerful intermediary. This model of governance is deemed inherently inferior due to its vulnerabilities and its inclination to accrue power in the hands of a few individuals. On the other hand, governance is decentralized, dispersed among equipotent peers characterized by a flat, rather than hierarchical structure (Atzori, 2015; Atzori & Ulieru, 2017). This latter model of governance is portrayed as intrinsically better and more desirable than the former (Arruñada & Garicano, 2018; Baldwin, 2018). While this conceptualization of centralized versus decentralized structures has gained prominence in the blockchains space, and it has the benefit of theoretical simplicity, things are more nuanced. More precisely, sound and proven coordination mechanisms tend to exhibit both elements of centralization and decentralization in a multi-layered arrangement.

Law is selected as a measuring stick for governance mechanisms for the following reasons. First, the famous dictum "code is law" is ever-present in the blockchain discourse, both in academic writing and in the discussion within the community (Yeung, 2019). Additionally, the Lessigian formula is often used

to justify or argue in favor of contentious decision regarding the governance of blockchains' software (DuPont, 2017). Second, the blockchain lingo is filled with improper use of legal terminology. Think, for example, of the notion of smart contracts examined in the second chapter, or at the attempts to implement smart properties regimes within blockchain systems (Ishmaev, 2017; Merkle, 2016). Thus, it seems fitting to adopt the conception of the law as a coordination mechanism to measure and evaluate the attempt to establish concurring code-based system of rules based on distributed consensus systems. And, consequently, to evaluate if blockchain's adoption is justify based on their innovation in the governance space, or if it falls short thus pointing to the need to examine other reasons why agents engage with this class of technologies.

Third and final, the law is arguably the most diffused mechanism for coordination. On the contrary, this chapter sets out to argue that the promises of governance by and with blockchains or distributed ledgers suffer from a conceptual hurdle. That is, as it stands blockchains are an incomplete system of rules, therefore, unable to provide an alternative system for coordination. In light of these remarks, the following chapter begins by fixing the variables of the issue at hand, namely, by qualifying the actors, the context and the technologies. Then, section two delves into the consequences of adopting an incomplete system of rules to achieve coordination, by exploring some real-world examples of (s)co-ordination by distributed consensus systems. Section three explores the literature on the governance of distributed consensus systems and sets the stage for section four, which attempts to pinpoint the reason for the incompleteness of these systems.

4.1 Variables

This section lays out the governance issue by examining the different variables that come into play at different levels of analysis. Finck argues that blockchain governance is multidimensional, in fact, it is trivial to note that the issues related to the governance of blockchains and distributed ledgers are, per se',

a sign of its multidimensionality (M. l. Finck, 2018). While different authors have established, explicitly or implicitly, this multidimensionality the next pages aim to flesh out other aspects that have been neglected by the literature on the topic.

The aspiration of this section is to provide the reader with the appropriate theoretical lenses to examine the governance of a blockchain or a distributed ledger system. The method of the level of abstraction is borrowed to highlight the salient characteristic of the issue at hand (Floridi, 2008). Preliminarily, it is important to note that a mix of variables is adopted to better understand the problem. That is, the variables that populate our model are not only technical - as in the case of computational complexity - but also social - as in the case of values embedded in some systems - and legal.

Preliminary, it is crucial to delimit the scope of the concept of governance in the context of blockchains and distributed ledgers. At the first level of abstraction adopted by this chapter, one ought to distinguish between three aspects of governance that are relevant. Campbell-Verdun provided a useful conceptualization that this section borrows to populate the first LoA with three variables (Campbell-Verduyn, 2018). When it comes to our subject matter, there are three types of governance: governance of blockchains, governance by blockchains, and governance with blockchains[26]. The ordering of the variables points to the relation between them. The governance of blockchains determines the limits and scope of the governance by blockchains which, in turn, shapes the governance with blockchains.

Bitcoin's monetary policy implementation provides a clear example of the interplay among the variables at the first LoA. At the inception of Bitcoin its creator, Satoshi Nakamoto, decided to limit the total supply of Bitcoin at 21 million bitcoins. This decision exemplifies governance of the Bitcoin blockchain as Satoshi determined the monetary supply of Bitcoin. Later, the software was implemented according to the monetary policy envisioned by Nakamoto, hence, the parameters of Bitcoin's software provided the governance - in terms of monetary supply - by the blockchain. Finally, the Bitcoin system

[26] The term blockchains is used as a placeholder for the broader concept of distributed consensus systems.

imposes the monetary scheme on users of the network in what is an example of governance with blockchains. That is, users and other stakeholders are subjected to the monetary scheme as determined by Nakamoto at the level of governance of Bitcoin, implemented at the level of governance by/with Bitcoin.

Therefore, it seems possible to contend that the governance of blockchains is of primary importance because both governance with and by blockchains seems to be directed by the governance of blockchains. Lastly, as the rest of this chapter aims to elucidate, the lack of a clear framework for the governance of blockchains is the primary cause of the incompleteness of blockchains as a system of rules. As well as the main reason why blockchains' adoption does not appear to be justified solely by the argument that this class of technologies enable new modes of governance similar to markets, and governments. On this basis, it is now possible to continue examining the other levels of abstraction of the issue at hand.

The second level of abstraction is the degree of openness of a system. Simply put, different methods are used to grant permission to read/write/append to different parties as explained in chapter two. In matters of governance of blockchains, it is crucial to keep this distinction in mind for distinct considerations apply to, on the one hand, permissionless systems and, on the other hand, permissioned or private ones. More precisely, the governance structure of a permissioned or private system is designed and enforced by the root authority of each system. Therefore, even if specific governance arrangements might represent an interesting object of study, they lie outside the scope of this chapter because they are, arguably, complete systems of rules as opposed to the incompleteness nature of permissionless blockchain. In other words, the critical issue of the governance of blockchains does not affect permissioned or private system for their implementation of a hierarchical, instead of a flat, power structure. That is, someone in permissioned or private blockchain has complete decision powers on, arguably, all the facets of the governance of the system. Hence, by leveraging LoA(2) one can set aside systems which belong to the category of permissioned and private and focus one's attention on the open

or permissionless architectures. This is also necessary because the arguments for adopting blockchains as a system of technical rules for coordination point to permissionless systems rather to permissioned ones, such is the case in the context of the Bitnation project[27].

After having established that this chapter deals with the governance of permissionless blockchain systems one ought to further identify other elements of blockchains' architecture that are relevant to this study. At LoA(3) one finds the computational complexity. More precisely, blockchains are either (a) Turing incomplete or (b) Turing complete, tertium non datur. Turing incomplete blockchain systems are designed to only execute a pre-determined set of computations, meaning that – by design - users of these systems have a limited degree of freedom in what can be executed within the system. For example, users interacting with Bitcoin, Litecoin and Zcash have access to a limited set of functions such as the transfer of tokens, simple escrow arrangements, time-delay transactions, etc. On the other hand, Turing complete systems can simulate any real-world general-purpose computer. Therefore, users of this second generation systems can deploy arbitrary programs that the network executes in a distributed fashion. For example, users of the Ethereum platform can write and deploy programs – aka the smart contracts examined in the previous chapter (Bartoletti & Pompianu, 2017; Bhargavan et al., 2016). Think of a world computer where the execution of software occurs in thousands of computers distributed across the globe. The most prominent example of a Turing complete blockchain system is Ethereum. In principle, any program that runs on a regular computer can also run on the Ethereum blockchain using the Ethereum virtual machine.

Distinguishing between Turing incomplete and Turing complete blockchains is relevant because of the distinction between on-chain and off-chain governance. On the one hand, the former refers to the implementation of governance rules at the system level (i.e., coded in the software on the blockchain). In other words, governance processes are endemic to the system's architecture. In the wild, on-chain

[27] https://tse.bitnation.co/ accessed regularly for the author's amusement.

governance is implemented via voting protocols in the form of smart contracts. Examples of systems that implement this logic are Tezos, and Decreed. On the other hand, off-chain governance refers to governance processes outside the system's architecture. In other words, it refers to decision processes that are not coded into the system's repository. As it stands, the governance of most systems unfolds off-chain, while significant efforts are being channeled to put it on-chain.

Lastly, at LoA(4) one finds the actors and forces at play on the stage of off-chain permissionless blockchain governance. In other words, LoA(4) is concerned with the stakeholders - both active and passive - of the governance of blockchains, and with the distinct instances that activate the governance process. There are several actors in the governance of blockchains. Finck identifies three main actors in the context of blockchain governance and three marginal ones (M. Finck, 2018; M. l. Finck, 2018). On one side, the main actors in the governance of blockchain are the core developers, the miners, and the coin holders. On the other side, Finck identifies the marginal actors of blockchain governance as the users, the exchanges, the press and prominent voices in the blockchain space. This section adds to the previous categorization in order to generalize the model put forward in this chapter. More precisely, the founder(s) and the legal entities are added. A brief definition of the characteristic of the preceding actors is in order.

The core development team has been defined by Finck with regard to their function, hence, she regards the core software developers as the only holders of the commit key. This account is unprecise. First, the term core developers seem to have originated in the context of Bitcoin where the main version of the software is called Bitcoin Core. Second, core developers in the context of Bitcoin, for example, are the individuals who develop the software core, that is, anyone who contributes to the software's repository. Third, commit keys are an element of GitHub, hence this account potentially excludes developers of systems who are not developed on Microsoft's platform. Therefore, maintainers is a better term to define the individuals who have access to the commit key, because it applies to systems which do not have a 'core' software and better highlights the role of these individuals. That said, in the

governance context the maintainers team is supposed to hold some version of a cryptographic mechanism of identification. For example, the maintainers team of Bitcoin signs every commit with a PGP fingerprint to prove that the change has been endorsed by one of the maintainers. Putting aside this digression, it is important to highlight that the maintainers team endorses new changes to the protocol of a given system as a safeguard to the ones running the same version of the protocol.

The second actors in the governance of blockchains are miners or validators[28], for the purpose of this analysis we can set aside this difference, accordingly only the term miners shall be used. As defined in chapter 2, miners append new blocks to blockchains. Hence, they can decide to support or disregard the protocol changes implemented by developers. Their technical role does not clarify the extent to which miners play a role in each system, in particular, their role in the governance process seems to derive from their influence on the ecosystem as powerful stakeholders that provide the resilience of the consensus process. It is important to note that miners have a different influence degree depending on the consensus algorithm implemented. So that, miners within Bitcoin hold more sway in comparison to miners in systems based on other consensus protocols as TRON and EOSIO.

The third actors in Finck's conceptualization are coin-holders. Coin-holders exert much more influence when some aspects of the governance process unfold on-chain, this is because access to voting requires coins, e.g. voting tickets in the case of Decred. However, if the most important decisions are discussed and taken off-chain, the role of coin-holders is limited. However, the governance of public blockchains is generally aligned with the interests of coin-holders' because the increase in value of the coins is a goal shared by all the participants in a system. It is not clear that the classification presented above is exhaustive. Therefore, the next paragraphs consider other actors that appear to exert significant influence of the governance of this class of technologies.

[28] The presence of miners or validators depends on the type of consensus algorithm implemented in each system. Generally, in systems based on Proof-of-work miners append new information to blockchains while in other systems nodes who append new information are considered validators.

The founders play a central role in the governance of the systems they founded. The same holds for the legal entities that are often incorporated before the launch of the network, such legal entities range from non-profit foundation established in Switzerland (e.g. Ethereum) to for-profit corporation established in fiscal paradises (e.g. EOSIO is developed by block.one, an exempted limited liability company formed in the Cayman Islands). Although Finck does not include these entities in her classification of governance actors, they are involved in steering the direction of the development of blockchains. For example, the Ethereum foundation pays the maintainers of the Ethereum system and holds its intellectual properties. Moreover, it issues grants to foster the development of the ecosystem. Hence, it seems reasonable to regard it as an important player in the governance of Ethereum. Moreover, some systems are run by a for profit company behind their permissionless and distributed protocol, so that, it is fair to include this variable in the present discussion.

The founders also exercise a significant influence in steering the governance of blockchains as their opinions are highly regarded within the community. It is likely that founders are seen as charismatic figures. If Satoshi Nakamoto came back from the dark, it seems fair to assume that his opinion would be taken in high consideration by the Bitcoin community. This remark is supported by noting how, in the scaling debate that has been plaguing Bitcoin for the past few years, opposite sides argue in favor of their position also by claiming to represent the founder's true vision (Hearn, 2015).

Lastly, at LoA(4) one finds another set of variables that influence the governance of blockchains. If actors of blockchains governance 'call the shots' the second class of variables at the current level of abstraction are the stimuli in response to which the shots are called. It is possible to further distinguish the stimuli in two different subsets, namely, endogenous and exogenous ones. On the one hand, endogenous stimuli refer to the occurrences strictly related to the software of the protocol. Therefore, at LoA(4) in the set of variables of endogenous governance stimuli, one finds bugs in the software, technical fixes, optimization techniques, and technical additions to the software stack. These instances appear uncontroversial in their nature; hence this section will not provide a definition, yet this is not to

say that these variables do not influence the governance decisions of blockchains and distributed ledgers, as it will be showed in the next section.

On the other hand, one finds exogenous stimuli. These are the critical and most controversial drivers of blockchains governance, and, therefore of the governance by and with blockchains. An exhaustive list of variables at this level of abstraction is precluded for the open nature of this subclass of variables. However, one can still provide a sample of variables that belong to the category of exogenous stimuli of blockchains governance. Examples are disagreement of the philosophical foundations of the system, unexpected events, political controversies, ex-post mitigation strategies, and legal issues. The next section provides relevant examples of current governance practices present in the landscape of blockchains and distributed ledgers.

4.2 Real-World Scenarios

Among the thousands of blockchain projects launched in the 10 years since Nakamoto's conceptualization of the specification of the technology, one does not struggle to find events that exemplify the incompleteness of blockchains as a mode of governance. Additionally, these occurrences provide for an appropriate test-ground for the model of governance put forward in the previous section. That said, the following paragraphs deal with the Bitcoin software update from version 0.7 to 0.8, the Bitcoin block-size scaling debate, the frozen funds of the start-up Parity, the controversy over the funds raised by the Tezos project, the fix of Zcash's counterfeiting vulnerability, and the DAO case. The next paragraphs deal with each one in order.

In March 2013, the Bitcoin core maintainers rolled out an update to the Bitcoin core software in order to fix some issues and vulnerabilities, an example of endogenous governance stimuli as in LoA(4). Due to a bug in the update, the new version of the software was incompatible with the older one. Thus, a hard fork occurred[29]. The price of Bitcoin plummeted; immediate action was needed. The core maintainers persuaded two of the biggest mining operators to roll back to the previous version of the software for the sake of Bitcoin's integrity, these were the only actors involved in the final decision. In a matter of hours, the blockchain running the version 0.7 caught up the one running the new software thus solving the issue. In this case, the governance of the Bitcoin blockchain unfolded in a technocracy fashion. Few persons resolved the issue by coordinating without informing the other actors of blockchains governance. It is important to note that the miners running the new version of the code suffered the loss of the reward for mining 'on the wrong chain', legally speaking, a case could be made that the core maintainers who coded the update should be held responsible for the miners' loss on the grounds of, for example, extra-contractual liability. Putting legal concerns aside, two actors resolved the issue on the grounds of technical error, which, as shown above, had a real economic impact. It turns out that technical fixes are often charged with non-technical consequences.

No other discussion within the Bitcoin community has been as polarizing as the debate on the block-size of the Bitcoin's blockchain. By design, the block-size is limited to 1mb, therefore, the throughput of Bitcoin is in the order of 6-7 transactions-per-second. In order to improve the scalability of the system, some of the core maintainers at the time (namely, Gavin Andreessen and Mike Hearn) proposed to increase the block-size to accommodate more transactions and, consequently, increase the TPS. Against the increase of the block-size others argued that such a measure would lead to an unwanted centralization of the system for the added resources required to run a node if the size of the block had increased. Although empirical research on the topic suggests that Bitcoin "can increase the block size by a factor

[29] A hard-fork occurs when two incompatible sequences of blocks originate within a given network. Hard-forks are different from soft-fork as they persist indefinitely unless a fix is implemented.

of 1.7x without any decrease in decentralization" (Gencer, Basu, Eyal, van Renesse, & Sirer, 2018, p. 15) 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.

From the governance perspective, one witness an exogenous stimulus (the need to increase the TPS of the system) activating virtually every governance actors within Bitcoin (such as core maintainers, developers, miners, full nodes operators, coin-holders etc.) and even the long gone founder, Satoshi Nakamoto. Interestingly, both sides claimed to represent Satoshi's true vision. The block-size issue has not been resolved short of the system splitting multiple times to accommodate different opinions, what seems fair to note is that this ongoing saga 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 heavily influenced by their founders. It appears that the window for amending Bitcoin has been shut and the strength of the original blockchain lies in its traditional architecture. However, Bitcoin is not alone. In fact, other examples of governance hurdles can be easily found by looking at other blockchain systems, consequently, this subsection proceeds by providing further examples in Ethereum, Tezos, and Zcash.

The first episode in the Ethereum system under examination concern the freezing of the funds of the start-up Parity Technologies. Parity Technologies is a start-up founded by two former prominent members of the Ethereum platform, Gavin Wood and Jutta Steiner. Parity provides a technical infrastructure to build blockchain solutions for decentralized technologies. On November 6th, 2017 an unknown developer exploited a bug in the smart contract that serves as a library function for multi-sig hardware wallets made by Parity suiciding the smart contract. Consequently, an estimated 500.000 Ether were frozen, that is, no one can access the funds. Beyond the interesting legal ramification of this event, several solutions have been put forward by Parity to recover the funds, one of which - EIP proposal 999 - requires a hard-fork. It is possible to argue that Parity would happily compromise the Ethereum immutability - again - to recover the funds, the relevance of this occurrence from a governance perspective is self-evident. More precisely, several factors are critical at many different variables of our

model. For one, influential figures are personally involved in the controversy, thereby showing signs of a strong conflict of interests. The cause of the event is both an endogenous (a bug in the software) and exogenous example of the push for a governance decision. Additionally, there are no procedures in place to recover lost funds as such mechanisms require sacrificing important aspects of blockchains' philosophical foundations. As the time of writing, EIP n. 999 is still in draft status and it is unclear what, if any, solution will be implemented. What may seem suspicious to some is that after the Ethereum foundation granted a 5 million grant in real money - USD - to Parity Technologies for scalability, usability, and security, the impetus behind EIP n. 999 has substantially decreased.

A further example of governance hurdles plagued the start-up Tezos, which, quite ironically, aims to address the governance problems of blockchains. Tezos raised 232 million USD in an ICO in 2017, via a Swiss foundation. Shortly after the ICO ended, an acrimonious controversy arose between the president of the foundation - Johann Gevers - and Arthur and Kathleen Breitman, the founders of Tezos. It is sufficient to say that the founders of Tezos resorted to lawyers and courts to address the issue. Unsurprisingly, existing governance structures - which belong to a complete system of rules such as the law - provided the solution. Additionally, the coin-holders of Tezos were left wondering and kept in the dark while this process was unfolding.

Another controversial event in the governance of blockchains occurred recently within the cryptocurrency Zcash. Zcash is a privacy-protecting digital currency built on 'strong science', in other words, the Zerocoin electric coin company built Zcash relying on the scientific literature in the field of cryptography. Again, it is important to note the peculiarity of each system as Zcash has a for-profit company driving the development of the platform as well as a foundation in charge of fostering the value of financial privacy. The governance stimulus in this example concerns an endogenous variable, namely, a bug in the Zcash software. On March the first 2018, Ariel Gabizon a cryptographer working for Zcash discovered a flaw - so-called counterfeiting vulnerability - in one of the academic papers that laid the foundations for the cryptocurrency's software. Soon after discovering the vulnerability, which allows an

attacker to create false Zcash coins, Gabizon informed Zooko Wilcox (the CEO of the company behind Zcash) and Nathan Wilcox (CTO) of the vulnerability. Immediately, they deleted the transcript necessary to exploit the vulnerability from a web page where it was hosted, then they agreed to push a fix on a planned update to the platform later in October 2018. On February the 5th 2019 all the relevant information was disclosed to the public. Ça va sans dire, that the unfolding of this event strongly hints at centralization of the platform, in stark opposition to the ethos of blockchain communities. Additionally, no procedures are in place to deal with such an event, making the ad hoc solutions problematic from a legitimacy standpoint and, more importantly, the few people who knew about the vulnerabilities could have exploited it. Hence, in the trustless space of blockchains one needs to take their word for it and trust that they did not create any fake Zcash coin or conspired with another party to do so. The last example relevant to the argument put forward in this chapter concerns, arguably, the most well-known example of the failure of governance structures within a blockchain project. In fact, the following example lead to abandoning one of the much-heralded properties of blockchains: immutability.

The DAO was a short-lived experiment that aimed to create a new social and political paradigm using algorithmic authority mediated by cryptocurrency and blockchain technology (DuPont, 2017; Merkle, 2016; Reijers et al., 2018; Shakow, 2018). Simply put, The DAO was intended to be a decentralized, directly managed crowdfunding and investment vehicle to back development projects on the Ethereum blockchain; Kickstarter but on the blockchain (Alberini & Pfammatter, 2019; Chohan, 2017; Hsieh & Vergne, 2017). The DAO launched on April 30th, 2016. During the first stage of the project – the so-called creation period – The DAO raised the internal capital before being deployed on the Ethereum blockchain. Participants in the project deposited ETH (the native currency of the Ethereum platform) in The DAO smart contract and received DAO tokens in return at the ratio of 1:100. The DAO tokens would provide participants with voting rights to decide which project to fund and how to oversee them.

If this scheme appears to the legally trained reader as an unlicensed issuance of securities, she would be correct. In fact, the SEC considered The DAO to be an unlicensed issuance of securities after it brought an investigation on the leading proponents of the platform - the German startup slock.it despite their best effort to dodge any legal responsibility (Debler, 2018).

Brushing legal problems aside, The DAO broke all existing crowdfunding records by raising 11,994,260.98 ETH. Yet, despite the outstanding success of the creation phase, The DAO did not fund a single project. On June 17th, 2016, an unknown attacker executed an exploit (so-called race to empty attack) that drained about 30% of The DAO funds. It is important to note that the exploit resulted from a bug in the code and not from another type of hack. The DAO was subsequently put on hold; the experiment had failed. In the days after the exploit, a vivid debate arose within the Ethereum community (DuPont, 2017).

The community split in two. On one side, hardliners held the technical immutability of the blockchain to be of greater importance than recovering the drained funds, hence participants in The DAO ought to bear the loss. Their arguments resembled an oversimplification of the famous formula "Code is Law" coined by Lessing (Lessig, 2006). On the other side, the moderate position argued for rewriting the Ethereum blockchain to restore the funds lost to the exploit by erasing The DAO from existence. They were willing to forgo the much-heralded technical immutability of the blockchain for what they believed to be morally right, that is, recovering the stolen funds. Eventually, the moderate position won. The Ethereum network performed a hard-fork that erased The DAO from the Ethereum blockchain. It is worth noting that not all the users adopted the update, and another version of Ethereum was born (Ethereum classic, ETC). ETC is still being supported, and it ranks 22nd in market capitalization among all cryptocurrencies. It is also worth noting that recently ETC suffered a 51% attack that, however, seems not to have hindered its support[30].

[30] https://www.coindesk.com/ethereum-classic-price-stumbles-amid-suspected-51-attack accessed on 5th of September 2019

The aforementioned examples show some of the problems related to the peculiar governance structures of blockchain systems. If one is to believe some of the claims regarding this class of technologies one ought to be skeptical about it. In section 4, this chapter aims to provide an explanation that could account for some of the problems described earlier and which sets the stage for the rest of this dissertation. However, before examining the missing piece of blockchain governance one ought to delve into the available literature on the topic in order to assess possible solutions or mitigation strategies. Accordingly, the next section examines the literature on the governance of blockchains.

4.3 Literature Review

The academic discourse around blockchain governance is still developing. Interestingly, many contributions critically evaluate two aspects of the governance issue. On the one hand, a strand of the literature focuses on the pitfalls of the governance by/with blockchains (Atzori & Ulieru, 2017). On the other hand, another focuses on the governance of some well-known blockchain systems, namely, Bitcoin and Ethereum (Craig & Kachovec, 2019; De Filippi & Loveluck, 2016; Dodd, 2017; Hayes, 2019; Hsieh & Vergne, 2017; Jeong, 2013; Zachariadis, Hileman, & Scott, 2019). What seems to be lacking so far is an in-depth analysis of the third aspect of the governance scene from a general perspective, that is a general outlook on the governance of permissionless blockchains considered as a system of rules. Thus, this chapter aims to contribute by providing a general conceptualization of the issue of the governance of blockchains and distributed ledgers. A further clarification is in order, namely, an interesting part of the debate on blockchain governance is unfolding among prominent figures involved in the development of blockchain systems outside of academic circles. These 'grey' - yet important - sources will be included in the rest of this work where appropriate. On this basis, the following paragraphs outline relevant academic contributions on the governance of/by/with blockchains in chronological order.

Atzori describes some of the issues relative to the blockchain-based governance, which, within our model is analogous to the concepts of governance by/with blockchains. She considers blockchain-based governance as "the final stage of this process of decentralization and disempowerment of institutions" (Atzori, 2015, p. 15). After explaining some of the common assumptions related to the push toward blockchain-based governance she notes that "the regression of democracy to governance-by-computation or Decentralized Autonomous Organizations [...] would represent the ultimate triumph of Homo Economicus: an agent renowned for being 'autonomous, instrumentally rational, psychologically self-sufficient, 'under socialized' and motivated into action by the utilitarian principle of maximizing pleasure'. And with the bad reputation of 'anthropological monster'" (*ibidem,* p. 23). In her view, the triumph of blockchain-based governance, therefore, "would be the general disempowerment of individuals, the 'deification of the market and the triumph of antipolitics'" (*ibidem,* p. 25). She concludes her analysis of governance by and with blockchains by stating the "blockchain-based governance should be seen as an organizational theory - with significant technical and managerial advantages for markets, private services, communities - while it is not meant to be a stand-alone political theory. Likewise, blockchain technology and decentralized platforms are not hyper-political, but rather pre-political tools." (*ibidem*, p. 32). Arguably, her conclusions should be shared in so far as they highlight common pitfalls in the blockchain narrative. However, the claim that blockchain-based governance is purely organizational, seems to hinge on the assumption that such a governance arrangement is ontologically incomplete, and, therefore, pre-political. On the contrary, the next section argues that, while virtually all current examples of blockchains are incomplete, it would be conceptually possible to design and implement a complete, and hence, political version of blockchain governance. That said, it is not clear that a complete version of a distributed consensus systems would be effective due to the unspoken elements of rules, that is, a certain degree of social acceptance that is often presupposed.

De Filippi and Wright argue in their "Decentralized blockchain technology and the rise of lex cryptographia" that “the blockchain [sic] enables the development of new governance systems with more

democratic or participatory decision-making, and decentralized (autonomous) organizations that can operate over a network of computers without any human intervention" (Wright & De Filippi, 2015, p. 1). Moreover, they argue that "[b]y facilitating coordination and trust, a blockchain enables new forms of collective action that have the potential to bypass existing governance failures" (*ibidem*, p.16). Along the same line, they further contend that "[b]lockchain-based applications present a genuine promise for new kinds of scalable innovations in governance and institutional design, where the ideals for a corruption free and effective social democracy may come true" (*ibidem*, p.36). Finally, they link blockchains and smart contracts to algorithmic governance by writing that "[a]s more of this data [data mined from big datasets] is used to inform the operation of smart contracts and decentralized (autonomous) organizations, algorithms and source code will soon start playing a significant role in our everyday life [...] we could witness the emergence of so-called algorithmic governance: a new normative system capable of regulating society more efficiently, reducing the cost of law enforcement and allowing for a more customized system of rules that is personalized to every citizen, and that is constantly revised based on their corresponding preferences and profiles." (*ibidem*, p. 41). Their understanding of blockchains is aspirational rather than realistic. While it would be desirable to achieve "individual freedoms and emancipation, democratic institutions, and creative expression" via blockchains it is not clear how automation of rules via computer code is conducive to such values. More precisely, the difficulty in describing important human values formally - and therefore the practical impossibility of building computer systems to provably achieve such values - is more a feature than a bug. Moreover, they fail to outline that all the purported 'good' applications of blockchains hinge critically on their completeness as a system of rules. That is, 'good' blockchains are possible only in so far as the governance of the software develops according to sound principles, yet this is hardly the case in the current state of affairs.

Abramowicz 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" (Abramowicz, 2016, p. 368). Moreover, he correctly notes that Bitcoin uses P2P governance for transactions and not for changes to the rules themselves. While this solution is a worthwhile experiment in governance structures, it logically rests on a pre-existing set of rules. Thus, it is fair to observe that Abramowicz's solution - based on private ordering - is an example of governance with blockchains but does not address the governance of the blockchain. The limitation of Abramowicz's position has been expressed as the 'blockchain paradox' by Vili Lehdonvirta.

Lehdonvirta argues that thinking about the governance by/with blockchains turns out to be a naïve understanding of the technology since the real issue lies in who sets the rules that the network enforces. That is the governance of blockchains in the current classification. Therefore, blockchain technologies cannot escape the problem of governance by code; in his own words "you can't engineer away governance as such", this is the blockchain paradox (Lehdonvirta, 2016). The next section aims to provide an exhaustive explanation of this phenomenon.

Davidson et al. argue that "blockchain distributed ledger technology is a rare and special general purpose technology because it adds a further category to the suite of Williamson's 'economic institutions of capitalism' - namely, markets, hierarchies and relational contracting" (Davidson et al., 2016, p. 20). Again, it is possible to note the aspirational character of this contribution as it focuses on what could be possibly achieved with blockchains. In other words, these authors focus on the perspective governance by/with blockchains without addressing the problem of the governance of blockchains. Most importantly, markets, hierarchies and relational contracting often operate within the boundaries of the law, while blockchains aim to exist parallel to it.

De Filippi and Loveluck examine the governance of the Bitcoin system and find a highly technocratic power structure (De Filippi & Loveluck, 2016). They entertain the opportunity to establish a body similar to ICANN and then 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 the very purpose of the Bitcoin network" (*ibidem.* p. 19). These authors rightly focus on the issue of the governance of Bitcoin, but their centralized solution seems unfit for the Bitcoin system, additionally, they do not generalize their study to move beyond a single blockchain system.

Hacker, instead, applies complexity theory to blockchains and suggest an institutional approach based on a comply or explain mechanism drawn from the field of corporate governance (Hacker, 2017). He argues for 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" (*ibidem,* p. 35). Interestingly, Hacker focuses on the issue of the governance of blockchains and provides a solution drawn from the experience of internet governance, while this is a welcome contribution to the problem, he does not address the issue of the incompleteness of blockchains. Additionally, it seems fair to note that ICAAN arose from the implementation of a centralized layer (the DNS system) on top of the internet's distributed architecture (TCP/IP). On the contrary, blockchains do not (yet) operate under a centralized layer such as the DNS. Thus, the comparison of blockchains and the internet may be unwarranted, thereby undermining the proposal to 'port' internet governance structures to blockchains and distributed ledgers.

Hutten explores the discrepancies between the ideal governance of blockchains and the factual reality by focusing on the Ethereum platform and, more specifically on The DAO case examined in the previous section. He concludes that "[p]re-crisis commitments to strict governance by algorithms and the credo that 'code is law' failed to hold up under pressure" (Hütten, 2018, p. 15). Moreover, he correctly notes that "the public blockchain was all too human at its core, forming indeed the soft spot of a utopia of governance by hard code. The response to the crisis revealed that the public Ethereum blockchain has not transcended politics. The lack of proper procedures instead leads to a mimicry of the murky interventions that sparked discontent with the financial system." (*ibidem*). Hutten pinpoints the core

problem of the governance of blockchains, that is, the lack of proper procedure, which will be discussed at length in the next section.

More recently, Reijers et al. conceptualize the issue of the governance of blockchains from a legal philosophy perspective, namely borrowing on Kelsen's positivist account of legal systems and Schmitt's critique[31] of that conception (Reijers et al., 2018). These authors relate this opposition to the dichotomy between on-chain and off-chain governance solutions, that said, the next section makes clear that purely relying on on-chain mechanism is necessarily incomplete, and thus undesirable. More precisely, a complete system of rules cannot be grounded in the code for governance of a rule system is only complete in so far as it is general enough as to account for unknown unknowns, and able to persist due to the underlying social acceptance. These authors conclude by saying that "extant blockchain governance regimes need to be carefully reconsidered and aligned with the ideology of their relevant communities" (*ibidem,* p. 10) the relevance of this design goal for blockchains and distributed ledgers, more precisely, crypto communities ought to recognize the values on which their systems are built so that off-chain principles could drive the establishment of sound governance structures.

This section provided a selected sample of academic contribution to the issue of the governance of blockchains. In conclusion, it seems possible to argue that most of the academic literature focuses on the distinction between on-chain and off-chain governance structures with a focus on Bitcoin. On the contrary, the next section aims to construct a broader account of the governance of blockchains as systems of rules. It will be argued that on-chain governance is ontologically incomplete due to the inherent characteristics of the scope of governance and that blockchains ought to draw salient insight from legal philosophers. Blockchains, like any other system of rules are understood under a background of social circumstances that cannot be fully stated and therefore are impossible to implement into code.

[31] For an interpretation of the debate see (Přibáň, 2011)

4.4 The Incompleteness of Distributed Consensus Systems

Before attempting to describe and suggest what is the missing piece in the puzzle of the governance of blockchains a methodological clarification is in order. Crypto-enthusiast and developers do not rely on academic rigor to ground their arguments, this is especially true when it comes to legally relevant concepts and constructs. Therefore, the next paragraphs depict a picture of the current governance debate also inspired from grey sources and social media posts. That said, the rest of the section aims to re-establish methodological rigor in attempting to describe and conceptualize the missing piece of the governance of blockchains.

Among the circle of blockchain technologist and developers, two positions have gained prominence in the narrative around the governance of blockchains. On the one side, one finds what can be described as Szabo's law on blockchain governance. Szabo's law inherits its name from the cryptographer and amateur lawyer Nick Szabo, who - in 1994 - proposed the concept of 'smart contracts'. Szabo's conception of the law is questionable. On the issue of governance Szabo's position is that changes to the protocol ought not to be implemented unless the changes are required for the purpose of technical maintenance. It is possible to summarize this position as non-intervention (CleanApp, 2018a).

On the other side, one finds Vlad Zamfir's view on blockchain governance (Zamfir, 2017, 2018a, 2018b, 2019). Zamfir is a former scientist at the Ethereum foundation working on the Casper upgrade on the Ethereum system. Recently, Zamfir moved to work with a new start-up CasperLabs perhaps due to philosophical clashes within the Ethereum foundation. Simply put, Zamfir identifies three 'laws' that govern blockchain protocols in case of governance disputes. The first law is quite simple and straightforward: 'Don't Break the Protocol'. Simply put, this principle rather than legal provision requires that solutions to governance disputes ought not to be resolved by the introduction of known critical bugs into the blockchain protocol. The second principle is also quite simple from a conceptual perspective, according to the second principle blockchains should remain [*recte*, become] legal. Zamfir notes that

blockchains are structured by existing legal systems because they operate in pre-existing jurisdictions, which - coincidentally - explains why most of the legal entities that manage open blockchain systems are established in Switzerland. The third and last principle of blockchains governance according to Zamfir is Szabo's law. By contradiction, Zamfir argues that the third principle - Szabo's law - goes against the second principles, and, therefore is untenable and should be amended. In light of the previous conceptualization, Zamfir concludes that "we [the blockchain community] have an obligation to manage the disputes that will arise from the operation of global public blockchains to the best of our crypto legal ability, so that as many people as possible can enjoy the benefits of global public blockchains" (Zamfir, 2019).

In one sense, both sides define the variables and then compute their arguments, unfortunately, blockchains do not exist in a vacuum, nor legal systems developed in one. Hence, one needs to set aside the crypto governance debate in order to show that both sides seem to miss an important point. Blockchains are not a complete system of rules, thus debates on the content of their governance ought to start by acknowledging that. More precisely, blockchains are systems of primary rules that lack secondary rules, hence their incompleteness. The introduction of the notion of primary and secondary rules deserves some clarification.

While H. L. A. Hart introduced the distinctions between primary and secondary rules of law in the ’60, this chapter draws on the conceptualization done by Pagallo (Hart & Green, 2012; Pagallo, 2016, 2017a, 2017b). According to Pagallo’s perspective, primary rules of law aim to govern social and individual behavior, while secondary rules of law dictate recognition, adjudication, and change. In other words, when regulatees - which can be considered the stakeholders in a blockchain system - are required (or allowed) to do or abstain (or denied) from certain action one deals with primary rules. On the contrary, secondary rules provide regulatees with the ability - by doing or saying certain things - to introduce, extinguish or modify primary rules, or determine their incidence or control their operations. The three different types of secondary rules can be conceptualized as follows.

Rules of recognition are a remedy for uncertainty. In modern legal systems, rules of recognition identify primary rules by some of their general attributes, as - for example - having been enacted by a specific body, by customary practice, or by their relation to judicial decisions (Hart & Green, 2012). Rules of adjudication, on the other hand, allow individuals to establish whether on a given occasion a primary rule has been broken. In modern legal systems, rules of adjudication often identify the individuals or institutions who are to adjudicate and the procedures according to which the adjudication process ought to follow. Lastly, 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, i.e., that which counts as valid law within that system" (Pagallo, 2017a, p. 42).

Additionally, secondary rules include meta-rules of procedural regularity to ascertain whether a decisional process conforms to a given value (Barnett, 2003). The existence of explicit secondary rules is essential for the completeness of a system of rules, because, without secondary rules, there would be no grounds upon which one could recognize primary rules both in terms of legitimacy and procedural regularity. Were this the case, regulatees within a rule system with no secondary rules would have no basis to determine, change and adjudicate the plethora of rules that direct their behavior. In the legal domain, secondary rules are found in several bodies of law ranging from constitutions to specific regulations as in, for example, the GDPR. Examples of secondary rule within the GDPR are the procedures that supervisory authorities should follow pursuant to art. 36 or 83 of the GDPR.

Arguably, secondary rules achieve critical functions in legal systems. On the one hand, secondary rules determine the balance between different values and goals of legal systems. For example, within the GDPR secondary rules provide the balance between concurrent regulatory systems, coordination, risks of breaking down, and the protection of multiple legal rights. On the other hand, secondary rules also provide the resilience and integrity of legal systems by ensuring their ability to cope with change and to

evolve according to the demands of society. Lastly, secondary rules - arguably - enable legal systems to reach specific goals such as the separation of powers and procedural regularity.

Given the characteristics of secondary rules of law one can argue that they perform critical functions which lie at the core of the broad notion of the governance of legal systems (Pagallo et al., 2019). This section, therefore, argues that blockchains are incomplete because they lack secondary rules to determine their primary ones. Yet, blockchains are not legal systems, hence one might be skeptical in applying the concept of secondary rules in this case. Granted the previous objection, it does not follow that one has to accept the ontological equivalence of blockchains and legal systems - peace code as/is law. The stance of this chapter implies neither that blockchain are as legal systems nor that they are an isolated example of an extra-legal system of rules. Instead, one can contend that the distinction between primary and secondary rules of law sheds light on the issues of the governance of blockchains and distributed ledgers. More in depth, it seems fair to argue that, without secondary rules, blockchains cannot escape the blockchain governance paradox, remain pre-political tools, violate Zamfir's second principle and, which is more salient, fail to deliver on the promising of fostering a more equal and fair mechanism for co-ordination.

Therefore, this section can now look back at the informal governance debate between Szabo and Zamfir in a new light. In particular, the notion of secondary rules enables one to quickly dismiss Szabo's non-interventionist stance. In fact, the act of deciding whether a protocol needs maintenance hinges on a secondary rule - or more - of adjudication. More precisely, a malfunction at the level of the protocol is - arguably - analogous to a rule of adjudication because it entails a determination on the violation of a primary rule. Thus, it seems fair to contend that Szabo's law for blockchain governance is untenable. However, what about Zamfir's first and second law of blockchains governance?

It seems fair to argue that both principles can be properly enacted at the level of secondary rules. In particular, the first principle entails a secondary rule of adjudication in case of a dispute regarding - but not necessarily limited to - blockchain governance. Additionally, the second principle - namely to keep

blockchains legal - could also be implemented at the level of secondary rules. Think, for example, of a rule of recognition which dictates that legal decision ought to be implemented at the chain level. It seems possible to contend that such a mechanism could help to achieve the objective and "keep crypto legal" (Zamfir, 2019). One last remark on the conceptualization of the governance of blockchains made by Zamfir. It is important to note that Zamfir elaborates his thoughts on cryptolaw with the understanding that "legal systems are protocols for the management of disputes" (*ibidem*). While this conceptualization of law has little following in the philosophy of law it is adopted for it helps Zamfir to build his argument against Szabo. However, this section argued in favor of a different conceptualization of blockchain governance which is grounded on the distinction of primary and secondary rules and that, it is argued, is better suited to delineate the contour of the governance problem.

It is also important to note that secondary rules do not restrict the ability of blockchains to experiment with new governance models nor they shield them from governance failures. Yet, secondary rules would establish how the governance of blockchains is supposed to unfold, thereby reducing uncertainty. In particular, secondary rules are compatible - in principle - with any system of governance, hence blockchains would still be free to establish cutting-edge modes of governance such as blind coordination games, radical markets, futarchy, liberal radicalism, or - even - direct democracy (Buterin, Hitzig, & Weyl, 2018; Hanson, 2003; Posner & Weyl, 2018).

In conclusion, it seems fair to argue that the crux of the governance problems of blockchains lies in their incompleteness as a system of rules due to the absence of rules of recognition, adjudication or change. Therefore, one may argue that if blockchains implement rules of recognition, adjudication, and change would become complete systems of rules capable of solving the governance problems as exemplified in section 4.2. Additionally, another benefit arises. Arguably, complete blockchains would prevent hard-forks that stem from ex-post solution to unforeseen events by improving legitimacy, involvement, and accessibility to key decision processes (A. Zamyatin, 2018; Kim & Zetlin-Jones,

2019). This entails that agents could evaluate blockchains based on both their on-chain (primary) and off-chain (secondary) rules before committing resources to a given protocol.

4.5 Conclusion

This chapter examined the issue of the governance of blockchains, the main conclusion is that, if one regards blockchains as systems or rules, blockchains and similar solutions are incomplete. Most importantly, they are - generally - systems of solely primary rules. Hence, the argument of adopting blockchains and distributed ledgers based on their ability to unlock new avenues of cooperation falls short. As with the case of trustlessness, we must find another reason to explain why blockchains and distributed ledgers are being used in their current state.

As some have argued, if one considers blockchains as a new mechanism for coordinating human activities one can also regard blockchains as quasi-constitutional orders. Berg et al. discuss that, once one starts to see blockchains as possessing constitutional properties enabling heterogeneous users to compete and collaborate for mutual benefits (A. Berg, Berg, & Novak, 2018; C. Berg, Davidson, & Potts, 2018a, 2018b), then it becomes apparent the relevance of the current moment in the development of blockchains. More precisely, they argue that "[t]he emergence of blockchain rules [...] reflects a participatory process wherein users of this technology are seeking to achieve (net) benefits, not only in an institutionally comparative sense against mainstream hierarchical methods of data recognition and storage. The 'constitutional catallaxy' of the blockchain [sic!] is unfolding to improve internal coordination and governance practices within this ecological techno-system" (Berg & Novak, 2018, p. 2).

The previous comparison allows us to transition to the second part of this work. In exploring the main research question, it has been argued that neither the effects on trust or governance appear to justify the adoption and advocacy of blockchains and distributed ledgers. On this basis, I venture in making the

following claim. Distributed consensus systems are perceived as the desirable way to perform a function. If this is true, then one might explore on which basis these systems are regarded as desirable, or, which is equivalent for the purpose of this argument, legitimate. Accordingly, in the following chapters, it will be assumed that blockchains and similar systems are being used because they are perceived as a legitimate tool to achieve a given objective. This allows us to investigate the plethora of motives put forward by proponent of these technologies. The next chapter begins the investigation on the elements behind the perceived legitimacy of blockchains and distributed ledgers by delimiting the understanding of legitimacy to the sociological level. Additionally, it adds other arguments to support this line of investigation.

5. Perspectives on The Legitimacy of Systems of Rules

The present chapter deals with the justification of the study of the legitimacy of distributed consensus systems. To do so, it explains why the viewpoint of legitimacy appears to unlock useful insights in the context of blockchains and distributed ledgers, then it examines the notion of legitimacy from three perspectives. First, the normative account of legitimacy typical of philosophical studies, then, the one from the perspective of the law will be presented. Later, this chapter will focus on the descriptive account of legitimacy from the sociological perspective. In other words, three LoA will

be adopted to define the concept of legitimacy. The third LoA, namely, the descriptive account of legitimacy will then be adopted for the rest of this work in order to explain blockchains' relevance as systems of rules and attempt to account for their adoption. This chapter provides the theoretical foundation for the rest of this work, in which the descriptive account of legitimacy will be adopted to describe current systems (chapter 6) and, later, to theorize the beliefs that appear to cultivate the legitimacy of blockchains more generally (chapter 7).

Different LoA are informed by different disciplines. Following the teaching of Galloway, it is my hope that the reader can tolerate some degree of discipline-hopping for a broader, clearer, analysis of the phenomena at hand (Galloway, 2004). Accordingly, the vast literature on the concept of legitimacy has been reduced for reasons of space and conciseness. The concept of legitimacy from the normative perspective (LoA(1) is informed by normative accounts of legitimacy proper of political philosophy (Raz, 2001). LoA(2), instead, examines the notion of legitimacy from the perspective of the law, i.e., when legal acts norms are understood as valid (Hart & Green, 2012; Kelsen, 1967; Pagallo, 2017a). Lastly, LoA(3) takes the sociological perspective and outlines a descriptive account of the notion of legitimacy that originated form the work of Max Weber (Bensman, 1979; Greene, 2017; M. Weber, 1978). Before exploring these different accounts of legitimacy, it is necessary to explore why legitimacy appears to offer fertile ground to study blockchains. Therefore, the first section of this chapter aims to elucidate the benefits and insights unlocked by looking at this class of technologies through the lens of legitimacy. Accordingly, the present chapter develops as follows. After having defended the choice of examining blockchain from the viewpoint of legitimacy, it unravels distinct accounts of the essentially contested notion of legitimacy. To do so, section 5.2 analyzes legitimacy from the normative perspective. Then, the following one (section 5.3) describes legitimacy form the viewpoint of the law, while section 5.4 examines the descriptive notion of legitimacy. Then, section 5.5 defends the choice of examining

blockchains and distributed ledgers through the lens of the sociological understanding of legitimacy, rather than the philosophical or legal one.

5.1 Looking at blockchains from the perspective of legitimacy

Blockchain systems offer fertile ground to explore the interplay of social and technical artifacts from the perspective of legitimacy (Dodd, 2017; Hayes, 2019; B. Weber, 2014). Regardless of the specific understanding of legitimacy adopted it appears that blockchains are an interesting case to explore via the notion(s) of legitimacy. There are several reasons for it.

It is a truism that the interest in the technology of distributed ledgers has increased since the invention of Bitcoin in 2008 (Casino et al., 2018). Beyond online payments, blockchains have been portrayed as "Lego mind-storm to build socio-economic institutions"(Buterin, 2014). Moreover, some authors have argued for an upcoming 'blockchain revolution' capable of disrupting the whole economy (Swan, 2015; Tapscott & Tapscott, 2016). These authors, along with other who hold a more moderate position on the impact of blockchains, assume that blockchains have desired properties that should push groups of people to adopt some version of them (Iansiti & Lakhani, 2017). The underlying assumption appears to be that blockchains and distributed ledgers alike constitute a better way to pursue goals such as coordination, enforcement of contracts, management of information, and recordation of titles to cite a few avenues in which these systems have been proposed (Conte de Leon et al., 2017).

Another important assumption in the advocacy for the adoption of blockchains seems to be that these systems are legitimate. It is possible to leave aside for a moment a precise definition of legitimacy and work with the assumption that, for example, Bitcoin is a legitimate mechanism to transfer value

online, according to the various declination of the term found in its common definition. This is not to say that some people would not object to the legitimacy of Bitcoin because, for example, it is perceived as enabler of terrorist financing (DuPont, 2018; Weaver, 2018). However, to the extent that we are dealing with blockchains and distributed ledgers, the recent push to deploy it across many sectors appears to grant the statement that these technologies are perceived as legitimate, or, to the least, that they could be (Hanson RT., 2017). Then, considering blockchains as legitimate supports their adoption. This is the last argument to deploy these technologies under scrutiny. After having examined the arguments based on the trustlessness and the new mode of governance, the belief that blockchains and distributed ledgers are legitimate appears to be inform the engagement of this class of technologies.

It is also relevant to note how, as noted in closing the previous chapter, some compared blockchains to constitutional orders, so that studying blockchains from the perspective of legitimacy appears desirable if the comparison, as it seems to be, deserves merit (A. Berg et al., 2018; C. Berg et al., 2018a, 2018b; Rajagopalan, 2018). Berg et al. argue that "blockchains are constitutional orders – rule-systems in which individuals (or firms, or algorithms) can make economic and political exchanges, and so offer a unique economic environment for institutional discovery and experimentation." (C. Berg et al., 2018a). In this sense, the study of the issue of legitimacy might prove insightful to understand how blockchains experiment with new rules to enable economic and political exchanges. Much in the same way as a fertile avenue for research has been the legitimacy of current constitutions (Fallon Jr, 2004). The fact that some blockchain systems have developed constitutions themselves, such as EOSIO and Decred, supports the study of such systems through the lens of legitimacy.

Another point of contact of the study of distributed consensus systems and legitimacy has been put forward by Reijers et al. (Reijers, O'Brolcháin, & Haynes, 2016; Reijers et al., 2018). They studied how blockchain communities use social contract theories as a method for justifying their political

principles, i.e. the legitimacy of blockchains. They argued that "some essential aspects of the justification for blockchain governance show significant similarities with justifications offered by social contract theories." (Reijers, O'Brolcháin, & Haynes, 2016, p. 139) These similarities can be found in the justification of the use of blockchains against the ideal of an initial "pre-blockchain" society, or in the way in which the technology itself acts as a "veil of ignorance" because it is unable to discriminate or to have a goal of its own, in contrast to conventional institutions. It seems fair to argue that the justification of blockchain governance tied with the push toward their deployment should be complemented by the studies of the different structures, both social and technical, that have been developed across many blockchains' communities. To do so, studying the legitimacy of blockchains appears to offer the best viewpoint. However, as section 5.4 will explain this work departs from the perspective of moral philosophy, in favor of a descriptive account of legitimacy.

Similarly, Scott's argument that any blockchain can be seen as a technological Leviathan – i.e. techno-leviathan – further hints at the opportunity to study blockchains' legitimacy (Scott, 2015). He writes, "trustless blockchains floating above human affairs contain the spectre of *rule by algorithms"* to argue that blockchains can be considered as technological sovereign whose rule people can contract to. Then, he continues, "[t]hese rules are a series of algorithms: they represent step-by-step procedures for calculations that can only be overridden with great difficulty. Perhaps, at the outset this represents, à la Rousseau, the *general will* of those who take part in the contractual network, but the key point is that if you become locked into a contract on that system, there is *no breaking out of it".* (*ibidem*, p. 4). Again, it is possible to see a reference to social contract theories when dealing with the subject of blockchains. Simply put, *rule by algorithms* requires justification, or, which is equivalent, legitimacy within the group in which it is implemented. Hence, Scott provides a similar reason to study the legitimacy of blockchains to the one previously mentioned.

Beyond theoretical reasons as to why the study of legitimacy of blockchains appears desirable, there are empirical ones as well. In a sense, blockchains represent a third wave of libertarian attempts to

self-organize around technology. The first one traces back to the birth of the internet with the P2P movement as represented by the cyberspace manifesto (Barlow, 1996). The second one arose around utopian assumptions of early internet boosters with the creation of online virtual words such as Second Life and World of Warcraft (McKnight, 2012). In this latter case democratic arrangements are the exception rather than the norm. In fact, managerialism is the norm as showed by ethnographic research carried out on the topic, given the choice "people almost without exception reject self-governance in favor of professional management in their voluntary associations online" (*ibidem*, p. 373). This clear rejection of democracy in virtual worlds might be explained by the fact that virtual communities lack sufficient legitimacy to engage their users. Then, studying how blockchains attempt to establish their legitimacy as online rule-systems to coordinate social and economic activities might shed light on the trend toward managerialism. So far, blockchains appear to be on the same trajectory of other virtual communities, then, improving their legitimacy might offer a way out of benevolent dictatorships or managerialism. This is essential for these systems to have a significant impact on society.

However, blockchains are crucially different from previous attempts to self-organize with technology. This is because blockchains are for real. While real-world effects of other virtual endeavors are possible to identify blockchains have established themselves as alternative mechanisms to organize with respect to traditional institutions. Bitcoins or DAOs are not designed to be entertaining, rather, they are design and implemented as a way to offer individuals an alternative road, i.e. the short one proper of P2P systems in several other areas (Pagallo & Durante, 2009). Accordingly, the study of their legitimacy ought to be carried out with methodological tools and notions developed for the study of the legitimacy of traditional institutions against which blockchains are often compared (Frantz & Nowostawski, 2016; Ishmaev, 2017; Vaz & Brown, 2018). Furthermore, there are some crucial characteristics of blockchains that make them interesting from the perspective of legitimacy.

These characteristics are cryptocurrencies, and forks. On the one hand, it seems fair to argue that cryptocurrencies add for the first time a significant degree of freedom to self-organizing communities, that is, a medium of exchange with a non-trivial value. Moreover, cryptocurrencies add a significant metric for the evaluation of the legitimacy of blockchains, for it may be argued that the value of any given cryptocurrency is a proxy for the popularity of a given blockchain project, which might arguably be an indicator of the project's legitimacy. Then, it is likely that, among the more than 3000 cryptocurrencies available, those with the higher market capitalizations are perceived as more legitimate than others.

On the other hand, forks provide a measure of the legitimacy within crypto communities. When a blockchain system splits in two incompatible ones, as is the case with hard-forks, and both resulting systems have a significant following, one might think of hard-forks as case of disobedience. In other words, if a system splits it is likely because a significant part of the community did not recognize the authority of that system, hence the need for the creation of a parallel one, usually with minor differences from the original. This is the case as with the multiple hard-forks of Bitcoin. To recall a prominent example, BitcoinCash split form Bitcoin because of the disagreement regarding the block-size of the Bitcoin blockchains (8mb vs 1mb), the rest of the system stayed mostly the same. Additionally, hard-forks might manifest either as a consequence of a contentious decision (as in The DAO case within Ethereum) or as the result of the characteristic of a system. The latter is the case of the recent implementation of the technology so-called *mimblewinble*[32] initially proposed as an upgrade for Bitcoin. This might suggest that the decision process of Bitcoin is perceived as ill-equipped to allow for new solutions to be implemented on the network.

[32] Mimblewinble is a privacy focused modification to the reference transaction structure of Bitcoin. https://download.wpsoftware.net/bitcoin/wizardry/mimblewimble.txt accessed on 28th of October 2019.

Therefore, hard-forks could offer a proxy to evaluate the legitimacy of a blockchain systems under the assumption that if a system fails to preserve its unity then it lacks legitimacy, and therefore, obedience to the rules of that system. On this basis, hard-forking a blockchain has been referred to as vote-with-your-cpu to reference the digital equivalent of the mechanism of voting with one's feet in case of disagreement with an analog rule-system bounded by geographical borders. Moreover, since the cost of forking appears significantly less than its analog counterpart it is possible to argue that blockchain systems must maintain a significantly higher degree of obedience. This is also due to the fact that the authority of blockchains is not absolute and does not have access to coercion. To put it differently, the authority of blockchains based on the belief in their legitimacy by their users is of paramount importance to maintain the cohesion of each systems and prevent fragmentation. And, due to prominent network effects among blockchains the goal of preventing hard-forks is vital. Then, the study of the legitimacy of blockchains appears to provide useful insights to preserve the integrity of systems by understanding what, in the first instance, keeps them together and on which basis users contract to the rule by/with algorithms of blockchains.

The last reason for studying the legitimacy of blockchains is that it could provide useful insights for designing other rule-systems. This is because once it is understood why groups of people grant obedience to blockchains and on which basis, then it would be possible to adapt the ideas on which the legitimacy of blockchains rests to other rule-system. Such adaption would prove beneficial if, as it seems, blockchains appear to establish their legitimacy on a belief based on the authority of algorithms. If States and other established institutions aim to deploy blockchains of their own, understanding the basis on which blockchains are being adopted by groups of people is essential because it is unclear that reasons of efficiency unbounded by ideological elements fully explain the rise of blockchains. Recent initiatives both at the national level, as in the case of Sweden, or international one with the European Blockchains Service Initiative should benefit from a deeper understanding of the legitimacy of existing blockchains. On this basis, the current chapter deals with

distinct notions of legitimacy informed by three levels of abstraction. The following sections aim to elucidate, albeit briefly, different conceptions of legitimacy before selecting one for the rest of this work.

5.2 Normative Legitimacy

At the level of abstraction of political philosophy legitimacy is a normative concept. According to this perspective, a system of rules like a state is legitimate if it is morally acceptable. Political legitimacy was developed to justify liberal democracy by the likes of Rawls and Habermas from the moral perspective (Greene, 2017). These accounts of legitimacy were developed to understand the concept as the basis upon which the coercive force is exerted on citizens by States. Philosophers generally consider legitimacy as a benchmark of acceptability or desirability of authority or political power, sometimes even in terms of an obligation. This section briefly describes the main theories of legitimacy at the level of abstraction of political philosophy to distinguish this notion from the others that will be recalled in the following sections. For reasons of brevity, the centuries-long debate has been simplified.

A prominent view of legitimacy at the current level of abstraction is grounded on consent. Simply put, citizens consent to be the subjects of coercive force. This view gave birth to the well-known political theory based on consent captured by the 'fiction' of the social contract between the state and its citizens. Social contract theories might diverge on the circumstance that gave birth to the 'contract', see – for example – the different account of the state of nature put forward by Hobbes and Rousseau; however, in these theories consent of the governed is of paramount importance to grant legitimacy for the use of force by the state. It is fair to say that justifications of political legitimacy

based on consent are out of fashion. This is mostly due to the fact that strong arguments against consent have been put forward.

Barnett and Dworkin note how nowadays no one has actually given consent to the be subject to the coercive power of the state established, for example, in a constitution (Barnett, 2003; Dworkin, 1986). Dworkin, for example wrote that “even if the consent were genuine, the argument would fail as an argument for legitimacy, because a person leaves one sovereign only to join another; he has no choice to be free from sovereigns altogether” (Dworkin, 1986, p. 192).

Another strong argument against social contract theories is empirical. In fact, David Hume recognized that consent is not feasible for the simple reason that in the real-world modern states always have arisen from violent acts rather than peaceful deliberations. Even if that were not the case, one is likely to concede that the notion of consent would be treated differently if every citizen were a party to an actual agreement to obey political decisions in a given way.

A different view of political legitimacy grounds its claims on utilitarianism. Bentham, for example, stipulates that the legitimacy of a system of authority depends on whether its laws contribute to the happiness of the citizens (Bentham, 1996). As with other arguments grounded on utilitarian principles, it may be argued that the utilitarian view of legitimacy will convince only those who benefit from it and not those who stand to lose. In defense of that objection stands Raz's conception of legitimate authority as stated in his normal justification thesis (Hershovitz, 2003; Raz, 2001).

Lastly, several theories attribute the source of legitimacy either to democratic participation or an idea of public reason. The latter view is represented by Rawls and his argument that political coercion is justified if it is based on reasons that all reasonable persons can share (Rawls, 2001). In his own words, "political power is legitimate only when it is exercised in accordance with a constitution (written or unwritten) the essentials of which all citizens, as reasonable and rational, can endorse in

the light of their common human reason" (*ibidem, p.* 41). It is rather evident how theories based on public reason are strongly influenced by the Kantian notion of rationality (Fabienne, 2010).

Another position grounds political legitimacy on the decision-making process. More precisely, such theories hold that a political decision as legitimate if it has been taken in a process that allows for equal participation of all relevant stakeholders. These accounts build on Rousseau's idea that (tacit) consent is not enough for establishing legitimacy, and that citizens' active participation is a necessary condition for political legitimacy. A prominent example of this view can be found in the work of Habermas. It appears that this account of legitimacy is not helpful when studying blockchains. Primarily, because these systems do not coerce individuals, nor they are absolute in terms of power and participation. Therefore, the next section considers a different level of abstraction, namely, the legal account of legitimacy.

5. 3 Legal Legitimacy

At the level of abstraction of the law, one finds that the notion of legitimacy is sometimes referred to as validity. In legal theory, the validity or legitimacy of a norm is an essentially contested concept. In fact, many different accounts of legal validity have been put forward (Casanovas, 2012; Michal Araszkiewicz, 2016; Pagallo, 2013; Sartor, 2008). It is useful to start with known sources of law to introduce the discourse on legitimacy at the current level of abstraction.

Under Italian law, we find both the concepts of validity and legitimacy. The former is found in the Italian Civil Code in, for example, art. 1325, which states that a contract is invalid if it lacks one of the essential requirements (parties, object, cause, and form if requested see section 2.4). Under Italian law a contract is invalid if it violates a legal norm. In this sense, validity is understood as the absence of violation of another legal norm. If a contract is invalid it can either be null or nullable depending on the norm it violates. The latter notion of legitimacy, instead, is used by the Italian legislator when dealing with matters of public law. Examples are the judgment of constitutional legitimacy (art. 134.1 of the Italian Constitution) or the artt. 21-octies, 21-novies of the Legge n. 241 del 1990. The notion of legitimacy is defined by the violation of constitutional norms in the first case, and violation of norms, incompetence or ultra vires in the second one within administrative law. Under Italian law, the concepts of validity and legitimacy have similar operational capacity as they both entail the violation of another legal – valid – norm. Hence, at the current level of abstraction it is possible to consider jointly the notions of validity and legitimacy.

As a legal concept, validity depends on legal norms, "that which is lawful is also legitimate" (Fallon (Fallon Jr, 2004, p. 1794). To put in other words, what is legal is also legitimate or, which is equivalent: "a valid norm is a legal norm. And, to acquire this quality of law, a rule or norm is expected to be (or become) valid" (Casanovas, 2012, p. 34). There is an apparent circularity in the notion of validity as explained by Luhmann: "[d]ecisions are legally valid only on the basis of normative rules because normative rules are valid only when implemented by decisions" (Luhmann, 1984, p. 6). This paradox is apparent in the conceptualization of secondary rules of law examined in the previous chapter. Since secondary rules can be defined as "meta-rules by which all other rules of the system are identified and understood as valid" (Pagallo, 2017 p. 36) it seems that every secondary rule should require another one to be understood as valid, else that secondary rule would not count as valid law within that system. The current circularity engages an infinite regress which is not tolerable. To resolve this conceptual paradox great legal theorist have proposed different solutions. Kelsen

conjectured the presence of a grundnorm, he posited that "the reason for the validity of a norm can only be the validity of another norm" (Kelsen, 1967, p. 194). The grundnorm is then the underlying 'basic norm' of a legal system from which all other norms are derived. It is important to note that the grundnorm is not an internal rule of a legal system but a basic presupposition outside of it.

Hart resolves the paradox of legal validity by resorting to the recognition rule. In Hart's account "the foundations of a legal system consist of the situation in which the majority of a social group habitually obey the orders backed by threats of the sovereign person or persons" (Hart & Green, 2012, p. 100). The rule of recognition is a social situation that, when accepted, provides private persons and officials with authoritative criteria for identifying primary rules. The rules of recognition in modern legal systems are complex: "the criteria for identifying the law are multiple and commonly include a written constitution, enactment by a legislature, and judicial precedents" (*ibidem*, p. 101). Schmitt criticizes positivistic accounts of validity via the notion of the state of exception. He argued that valid norms cannot be premised on existing legal norms but from "principally unlimited authority" (Schmitt, 2005, p. 12) that manifest itself during the state of exception.

There are other debates around the notion of legal validity as, for example, if it can be considered as a normative notion or a factual one (Bulygin, 1991). What is clear is that validity appears as an essentially contested concept in legal theory. From the perspective of this work it seems fair to conclude that the notion of legal legitimacy or validity does not allow us to study the reasons why blockchains and distributed ledgers are regarded as legitimate methods of co-ordination. Therefore, this chapter now turns to another conceptualization of legitimacy from the level of abstraction of sociology, for I believe that a descriptive account of legitimacy allows us to better describe the phenomena at hand and to comprehend its implications.

5.4 Sociological Legitimacy

The third level of abstraction describes legitimacy from the sociological perspective. From this perspective a given system of rules possesses legitimacy if its subjects regard it as appropriate, justified for reasons other than fear of sanction or personal reward or customs (Fallon Jr, 2004; Greene, 2017). At the current level of abstraction legitimacy is not a normative or legal concept, it is descriptive. It helps to unravel differences between system of rules by providing a methodological tool to examine social phenomena.

Legitimacy as a sociological notion in the descriptive sense originated from the work of Max Weber (M. Weber, 1978, 2012). From this perspective, legitimacy is not a binary concept as it is considered at the level of abstraction of the law, in which, legal acts are either valid or invalid, or a là Luhmann coded as legal or illegal (Luhmann, Kastner, & Schiff, 2004). Instead, legitimacy is a probability distribution that measures how likely people are to obey commands without the need to invoke punishments or rewards. Not every instance of obedience to commands is a consequence of legitimacy, loyalty may be simulated, material self-interest or customs might also account for the obedience. However, these considerations are not arguments against classifying different systems according to their legitimacy from the sociological perspective, because legitimacy is an empirical notion that can be adopted to explain factual phenomena, as the different architectures and types of distributed consensus systems. This is due to the fact that, according to the kind of legitimacy established, social structures and the means of its exercise vary. The same applies with regard to the legal structures developed within a given community.

Weber defines legitimacy as "the probability that certain specific commands (or all commands) from a given source will be obeyed by a given group of persons" (Weber, 2012, p. 324). In his work, legitimacy is a necessary condition for authority (*herrschaft*). The presence of legitimacy is what distinguishes power from authority. Then, legitimacy becomes a foundational notion to understand

social structures that do not resort to violence or rewards to influence the behavior of a group of persons. In his own words: "[legitimate] imperative co-ordination will thus mean the situation in which the manifested will (command) of the ruler or rulers is meant to influence the conduct of one or more other (the ruled) and actually does influence it in such a way that their conduct to a socially relevant degree occurs as if the ruled had made the content of the command the maxim of their conduct for its own sake. Looked upon from the other end, this situation will be called obedience." (Weber, 1978, p. 946) In this sense, legitimacy is "the basis of every system of authority [it] is a belief, a belief by virtue of which persons exercising authority are lent prestige." (Weber 2014, p. 382). Without legitimacy, the obedience could be only explained by the presence of physical threat, customs or self-interest from the ruled. As noted by Weber's most prominent translator, "a willingness to submit to an order imposed by one man or a small group, always implies a belief in the legitimate authority" (Weber 1978, p. 37). As is well known, Weber identified three type of legitimate domination, i.e. legitimate authority (Weber 2014, 1978). The elucidation of these pure types will be carried out in chapter 6 when different blockchain system will be examined according to Weber's methodology. For now it is sufficient to conclude this section by emphasizing how, at the third and final level of abstraction, legitimacy is a descriptive notion useful to discriminate among different systems of rules and which can be used to explore the different social and technical structures developed to exercise authority. The differences among the structures developed as a consequence of distinct sources of legitimacy are reflected in the normative operations of the systems, so that this perspective enables one to examine the legal underpinnings of blockchains and distributed ledgers.

5.5 Choosing the Appropriate Level of Abstraction

The previous sections outline three distinct notions of legitimacy at different levels of abstractions. To sum up, legitimacy from the perspective of moral philosophy seeks to understand when the exercise of power is morally justified. Legal legitimacy, or validity, conversely aims to distinguish valid legal acts from invalid legal acts according to the coding of legal/illegal. In this case legitimacy is a concept internal to legal systems. Lastly, legitimacy has been defined as a sociological concept that describes the basis on which a group of people obeys commands. At LoA(3) legitimacy is an empirical concept that helps to understand, descriptively, how system of rules are authoritative in the Weberian sense. In the current analysis of blockchains and distributed ledgers one perspective must be adopted going forward. I believe that, at the current stage of development of blockchain systems, the more appropriate level of abstraction is the sociological one. The reasons for adopting LoA(3) rather than LoA(1) or LoA(2) are the following.

First, chapter 3 and 4 have examined two core claims put forward to justify the adoption of blockchains so that it is a natural development attempting to understand how blockchains develop authority and on which basis current systems can be considered legitimate. Then, the sociological understanding of legitimacy appears to be best positioned with its empirical connotation to unravel how groups of individuals come to 'obey' these systems.

Along the same line, the sociological understanding of legitimacy allows one to deploy the methodological approach of Max Weber to examine different implementations. This is relevant for it appears that no such thing as the blockchain exists and that different systems seem to establish legitimacy on different grounds, and therefore develop distinct structures. The analysis of current blockchains with this methodology will be the subject of the next chapter.

Third, legitimacy at LoA(3) exposes an increasing trend in the reliance on algorithms to exert power, a phenomena which has been defined as algorithmic authority that appears to be best studied from the sociological perspective. In this sense, the normativity of blockchains might be illuminated under

a different light. By examining blockchains with the sociological understanding of legitimacy it is possible to outline an understudied belief in the authority of computations captured by the notion of algorithmic authority (see chapter 7).

Fourth, a descriptive account of the structures and designs of blockchains appears necessary before an inquiry at the level of moral legitimacy. It seems that the sociological account is a precursor to the philosophical one. Without a descriptive understanding of blockchain systems a moral examination might incur in the categorical mistake of treating a single implementation, for example Bitcoin, as representative of the whole landscape. And this is undesirable, in particular if policy recommendations would be drawn on the basis of an incomplete understanding of the different mechanisms and structures that different blockchain systems give birth to. Then the risk of over-regulating the technology would be considerably high.

Fifth, as with other system of rules the sociological understanding of legitimacy allows one to examine the different structures and ideas on which systems are grounded. Therefore, it is possible to discuss the varying institutions or technical solutions adopted by different blockchains without the complexity of examining them from the moral perspective. In this sense, the Weberian account of legitimacy appears best positioned to explain the reasons why different blockchains appear to establish their legitimacy on different grounds. Further, by examining the belief that are left out when analyzing blockchains according to Weber's pure types, it is possible to expose elements that do not belong to the classic pure types of legitimate authority (see chapter 7).

Sixth, to the extent of my knowledge, the study of blockchains with both their legal and technical structures has not been carried out from the perspective of legitimacy at LoA(3). Yet, I believe that this approach is conducive to a better understanding of the phenomena because it enables us to explore the underlying ideas that result in distinct technical solutions and in the understanding of the normative structures developed within blockchains and distributed ledgers. Then, once the core tenets

of the blockchain movement have been exposed it is possible to explain what drives the adoption of these systems and how existing ones could leverage it to improve their legitimacy.

Seventh and final, the sociological notion of legitimacy is apt to expose the motives that drive the adoption of different systems, both technical and social. Hence, this perspective helps us illuminate the way in which normative structures are understood within blockchains. In other words, self-executing smart contracts, management of digital tokens and so on are all manifestation of the ideas on which the authority of blockchains hinges. This chapter set the stage for the analysis of blockchains from the perspective of sociological legitimacy. It has examined three main understandings of the essentially contested notion of legitimacy by adopting three levels of abstraction, namely, philosophical, legal, and sociological. Then, it defended the choice of the sociological one to analyze blockchains and their many different technical and social solutions. On this basis, the next chapters will study blockchains from the viewpoint of legitimacy developed by Max Weber. Accordingly, the next chapter examines real-world system via the Weberian pure types of traditional, charismatic, and rational-legal legitimate authority. It turns out that, among the many blockchains out there, some resemble a pure type better than others and, consequently, their structures both at the technical level, that is, governance by/with the network, and the social level - governance of the network – differ significantly. This chapter ends the first part of this work in which I examined the reasons commonly put forward for adopting blockchains. In chapter 3 the claim that blockchains remove trust from interactions, i.e. the trustless attribute of the technology, has been examined as a primary reason. Then, chapter 4 looked at the new modes of governance brought about by this class of technologies. The current chapter, instead, argued that an overarching reason why people adopt blockchain is because they are perceived as legitimate mean to a wide set of ends. Introducing the concept of legitimacy demanded justification, therefore an early section of this chapter was devoted to explain why I believe that studying the legitimacy of blockchains is desirable. The next part of this work applies the sociological methodology provided by Max Weber to study different blockchains in an

attempt to establish why groups of people grant obedience to these systems of algorithmic rules. On this basis, the next chapter looks at existing systems through the three pure types of legitimate authority put forward by the German sociologist. This is a needed step toward understanding the core ideas on which the legitimacy of blockchains is established. It turns out that it is not clear if Weber's typology is sufficient to account for why people obey blockchains.

6. The Legitimacy of Distributed Consensus Systems for the Perspective of Max Weber

The subject of this chapter is the legitimacy of current blockchain systems from the sociological perspective. It studies the elements that ground the legitimacy of several systems in light of Max Weber's description. As mentioned in the previous chapter, blockchains and similar systems can be

conceptualized as system of rules that exert power so that the Weberian notion of *herrschaft*[33], defined as "the probability that a command with a given specific content will be obeyed by a given group of persons" (Weber, 2012, p. 152) can be adopted to study this technological innovation. In this sense, a distributed consensus architecture is a legitimate system of imperative co-ordination if stakeholders persist in participating in the network and do not fork it. That is, the commands in the context of blockchains and distributed ledgers are the instructions coded in the protocol of each systems along with its governance mechanisms. Hence, the next paragraphs describe the basis on which stakeholders believe in the legitimacy of prominent blockchains.

Like any other system of authority, blockchains do not voluntarily limit themselves but "appeal to material or affectual or ideal motives as a basis for guaranteeing [their] continuity" (*ibidem*, p. 325). Blockchains attempt to establish and cultivate what Weber describes as "belief in legitimacy" (*ibidem*). Different systems of imperative co-ordination ground their claim to legitimacy on distinct basis, so that, the structures developed to perpetuate them differ significantly. Generally, differences are reflected by the type of obedience, the administrative staff developed, the modes of exercising power, and the legal structures of each system. In the digital world of blockchains, these differences are also seen in the algorithms that make them tick. Accordingly, this chapter aims to describe the different ways in which blockchains cultivate their legitimacy as systems of *herrschaft* both at their social and technical levels.

Different beliefs in the legitimacy of blockchains and distributed ledgers give rise to distinct software arrangements. For expediency's sake, the next pages examine a specific part of the software stack of blockchains, namely, the consensus algorithm. Moreover, the analysis of consensus algorithms appears fitting to study how different beliefs in the legitimacy of blockchains are reflected in their

[33] The term has not a satisfactory English equivalent, the term imperative control is close to Weber's meaning. It has also been translated as 'domination', 'mastery', 'authority', or 'rule'. I will use it as imperative co-ordination because I think it applies better to blockchains seen as new solutions to the problem of co-ordination.

technical structure. This means that each blockchain system will be evaluated vis-à-vis on the mechanism that enables nodes to reach a consensus on the order, validity, and existence of transactions or computations, that is, state changes (Natoli, Yu, Gramoli, & Esteves-Verissimo, 2019; Sigrid Seibold, 2016).

The reason is twofold. First, a high degree of experimentation and development is ongoing at the level of the consensus algorithm, so that, of all the element of blockchains' software stack, the consensus algorithm is the one where one observes more variety. The same does not hold for other elements such as messaging protocols or scripting languages. Second, there are more than 60 different consensus algorithms either proposed or implemented in different distributed consensus systems that provide us with significant empirical evidence (Xiao, Zhang, Lou, & Hou, 2019). It is likely that different designs in the consensus algorithm are not justified purely in technical terms such as better throughput or lower computational load but reflect diverse beliefs in the legitimacy of each system.

The following sections consider different blockchains according to the Weberian methodology. Of course, no system perfectly fits a pure type, but each possesses elements belonging to different ones. The next sections explore how the classification of the German sociologist applies to existing blockchain systems. This chapter aims to assess which pure type of the Weberian classification better explains the authority exercised by/with different distributed consensus systems. In order to achieve this end, the next sections will provide an outline of each pure type and, then, examine one or more blockchain systems accordingly. The following analysis explores to what extent Weber's methodological apparatus enables us to describe and analyze blockchains as socio-technical systems of rules. Before moving to the next section, it must be noted that the merit of the choice of one system rather than another is justified by its usefulness.

This chapter is organized as follows. Section 6.1 describes the element of traditional authority and examines the Bitcoin system. Then, section 6.2 introduces the pure type of charismatic authority and

describes two other projects: Ethereum and Tron. Before concluding, section 6.3 analyzes the notion of rational-legal authority and studies Decred and EOS.

6.1 Traditional Authority

According to Weber's definition, a pure type of imperative co-ordination is traditional if legitimacy is claimed for it and believed on the basis of the sanctity of the order and the attendant powers of control as they have been handed down from the past, i.e., "have always existed" (Weber, 2012, p. 341). Chiefly, the exercise of authority is handed to persons designated according to traditionally transmitted rules. Another important aspect of this type of belief in legitimacy is that the bureaucratic staff does not have (a) specific competencies, (b) a relational ordering of superiority and inferiority (c) a regular system of selection and promotion based on the freedom of contract, (d) a technical training as a formal requirement and (e) fixed compensations (*ibidem*). Obedience is thus granted on two bases: first, in terms of traditions, second in terms of unbounded action by the chief and her administrative staff. Regarding norms, in these systems "it is impossible in the pure type of traditional authority for law or administrative rules to be deliberately created by legislation" (*ibidem*, p. 342). Other aspects relevant to our current analysis are that the opposition is not directed against the system as such and that donations are a prominent mechanism to support it. Lastly, Weber notes how the primary effect of traditional authority on economic activities is to strengthen traditional attitudes.

The next paragraphs highlight how Bitcoin resembles a system of traditional authority both at the social level (section 6.1.1) and the technical one (section 6.1.2). It is argued that the governance struggles of the Bitcoin network can be better understood once its *herrschaft* has been identified as

traditional. Moreover, these characteristics seem to support the argument that Bitcoin would always struggle to conform with systems of rational-legal authority as, for example, current legal systems. Therefore, Bitcoin - along with others- collides with existing systems of imperative co-ordination that are not purely based on tradition.

6.1.1 Bitcoin as a social system grounded on tradition

Many authors have studied the governance of Bitcoin from the perspective of the social structures involved in shaping it. What most have found is that behind libertarian ideals of equality, the social structure of Bitcoin resembles a technocracy rather than an egalitarian utopia (DuPont, 2014; Golumbia, 2016; Herian, 2018a). This section argues that the *herrschaft* of Bitcoin is based on tradition. That is, Bitcoin social and technical protocol (next section) are shaped by Bitcoin's own attempt to cultivate its traditional authority. Bitcoin's social structure is quite complex. This section focuses on specific actors within Bitcoin whose presence and characteristics appear to be readily explained by considering Bitcoin as a system that grounds its legitimacy on tradition. These actors are core maintainers, and miners; the next paragraphs examine each one in turn.

First, there are the five core maintainers of the Bitcoin core client. The lead maintainer, at the time of writing, is Mr. Wladimir J. van der Laan, who holds the PGP [34] key 71A3B16735405025D447E8F274810B012346C9A6 that allows him to have commit and merge powers on Bitcoin's GitHub repository. The other four 'horseman' of the Bitcoin core client are:

1. Pieter Wuille (PGP key 133EAC179436F14A5CF1B794860FEB804E669320);

[34] PGP stands for pretty good privacy which is an encryption protocol used to authenticate for data communication.

2. Jonas Schnelli (PGP key 32EE5C4C3FA15CCADB46ABE529D4BCB6416F53EC);
3. Marco Falke (PGP key B8B3F1C0E58C15DB6A81D30C3648A882F4316B9B);
4. Samuel Dobson (PGP key CA03882CB1FC067B5D3ACFE4D300116E1C875A3D).

These five individuals have commit access to the Bitcoin core repository. The lead developer, Mr. W.J. van der Laan has been appointed by the previous one, Mr. Gavin Andresen who, in turn, had been nominated by the creator of Bitcoin, Satoshi Nakamoto, in a chain of appointments that traces back to Bitcoin's creation. The core maintainers resemble the bureaucracy – in the Weberian sense - of Bitcoin and they partly administrate the Bitcoin core client.

This first group presents striking similarities with the bureaucratic staff described by Weber in the pure type of rational authority. More precisely, there is no 'regular system of appointment,' nor 'fixed salaries' or 'a clearly defined sphere of competence subject to impersonal rules', let alone 'a rational ordering of superiority and inferiority' (Weber, 2012). These characteristics are outlined on the Bitcoin GitHub page, which reads: "[f]irstly in terms of structure, there is no particular concept of 'Core developers' in the sense of privileged people. Open source often naturally revolves around meritocracy where longer term contributors gain more trust from the developer community. However, some hierarchy is necessary for practical purposes. As such there are repository 'maintainers' who are responsible for merging pull requests as well as a 'lead maintainer' who is responsible for the release cycle, overall merging, moderation and appointment of maintainers"[35]. Because the lead maintainer and developers 'have always existed' and their powers of control have been handed down from the past, Bitcoin shares significant elements with the bureaucratic staff typical of traditional systems of authority. On this basis, one can conclude that the core maintainers closely resembles the bureaucratic

[35] https://github.com/bitcoin/bips accessed on 22nd of March 2019

structure proper of traditional systems of authority, which implies that Bitcoin's authority is cultivated on the belief in tradition.

The second group of actors is the miners. Miners are in charge of collecting pending transactions and execute the Nakamoto Consensus algorithm to append new blocks to the Bitcoin's blockchain. In doing so, they secure the Bitcoin network by providing an enormous amount of computing power to solve a cryptographic puzzle. The rise of this group of stakeholders is a direct result of the performative nature of Bitcoins' architecture. Miners are the result of the Bitcoin protocol intended as a "technique for achieving voluntary regulation within a contingent environment" (Galloway, 2004, p. 7), so much so that it has been argued that the real decision power lies within this group (Dierksmeier & Seele, 2016). There are not many miners at work within Bitcoin.

Gencer et al. measured the distribution of the mining power within the Bitcoin network and found that, during the measurement period, "the top four miners have more than 53% of the average mining power" (Gencer et al., 2018, p. 10). This finding is consistent with the measurements provided by the website arewedecentralizedyet.com, which - at the time of writing - states that four entities control more than 50% of the mining power in Bitcoin[36]. The characteristic of the class of miners appears hard to justify in light of Satoshi's initial vision of 'one-CPU-one-vote' inspired by egalitarian ideals. Yet, if one considers Bitcoin's claim to imperative co-ordination as grounded on tradition, then it is possible to explain why – in more than 10 years - no practical solution has been implemented to limit miners' power and influence on the network. In particular, it appears that limiting miner's influence by substantially changing Bitcoin's traditional design could undermine the basis for the system's own authority. The persistence of this state of affairs is difficult to account for by looking at Bitcoin's

[36] https://arewedecentralizedyet.com/ accessed on 2nd of February 2019

decentralized and distributed ethos, conversely it is readily explained by regarding it as a system of imperative co-ordination based on tradition.

Another element to support the present argument is that conflicts resulted in multiple hard-forks, yet the social structure of the forked systems does not appear to change significantly. This is consistent with Weber's account when he writes that, in the pure type of traditional authority, "[o]pposition is not directed against the system as such" (Weber, 2012, p. 342). Rather, it is directed to specific choices within the paradigm of tradition. This remark is supported by the structure of forked versions of Bitcoin such as Bitcoin Cash, and Bitcoin SV. Interestingly, both these versions of Bitcoin claim to represent the true spirit of a "P2P electronic cash system" as handed out from the past by Satoshi. Moreover, they also have a group of lead developers as well as miners.

The previous paragraphs exposed how part of the social structure of Bitcoin can be described according to the pure type of traditional authority described by Weber. It seems fair to conclude that, if one grants that Bitcoin cultivates its belief in legitimacy on traditional grounds, it is then possible to explain some of the crucial elements of Bitcoin's social structure. However, as it has been argued throughout this work, blockchains are a mix of social and technical elements. On this basis, the next section examines the Nakamoto consensus algorithm to assess whether its implementation is consistent with the claim that Bitcoin is a traditional system of authority.

6.1.2 Bitcoin as a technical system grounded on tradition

The current section focuses on the technical mechanisms that execute Bitcoin's authority by looking at an important element of Bitcoin protocol, namely, the consensus algorithm. At this level, the performative nature of Bitcoin's protocol in shaping and dictating the behavior of the agents interacting within the network is taken into consideration. This is because "technology is social before it is technical" (Deleuze, 1988, p. 40). Therefore, we should expect Bitcoin's consensus algorithm to be 'traditional' in the sense that it persists through time and that is had been handed out from the past. Indeed, we find that all the technical components of Bitcoin's consensus algorithm originated in the academic literature of the 1980s and '90s (Narayanan & Clark, 2017). Further, Bitcoin's consensus protocol has not been modified since its original design by Satoshi, a circumstance that points to a traditional basis for its persistence.

The problem that the consensus algorithm solves is known as state replication, which is equivalent to ensure that the set of balances and transactions are consistent among nodes. Additionally, Bitcoin's software achieves Byzantine fault tolerance, that is, it can tolerate the unexpected behavior of a subset of the nodes under the assumption that more than 51% of mining nodes are honest (Lamport et al., 1982). It is important to note that Bitcoin is an open peer-to-peer network; hence, Sybil attacks are a source of concern (Douceur, 2002). Bitcoin adopts the proof-of-work technique to address the Sybil attack vector by making it expensive to participate in securing the network. By combining Byzantine fault tolerance and the PoW technique Bitcoin achieves reliability and consistency of state replications in an open, adversarial setting under the previous assumptions. It is important to note that some researchers suggest that the threshold for Bitcoin's security is higher than 51% if some miners engage in a strategy known as selfish mining (Eyal & Sirer, 2018). Within these adversarial assumptions, the NC algorithm can be described as follows:

Algorithm 3: Nakamoto consensus protocol general procedure

```
   /* Joining network                                   */
1  Join the network by connecting to known peers;
2  Start BlockGen();
   /* Main loop                                         */
3  while running do
4      if BlockGen() returns block then
5          Write block into blockchain;
6          Reset BlockGen() to the current blockchain;
           /* Gossiping rule                            */
7          Broadcast block to peers;
8      end
       /* Longest-chain/validation rule                 */
9      if block received & is valid & extends the longest
        chain then
10         Write block into blockchain;
11         Reset BlockGen() to the current blockchain;
12         Relay block to peers;
13     end
14 end
   /* PoW-based block generation                        */
15 Function BlockGen():
16     Pack up transactions (including coinbase);
17     Prepare a block header context 𝒞 containing the
        transaction Merkle tree root, hash of the last block
        in the longest chain, timestamp, and other essential
        information reflecting blockchain status;
       /* PoW hashing puzzle                            */
18     Find a nonce that satisfies the following condition:
                        Hash(𝒞|nonce) < target
        wherein more preceding zero bits in target indicates
        a higher mining difficulty;
19     return new block;
20 end
```

There are known issue with this solution. First, it requires users to possess specialized hardware to participate in the mining process as the BlockGen function is better executed by application specific integrated circuits or ASICs. So that the execution of this process has become an industrial activity. Second, this procedure result in significant energy waste which entails that the carbon footprint of Bitcoin is increasingly a source of concern (Krause & Tolaymat, 2018; Stoll, Klaaßen, & Gallersdörfer, 2019). Despite the availability of more distributed solutions, greener alternatives, and slow performance, Bitcoin's consensus algorithm has not been changed since its first implementation, nor it is likely to be changed in the future. It is possible to explain this circumstance if Bitcoin's legitimacy is traditional. The belief in Bitcoin as an imperative co-ordination system is sustained by

the fact that Bitcoin does not change, and that its consensus algorithm has always existed in this form. Hence, implementing any substantial improvement would imply undermining Bitcoin's attempt to cultivate its authority in the tradition. The previous argument is consistent with the so-called Szabo rule for blockchain governance – a popular position among Bitcoin's supporters - that states: do not implement changes to the blockchain protocol unless the changes are required for the purpose of technical maintenance[37]. Leaving aside semantic disputes on the exact meaning of 'technical maintenance' Szabo's rule appears grounded on the same basis as Weber's pure type of traditional authority. Therefore, the persistence of Bitcoin's consensus algorithm in its original form is consistent with the belief in its traditional authority. Another observation supports this perspective.

When debating changes to the protocol as in the debate to increase the size of blocks supporters of the increase argued that it was always intended to increase (Hearn, 2015). Weber's theory explains it elegantly: "What is actually new is thus claimed to have always been in force but only recently to have become known through the wisdom of the promulgator" (Weber, 2012, p. 342). Further, forked version of Bitcoin did not change the procedure of the consensus algorithm. Bitcoin is the most prominent example of blockchain's authority that resembles Weber's pure type of legitimate co-ordination justified on tradition, yet, the landscape of blockchains and distributed ledgers provides us with many other examples that do not appear to be grounded on the same beliefs. Other systems appear to cultivate their *herrschaft* on elements that are found in the other two pure types described by Weber's theory. Thus, this chapter turns to examine two blockchains which share several similarities with Weber's pure type of charismatic authority.

[37] See chapter IV for the relevance of Szabo's law in the context of the governance of distributed consensus networks.

6.2 Charismatic Authority

The second pure type described by Weber is charismatic; this section describes the charismatic pure type of authority before examining the charismatic traits found in two prominent blockchains. Charisma describes "a certain quality of an individual personality by virtue of which he is set apart from ordinary men and treated as endowed with supernatural, superhuman, or at least specifically exceptional powers or qualities" (Weber, 2012, p. 358). Based on 'charisma,' the individual is treated as a leader. Additionally, appreciation on the part of those subject to authority is decisive for the legitimation of imperative co-ordination systems grounded on charisma[38]. Akin to the traditional authority, there is no such thing as a definite sphere of authority and competence, let alone formal rules or abstract normative principles. The ideal type of charismatic authority applies the 'rule of genius' which elevates people of normal origin to leaders (*ibidem*, p. 362). It is important to note how the pure type of charismatic authority is inherently unstable and, therefore, tends to become either traditionalized or rationalized or a combination of both. In the context of blockchains, two systems appear to possess charismatic traits, namely, Ethereum and Tron. The next sections will show how both these systems appear to draw users and capital on the basis of the 'rule of genius' of their creators, and, how socio-technical arrangements reflect it.

[38] In the ideal type Weber identifies the basis of the claim to legitimacy in 'the conception that it is the duty of those who have been called to a charismatic mission to recognize its quality and to act accordingly', rather than the charisma itself

6.2.1 Ethereum and Tron as social systems grounded on charisma

Ethereum and Tron appear to partially establish their claim to legitimacy by leveraging the reputation of their founders, Mr. Vitalik Buterin and Mr. Justin Sun, respectively. Mr. Justin Sun founded the Tron foundation limited in July 2017; it is incorporated in Singapore under the discipline of a public company limited by guarantee. The foundation fosters the development of the Tron network, and Mr. Sun acts as the CEO. In July 2018 Tron announced the acquisition of the popular file-sharing platform BitTorrent to grow its user base and establish another market for a newly created token: BTT. More generally, Tron is a smart contract platform built on the blueprint of Ethereum and their similarities are striking, in fact, Tron was initially born as a forked version of EthereumJ, hence many technical aspects overlap. For example, the programming language solidity - developed for writing applications for Ethereum - can also be used to implement applications on the Tron network. What is essential for our analysis is how Mr. Sun pushes for a decentralized vision of the internet and a 'liberal and democratic community' where he is in charge. More precisely, Tron's narrative purports to achieve decentralization through centralization in the initial phase, in which many critical decisions have been taken by Mr. Sun. The charismatic allure of Mr. Sun is apparent when one considers that the smallest unit of the Tron cryptocurrency (TRX) is called SUN, and that Mr. Sun is one of the so-called Super Representatives (SR) that Tron utilizes in its consensus protocol (see next section). Additionally, it is beyond doubt the Mr. Sun acts as the public face for the Tron network and that he heavily influences much of its development. More recently, Mr. Sun won the annual charity lunch with Mr. Warren Buffet and made no secret about it. Lastly, on the Tron Website there is a list of Mr. Sun’s personal accomplishments that are not immediately related to the Tron project.

The other blockchain system possessing charismatic traits is Ethereum. Ethereum was founded - among others - by Mr. Vitalik Buterin, 19 years old Russian-Canadian recipient of the Thiel

fellowship, a 100.000 USD grant designed for kickstarting young entrepreneurs instead of having them going through college. Buterin is regarded as the leader and public face of the Ethereum system. It comes to no surprise that he has been referred to as the system's benevolent dictator. To a relevant extent, Buterin is a libertarian wonder boy who perfectly embodies the broader right-wing ideology behind most open blockchain projects. Buterin appears as a champion of technocratic reasoning; he appears to believe that every problem has a technological solution (Buterin et al., 2018). His influence on the Ethereum network is manifest. Recently, Buterin outline the road map for the future of the Ethereum platform, so-called Ethereum 2.0 expected to roll out in 2020.

In both communities, Mr. Sun and Mr. Buterin play prominent roles. Most stakeholders regarded them as the public face of each system, suffice is to note the drop in the price in Ethereum when false rumors about Buterin's health conditions spread. Both systems appear, in fact, significantly steered by these two figures under what can be defined as a version of the rule of genius. They both push for a decentralized future where the imperative of scalability is tantamount. For example, Buterin's imperative of scalability drives the study of network's improvements such as sharding and proof-of-stake protocols. The latter being a technical solution to the scalability problem that is hard to justify from the perspective of a decentralized system as it resembles an example of plutocracy because it grants rewards on the basis of how much wealth – measured in Ether – agents are willing to allocate for the verification process. In Ethereum and Tron, the end of decentralization is fostered by Buterin's and Sun's visions respectively, so that, it becomes the charismatic mission of these systems.

Both Ethereum and Tron establish their belief in legitimacy not on their charismatic figures per se but, as indicated by Weber, on the moral duty of those who have been involved in the charismatic mission: to decentralize. The authority of such systems is, therefore, justified by the goal of decentralization as articulated by their leaders. Their leadership role is accepted for the belief in the end goal of decentralization. Little attention is devoted to the fact that decentralization in itself is arguably not an end (Schneider, 2019; Walch, 2019b) and that systems such as Ethereum and Tron

provide "an illusion of circumventing economic power with decentralised nodes" (Baldwin, 2018, p. 6)

While the governance structures of both systems are informed by the blueprint provided by the FOSS movement both individuals play a crucial role in marketing the platform and vocally promote on social media, taking a role which could be defined as benevolent dictators (Bian, Mu, & Zhao, 2018). Hence, it seems fair to conclude that their presence and influence in the social environment of Tron and Ethereum, is a consequence, at some level, of their charisma. So that, the *herrschaft* of these systems appears to be grounded on elements qualified by Weber in the pure type of charismatic authority. More precisely, their leaders' charisma is apparent when observing their role within the respective communities. Chiefly, obedience is granted to the mission of decentralization. The next section explores if charismatic traits are to be found in the technical aspects of Tron and Ethereum.

6.2.2 Ethereum and Tron as technical systems grounded on charisma

Ethereum and Tron protocol differ from regular cryptocurrencies in that they provide a similar virtual machine (VM) to execute smart contracts computations. To recall a distinction, introduce earlier in this work (see chapter 4), these systems are Turing complete, which means that they are in principle able to run any algorithm. However, they differ significantly with respect to the consensus algorithm.

Ethereum uses a modified version of the Bitcoin's algorithm in which the main difference consists in a shorter interval between blocks and the use of another hashing function, Ethash. This function was designed to be memory intensive in an attempt to provide more resiliency against the concentration of mining power when compared to the SHA256 function. Ethash generates a directed acyclic graph (DAG) file which size increases every 30.000 blocks (called an epoch), at the time of writing the size

of the DAG file is 3.05 GB. This file has to be stored in memory in order to execute the consensus algorithm; thus, it provides more ASIC resistance than Bitcoin's one. Moreover, Ethash uses Keccak, a hash function eventually standardized to SHA-3, and a slightly modified version of earlier Dagger and Hashimoto hashes to remove computational overhead. The differences between the classical solution implemented in Bitcoin were originally justified to provide better resistance to miners' centralization, for example, Buterin famously tweeted, in occasion of a Bitcoin conference in Hong Kong, that when it is possible to gather more than 51% of the mining power and the core developers on one single stage, the system is hardly decentralized.

However, recent empirical data show that Ethereum is even less decentralized than Bitcoin, for example, Gencer et al. conclude that "[o]n average, 61% of the weekly [mining] power was shared by only three Ethereum miners" (Gencer et al., 2018, p. 10) Their finding is consistent with the measurement provided by arewedecentralizedyet.com, which - at the time of writing - suggests that three miners control more than 50% of the mining power. These findings should jeopardize Buterin's role in Ethereum and undermine his position within the community, however this is not the case. It is possible to argue that the rule of genius instantiated in Ethereum prevails over the empirical evidence for the lack of decentralization of the system (Wu et al., 2019). This might be due to the charismatic nature of the mission of decentralization as articulated by Mr. Buterin. Obedience is still granted in face of the empirical contradictions outlined above.

Tron, instead, uses an election-based consensus algorithm known as delegated proof-of-stake or DPoS to achieve better performance in terms of transaction throughput. Tron claims to handle 2000 TPS; however, their block explorer consistently ranks the maximum throughput of around 800 TPS. It should be noted that performance among blockchains does not come without its tradeoffs. Hence, Tron sacrificed openness and security for the sake of performance. The DPoS algorithm implemented by Tron can be described as follows.

The 27 validators (or Super Representatives - SR - in Tron's language) are selected among a pool of 127 candidates via an election every six hours. Once the validators are selected each take turn via a round-robin procedure[39] to produce a new block to append to Tron's blockchain. To become an SR, one must pay 9999 TRX (roughly 300 euros at the time of writing) and complete an application process on Tron's website. In order to vote in the election of the 27 SR, Tron power (TP) is needed, users can exchange TP for TRX at the ration of 1:1. Users can obtain votes by freezing units of the cryptocurrencies Tron. Once the election is over the funds are automatically released. The system incentivizes participation by allocating rewards to the users who participate in the election process in the following way. When a block is added the SR who adds a block receives 32 TRX, this occurs every three seconds. Annually, 336.384.000 TRX will be allocated to SRs, interestingly Tron does not have an issuance scheme for its currency. Therefore, the total supply of TRX is fixed until 2021, what will happen next is anybody's guess. From the exposition above it is clear how Tron's consensus algorithm is hardly in need of further elucidation, token holders vote based on their wealth - measured in TRX tokens - on who gets the permission to write new blocks to the chain for a reward.

The general procedure for DPoS consensus algorithm can be formalized as follows:

[39] Round-robin is an algorithm that assigns priority to each task in equal portions and in circular order, handling all processes without priority (also known as cyclic executive).

Algorithm 6: BFT-based PoS general procedure

```
1  Join the network by connecting to known peers;
2  Start BlockGen();
   /* Main loop                                   */
3  while running do
       /* Block proposing & broadcast             */
4      if BlockGen() returns block then
5          Add block to its tempBlockSet;
6          Broadcast block to the network;
7      end
       /* Block validation                        */
8      if block is received & is valid then
9          Add block to its tempBlockSet;
10         Relay block to the network;
11     end
       /* BFT consensus layer                     */
12     if new consensus epoch then
13         Perform BlockFinBFT() on tempBlockSet;
14         Write the winning block to blockchain;
15         Clear tempBlockSet;
16     end
17 end
   /* PoS-based block generation                  */
18 Function BlockGen():
19     (Any feasible PoS mechanism that injects a stable
        flow of blocks to the BFT consensus layer.)
20     return block;
21 end
   /* BFT-based block finalization                */
22 Function BlockFinBFT():
23     Participate in a BFT consensus that finalizes one
        winning block out of tempBlockSet;
24     return the winning block;
25 end
```

In Tron's case, the charismatic mission of decentralization is capable of justify implementing a procedure that privileges some nodes over others. This might be because Mr. Sun believed that scalability was a primary goal for the platform to truly decentralized the internet. In this case, decentralization- in terms of open participation - at the technical level of the consensus algorithm was sacrificed to achieve higher performance. It seems possible to justify this technical choice by the belief in the charismatic vision of Mr. Sun, according to which, 'to decentralize' justifies the trade-offs described above.

More recently, to address the shortcoming of some blockchain systems, new designs have been proposed that depart significantly from pre-existing ones. Interestingly, blockchains' evolution appears to trend in the direction of the last pure type theorized by Weber, namely, rational-legal authority. On this basis, the next section examines the pure type of rational-legal authority and two systems that appear to ground their legitimacy on it to a significant degree. Interestingly, both systems adopted a body of off-chain norms that they regard as their constitution.

6.3. Rational-legal Authority

The validity of the claim to legitimacy of the last pure type is based on rational grounds, and it rests on a belief in the legality of patterns of normative rules and the right of those elevated to authority under such rules to issue commands (Weber, 2012). Weber defines this pure type of imperative co-ordination as the rational-legal authority. In the next paragraphs, a description of the salient elements of this pure type will be provided.

According to the German sociologist, a claim to legitimacy based on rational-legal grounds depends on the acceptance of the following mutually inter-dependent ideas. First, norms may be established by agreement or imposition on all the subjects under a given sphere of authority. Second, a body of norms is a consistent system of abstract rules which have been intentionally established or imposed, which entails that persons in authority occupy an office. Third, obedience is granted to the impersonal order established by norms and not to any person; thus, in the rational-legal pure type, obedience is impersonal. The distinctive element of this pure type of imperative co-ordination is the bureaucracy. More precisely, Weber describes a particular bureaucratic arrangement based on the following elements: (a) continuous organization bound by rules (b) specified sphere of competence (c)

hierarchical organization (d) administrative-technical rules that require specialized training (e) separation of the members of the administrative staff from the ownership of 'the means of production or administration'. A further essential characteristic of this pure type is that administrative decisions and norms are expressed in writing. In his analysis of the rational-legal authority, Weber delves into the characteristics of the administrative staff employed in the exercise of legal authority. He distinguishes between monocratic and bureaucratic administration; the latter is to be found in modern nation-states, the former mostly among corporations. The reason is that the monocratic type of bureaucratic administration is "capable of attaining the highest degree of efficiency and is in this sense formally the most rational known means of carrying out imperative control over human beings" (Weber, 2012, p. 337).

The next paragraphs examine two examples of blockchains which, in their governance structure and design choices, appear to implement elements of the pure type of rational-legal authority, namely EOSIO, and Decred.

6.3.1 EOSIO and Decreed as rational-legal social systems

EOSIO is a software platform launched in 2018. As of the time of writing the cryptocurrency of EOSIO, known as EOS, ranks eight in total market capitalization[40]. According to Bloomberg, 48% of daily active users of all blockchain systems use EOSIO's platform[41]. EOSIO is built and managed by Block.one, an exempted company incorporated in the Cayman Islands that raised over 1 billion

[40] Data retrieved from https://coinmarketcap.com/ on the 29th of October 2019.

[41] https://www.bloomberg.com/news/articles/2019-03-28/better-version-of-bitcoin-loses-luster-as-apps-move-elsewhere accessed on the 8th of May 2019.

USD in its token sale in 2017. The EOS system is different when compared to other 'older' blockchain systems for the following reasons.

The idea behind EOS is to address the problems of other systems by enabling effective governance of the architecture. Daniel Larimer, CTO of block.one wrote that "[o]nly the most universally competent dispute resolution systems and blockchains will survive" (Larimer, 2018). EOS, then, adopted a constitution to cultivate its claim to legitimacy on norms written in natural language. EOS attempts to justify itself as a system of imperative co-ordination on rational-legal norms. For example, EOS formalizes the governance of the platform with institutions such as the Eos Core Arbitration Forum or ECAF[42]. Participants in the system must agree to the constitution by including a hash pointer of it in each transaction. The EOS - interim - constitution has 19 articles covering matters from restitution (article VI) amending (article XI) and choice of law (article X). The EOS platform was among the first systems to acknowledge the importance of off-chain rules in order to enable legitimate changes to its architecture.

In EOS a new group of stakeholders, named block producers, replaces miners. Holders of EOS token can vote and elect 21 block producers that will then add new information to the blockchain, similar to the solution adopted by Tron. The voting and the participation in the election process is free, instead of 'burning' tokens after voting EOS tokens are frozen and can be unfrozen by their holders, 1 EOS token equals to 30 votes. Votes have a half-life of 1 year, and they progressively lose weight over time. Block producers are actively involved in shaping the direction of development of EOS. What is more interesting for the current analysis is that much of the operations of EOSIO and of its stakeholders find their justification in a body of norms intentionally established that stakeholders are required to accept when joining the network. In this sense, EOS appears to significantly ground its

[42] It is worth noting that since its establishment the ECAF was at the center of several controversies until it was abandoned.

authority on rational-legal basis. Another example of this trend of building off-chain institutions which appear justified on the basis of a belief in the authority of an impersonal order is Decred.

Decred is an autonomous digital currency for the people, and similar to EOSIO it has a constitution written in natural language that 'defines a set of principles which guide the decision-making of the project's stakeholders and describes the processes through which the blockchain and Treasury are governed' [43]. The constitution is divided into three sections, namely, principles, blockchain governance, and project governance funding. The rationale of this document is to 'manage the expectations of prospective and actual Decred users' which is consistent with a claim to legitimacy based on rational grounds as described by Weber. Unique to Decred is the presence of both miners and voters who stake their assets in a PoS fashion, interestingly, in case of contrast, PoS voters can discard a block produced by a miner if a simple majority is reached. Further distinctive elements of Decred are its institutions: (a) project treasury administered by a development organization and (b) the Decred contractor collective (an organ to manage the contractors hired by the platform).

The creation of several institutions within Decred at the off-chain level is significant from the perspective of Decred's *herrschaft*. It appears as a manifestation of the trend to recognize the importance of governance structures and principles before any line of code is written. This entails that Decred's claim to the legitimacy of its off-chain operation hinges on the acceptance of a body of rules intentionally established. Similar to EOSIO, Decred departs significantly from previous governance structures. This is likely a consequence of the attempt to grant obedience on rational-legal grounds. The next section examines if the aforementioned rational-legal elements are reflected in the consensus algorithms of these systems.

[43] The Decred constitution is available here https://decred.org/

6.3.2 EOSIO and Decreed as rational-legal technical systems

A rational-legal base to foster legitimacy enables systems such as EOSIO and Decred to uphold principles and establish, before the implementation phase, the design specification of their consensus algorithm. This section first examines the consensus protocol implemented by EOSIO, and then the one of Decred.

The EOSIO protocol provides finality. This means that nodes on the network have high confidence that transactions are valid without relying on a probabilistic calculation. The first generation of consensus algorithms for blockchains mostly relied on a probabilistic finality, and this is the reason why it is commonly advised to wait for n confirmations in order to be sure that one's transaction will not be reverted. For example, in Bitcoin, the n that guarantees sufficient reliability is 6, which corresponds to around 60 minutes at the average block rate of ten minutes. On the contrary, EOSIO provides finality by implementing a pipeline BFT layer to order blocks among the set of the 21 validators elected by its users. This is possible because EOSIO implements a DPoS consensus algorithm as the one described earlier in the context of Tron; in fact, it is possible to achieve finality only when the validators are known. Validators rotate - again in a round-robin fashion - every 12 blocks (a new block is produced every 500ms) so that EOSIO achieves absolute BFT finality in 3 minutes and single block finality every 2 seconds. As with other BFT protocols, the system can tolerate at most 1/3 of its nodes engaging in a byzantine behavior. Thus, EOSIO can tolerate 6 out of 21 nodes behaving incorrectly, either for technical reasons or maliciously. However, it must be noted that - due to the process of election and mandatory disclosure necessary to become eligible to be elected as a validator - it is unlikely that any validators will act willingly against the network.

Block producers receive 1% of the total supply of EOSIO tokens as a reward for their efforts in maintaining the network, the recent resolution to reduce the inflation rate from 5% to 1% does not

affect the reward allocated to block producers but only the amount allocated to the eosio.saving account. This account is designed to fund further development of the EOSIO platform, and its presence is established in the EOS's constitution so that its technical protocol follows from the establishment of rational-legal, impersonal, rules.

Decred consensus algorithm is a combination of both PoS and PoW based on the work of Benton et al., Decred refers to this design as hybrid while the authors of the original work called it proof-of-activity (Bentov, Lee, Mizrahi, & Rosenfeld, 2014). In essence, this algorithm uses a staking procedure to simulate a lottery with a token that is then used by the proof-of-work miners in their calculation. More precisely, holders of the Decred token (DCR) can purchase the token necessary for participating in the staking process by locking DCR. The tokens needed to participate in the staking process are called tickets. The amount of DCR needed to purchase a ticket is automatically adjusted because the ticket pool size is capped at 40.960 Tickets, the price of tickets is re-calculated every 144 blocks. At the time of writing a single ticket runs for approximately 3.000 USD. It is also possible to buy a fraction of a ticket via a ticket-splitting software. Tickets are then used by PoW miners to sign the new blocks (a minimum of 3 votes is needed, but a reduction in the block reward occurs if fewer than five votes are included) therefore, the nodes holding the tickets must be connected to the network 24/7 to prevent missing the reward. In a ticket holder is not reachable, the ticket will be marked as missed, and no reward will be allocated. Tickets are selected pseudo randomly according to a Poisson distribution. Accordingly, any given ticket has a 99.5% chance of voting within 40.960 blocks, that is approximately 142 days. After this period if the ticket has not voted it expires and the funds locked for its purchase are released. Tickets are also necessary in order to vote on the Decred Change Proposal or DCP. These procedures enable users to approve changes to the system as established by Decred constitution. It is interesting to note how Decred blurs the distinction between on-chain and off-chain governance as the constitution provides formal parameters easily implemented in the software.

The second part of the consensus algorithm is the known mechanism of proof-of-work. It is useful to remember that Decred heavily draws from the Bitcoin design, hence the presence of UXTOs and OP codes in transactions. However, the PoW procedure presents some differences to which we now turn. The main difference is that PoW miners must include at least three tickets selected from the memory pool. Another difference is that Decred uses a different hashing function, instead of the SHA-256 function, it adopts the BLAKE-256 hashing function. The structure of this function is similar to Bitcoin's; therefore, regular users are practically excluded from the mining process. For this reason, Decred actively advises against so-called Solo Mining and encourages users to join mining pools. Interestingly, akin to Bitcoin, the supply scheme of block-reward is deflationary. Therefore, the last block reward will be created in September 2120; the upper limit on the total supply is 20,999,999.99800912 DCR. The reward is split three ways: 60% goes to the PoW miner, 30% to PoS voters and 10% to the Decred Treasury. The cost of the tickets renders users' participation extremely costly, and the presence of specialized miners might create the same lockdown effect observable in Bitcoin. As in the case of EOSIO, part of the resources of the network are allocated to foster the system’s development. Hence, both systems included elements of the bureaucratic principles outline in Weber’s conceptualization of the pure type of rational-legal authority. More precisely, bureaucratic institutions are established by means of deliberate norms that provide for specific spheres of competences.

The previous sections described two systems that appear to be closer to the pure type of rational-legal authority in justifying their claim to legitimacy. The next section summarizes the findings of this descriptive inquiry on the legitimacy of several blockchain systems.

6.4 Is this enough?

This chapter analyzed the *herrschaft* of several blockchain systems and evaluated different basis for their legitimacy. The goal of this chapter was to show how different beliefs in the legitimacy of each system are reflected at the social and technical level. Therefore, systems such as Bitcoin have different protocols and governance structures than others such as EOSIO because their legitimacy hinges on different basis. It comes to no surprise that the comparison between blockchains and other normative systems has appeared in the literature.

Berg et al. applied the concept of 'constitutional catallaxy,' that is 'constitutionalism as a catallactic enterprise of rule-setting' to blockchains and distributed ledgers (A. Berg et al., 2018). While these authors refer mainly to the work of Buchanan, the idea of the protocol as a constitutional type of ordering traces back to Patrick Feng who said in 2004 that "Creating core protocols is something akin to constitutional law" (cited in Galloway, 2004, p. 245). Complementing this view, the previous paragraphs attempted to show how diverse systems produce varied rules on the influence of their *herrschaft*. More precisely, Weber's account of the pure types of imperative co-ordination was adopted to highlight how different beliefs in legitimacy may explain the differences among blockchains. Consequently, it should be clear why speaking of the blockchain as an imperative co-ordination system is a categorical mistake for no such thing exists. This finding is particularly relevant for regulatory purposes as a regulation covering 'the blockchain' or 'distributed ledgers' would likely miss its target. Depending on the specific arrangements of each system, regulatory and policy response ought to be adjusted by, for example, taking into consideration the different technical solutions found by looking at the blockchain landscape.

To sum up, I attempted to show how different blockchains fit within the Weberian pure types both in their social and technical aspects. It is useful to remember that no system of imperative co-ordination

is likely to fit perfectly the description of a given pure type, this is even more evident when technology is adopted in the exercise of imperative co-ordination. However, Weber's model is suited for empirical analysis, and it has been useful to sketch the different beliefs on which some blockchains cultivate their claim to legitimacy. It is reasonable to conclude that some of the differences across blockchain systems are partly explained by examining what is considered legitimate among them.

On this basis, I examined the Bitcoin ecosystem through the lens of traditional authority, Ethereum, and Tron within the one of charismatic authority and, lastly, EOSIO and Decred via the pure type of rational-legal authority. Naturally, some systems resemble pure type better than others. However, this analysis shows that "according to the kind of legitimacy which is claimed, the type of obedience, the kind of administrative staff developed to guarantee it, and the mode of exercising authority, will all differ fundamentally" (Weber, 2012, p. 324). More precisely, within blockchains this differentiation is observed at two different levels, namely, social and technical.

In conclusion, systems that establish authority on rational-legal grounds seem to be better positioned to gain a competitive advantage on the ones who rely on charismatic and traditional grounds for the difficulty of traditional ones to adapt to changes in the environment and the inherent instability of charismatic ones. This is to say that blockchains might be on a path that resembles the one observed in other systems of authority, e.g. nation states, in which there has been a progressive shift form the traditional and charismatic types of imperative co-ordination to the rational-legal ones. Newer systems are striving to cultivate their belief in legitimacy on progressively more rational grounds in a process that could be defined as the rationalization of blockchains. The observed trajectory explains why newer systems adopted off-chain bodies of intentionally established norms that have been qualified as constitutions. This opens an interesting research avenue for legal research, namely, what kind of legal norms and institutions are likely to evolve within blockchains and which of the existing legal constructs might be ported successfully.

However, when examining the basis on which blockchains claim legitimacy it appears that Weber's account is incomplete. More precisely, popular narratives around these systems do not appear to perfectly conform to any of the pure type of imperative co-ordination or to a combination of them. It seems that other motives are put forward to justify power exert by blockchain networks that defy Weber's categorization, i.e. the belief that power is legitimately exerted using algorithms that have some specific characteristics. Hence, the next chapter attempts to complement Weber's methodology to better describe systems of imperative co-ordination such as blockchains and distributed ledgers that rely on algorithmic rules.

7. Algorithmic Authority

Blockchains and distributed ledgers exert power on their users via algorithms implemented and managed with complex governance processes (chapter IV). The use of technology to shape, nudge, direct agents' behavior is not new, many authors have discussed it from a multitude of perspectives such as law, sociology, and philosophy (Brownsword, 2019; Dos Santos, 2017; Fenwick, Kaal, & Vermeulen, 2016; Floridi, 2018; Floridi, Cath, & Taddeo, 2019; Hayes, 2019; Lupton, 2014). This chapter argues that distributed consensus systems appear to justify their authority on the basis of their algorithmic operations. It seems that technological solution that are transparent, open, unbiased, secure, immutable, tamper-evident, hard to stop, are perceived as better than other modes of exerting power. Following this narrative, Bitcoin is a better alternative than existing currencies because of the properties of its network, one of which is to reduce the need for trust by relying on code' Dangerous malleabilities, choices, and ambiguities are replaced by deterministic execution of transparent algorithms in a distributed peer-to-peer network. Moreover, transactions cannot be reverted, and third-party intervention is made difficult due to the system's architecture. Online payment is but one instance in which blockchain systems appear to establish their authority according to their algorithmic nature. In fact, what Bitcoin is in relation to payments, other systems are concerning different areas. For example, Ethereum allegedly allows individuals to build new socio-economic institutions more transparent, efficient, and predictable than existing ones (Wood, 2014).

Regardless of the domain in which blockchains are deployed, proponents believe in the legitimacy of these technical systems of rules because of their (technical) properties (Swan, 2015; Swan & De Filippi, 2017). In this sense, the claim to legitimacy of blockchains is based on the belief that power is better and legitimately exercised by algorithms rather than non-deterministic

institutional human processes, therefore blockchains and similar systems are perceived as authoritative. Hints to this ongoing process can be found across many areas, from the increasing relevance of techno-regulation, to the pervasiveness of digital technology in the on-life infosphere (Floridi, 2010, 2011). In the next paragraphs, the phenomenon of algorithmic appreciation is considered as one of the crucial elements that contributes to establish the legitimacy of distributed consensus systems and, ultimately, helps to explain agents' engagement.

When it comes to algorithms in matters related to judgment and decision-making psychological wisdom held that humans do not tend to rely on algorithms, a phenomenon called "algorithm aversion" (Dietvorst, Simmons, & Massey, 2015). The literature suggested that people might be skeptical in following algorithmic advice despite the superior accuracy demonstrated by algorithms in several areas relative to human judgment. However, recent research on the topic challenges this notion. In a series of experiments, Logg and colleagues demonstrated the opposite effect, that is, people adhere more to advice when they think it comes from an algorithm than from a person. Researchers called this effect "algorithm appreciation" (Logg, Minson, & Moore, 2019). The effect is significant because other researchers involved in the study predicted the opposite effect. Moreover, subjects in the study who faced a 'black box' algorithm were still willing to rely on that advice despite a total lack of transparency. When it comes to power exerted by/with algorithms, the phenomenon of algorithmic appreciation might play a crucial role. On the one hand, it partially accounts for the attempts to subtract authority from traditional sources due to perceived – and sometimes true – superior accuracy of algorithms. On the other hand, algorithmic appreciation might be the result of the low levels of institutional trust.

Algorithmic appreciation plays a role in the rise of the belief in the authority of algorithmic systems of rules as observed in the blockchain movement. Algorithmic appreciation is another element that points to the progressive relevance of algorithms and that it influences blockchains' claim to authority. Then, it is possible to explain the incomplete account of blockchains' legitimacy

given by the beliefs upon traditional, charismatic, and rational-legal basis. Something else, influenced by algorithmic appreciation is needed to explain satisfactorily why agents engage with blockchains and distributed ledgers. Therefore, this chapter adds to the pure type of rational-legal authority a technological dimension which will be named algorithmic authority. Interestingly, this extension partly contrasts the classical pure types of imperative co-ordination. In systems based on algorithmic authority, obedience is granted mostly on the basis of the characteristics of the computational algorithms that a given system runs. In code we trust.

The present chapter is organized as follows. The next section examines the term algorithmic authority; it traces back its origin and it distinguishes previous uses from the proposed meaning derived from the Weberian notion of authority. The second section describes the core ideas on which the legitimacy of algorithmic systems is predicated. The third section aims to evaluate to what extent the core elements of algorithmic authority are present in the current landscape of distributed consensus systems. Lastly, section 7.4 examines the consequences of the belief on the legitimacy of algorithmic systems of rules on the normativity within such systems, i.e. the law of distributed consensus systems.

7.1 The Meaning of Algorithmic Authority

The current section distinguishes the meanings of the term algorithmic authority and provides a definition for the rest of this work. This is necessary because the term algorithmic authority has been used before in other contexts, and the definition adopted in the current analysis departs from the previous ones.

Clay Shirky is credited as the first to use the term in public form on his blog[44]. On November the 19th 2009, he wrote a blog post titled "A Speculative Post on the Idea of Algorithmic Authority." Writing in the context of news media, Shirky defined algorithmic authority as "the decision to regard as authoritative an unmanaged process of extracting value from diverse, untrustworthy sources, without any human standing beside the result". He added three characteristics, namely, the aggregation of information from multiple sources, a record of good results, and the acceptability of it within a social group. In this sense, Shirky contended that internet companies such as Google or Twitter have algorithmic authority. Shirky's notion of authority appears to differ significantly Max Weber's notion of *herrschaft*, that is, 'imperative co-ordination.' In fact, Shirky's concept of authority seems better captured by the concept of reliability because it is not clear where power fits within his definition. Then, (some) algorithms have reliability because they aggregate information from multiple sources, have shown a good track record, and persons rely on them within a social group. It is important to note that, while being limited in scope, this use of the term algorithmic authority highlights the crucial component of reliability, which is important to explain the trend toward claiming the legitimacy of a system of imperative co-ordination because power is exerted with/by algorithms. After Shirky's post, the term gained traction in other fields.

In the legal domain, Frank Pasquale discussed the influence of algorithms in his popular book "The Black-box society," which draws upon his previous work on the topic (Pasquale, 2011, 2015). Pasquale argued that "[w]e can imagine a future in which the power of algorithmic authority is limited to environments where it can promote fairness, freedom, and rationality "(Pasquale, 2015, p. 16). He added that "authority is increasingly expressed algorithmically" citing Shirky's work. This definition of authority also does not fit the Weberian notion. For now, it is sufficient to note that algorithmic

[44] http://www.shirky.com/weblog/2009/11/a-speculative-post-on-the-idea-of-algorithmic-authority/comment-page-1/ accessed on the 20th of June 2018.

authority in the legal literature refers - mostly - to the increased reliance on automatic procedures and not as a mechanism to describe on what grounds power is legitimately exerted within a given system of rules. In other words, the current legal understanding of algorithmic authority regards it as a concept capable of exerting power on individuals, on the contrary, in this work authority is intended as the basis on which power is applied legitimately.

In the domain of human rights law, Aust argued that algorithmic authority "conveys the message that it is no longer just humans exercising power over other humans - but that the processes based on algorithms, machine learning, and big data mining may come to exercise some direct influence over individuals" (Aust, 2018, p. 2). Moreover, he framed the argument around the effects that the transition to algorithmic modes of influence has on agency "[t]his concept [algorithmic authority] captures the question of the potentially changing agency engendered by algorithms [...]. If we are indeed moving towards automated decision making, it would be apt to speak of 'algorithmic authority.' This authority would need to be exercised according to the law again." (*ibidem*, p. 7). Aust is right when he recognizes that algorithmic authority is about using computational techniques to exert power over individuals rather than authoring information. Therefore, his work is closer to the Weberian notion of authority adopted throughout this work. Other than in the legal domain, the term of algorithmic authority has also been used by sociologists and media scholars.

Sociologist Richard Rogers noted that "[m]ore recently, algorithmic authority, or the belief in the epistemological value of search engine results, became a way to phrase the power of Google" (Rogers, 2013, p. 119). Rogers was right in recognizing how the use of the term from Shirky and others, denotes "trust in the epistemological value of engine output" (*ibidem*, p. 96). In this sense, authority has little to do with power. It appears that the term algorithmic authority was used to denote the increasing reliance on the epistemological value of algorithmic outputs as in the previous uses by Shirky and Pasquale. While it is true that the epistemological aspect might be an important component in the establishment of a belief in the legitimacy of power exercised by/with algorithms, authority in

the Weberian sense is legitimate exercise of power. For this reason, Rogers' understanding of algorithmic authority is not sufficient for the purpose of this work, which is to explore the core claims that blockchains' proponents put forward when arguing for the adoption of these technologies.

Debra Lupton, another sociologist, helps us moving closer to our definition. In her work Digital Sociology, she explained the epistemological reliance on algorithms as a form of power over knowledge. Lupton wrote, "they [search engines] exert power over what sources are considered important and relevant"(Lupton, 2014, p. 49). Later, she added that power in a more general sense is exerted by algorithms on individuals not only at the level of search engines, "[t]he digital subject is made intelligible via the various forms of digital data produced about it using algorithms, as are the conditions of possibility that are made available" (*ibidem,* p. 105). Here, it is possible to note a synergy with Lessig's work in that the architecture of the cyberspace - that is, code - establishes the condition of possibility of the environment. Further, Lupton argued that "[t]his is a form of power but one that configures and invites choice (albeit by also structuring what choices are generated) based on the user's previous and predicted actions, beliefs and preferences." (*ibidem*) While Lupton was mostly concerned with private algorithms deployed by technology corporations, she recognized the ontological relevance present in the notion of algorithmic authority for its ability to promote a systemic analysis of the phenomena at hand. With regard to the field of distributed consensus systems, the term algorithmic authority has already been used.

Caitlin Lusting, along with others, wrote of algorithmic authority in the context of Bitcoin (Caitlin Lustig, 2018; C. Lustig & Nardi, 2015; Caitlin Lustig et al., 2016). While this perspective builds upon the Weberian notion of authority as the legitimate exercise of power it can be critiqued on the following grounds. First, their definition of algorithmic authority, that is, "the trust in algorithms to direct human action and to verify information in place of trusting or preferring human authority" does not correspond with the Weberian use of the term authority (C. Lustig & Nardi, 2015, p. 743). Therefore, one is left wondering the choice of adopting Weber's classification of legitimate

exercise of power when their conclusion hinges on the trust on algorithmic processes and not on the fact that specific algorithms grounds the belief in the legitimate exercise of power, i.e. authority, of a system of rules. Second, technology is relied upon rather than trusted (see supra, chapter 3). Third, the pure types of Weber do not imply a preference or trust toward humans, for example, rational-legal authority is based "on a belief in the 'legality' of patterns of normative rules" so that "it is held that the members of the corporate group, is so far as they obey a person in authority, do not owe this obedience to him as an individual, but to the impersonal order" (Weber, 2012, p. 328). Then, algorithmic authority is not necessarily about preferring computations to human judgement, rather it is about preferring computations to other mechanisms of co-ordination as, for example, the impersonal order established by legislation. Further, Lusting et al. maintained the epistemological element of algorithmic authority present in Shirky's account, yet, authority in the Weberian sense does not concern the verification or retrieval of information as explained above.

A last ground for criticism hinges on the reason put forward to explain the choice of Bitcoin as an object of study. Lustig et al. wrote: "[w]e chose Bitcoin as an example of algorithmic authority because it is not managed by governments or banks, but by algorithms," this is not correct (C. Lustig & Nardi, 2015, p. 744). Many contributions to the literature on the topic have highlighted how Bitcoin is not managed solely by algorithms but by a specific governance process, see chapter 4 (Mattila & Seppälä, 2018; Zachariadis et al., 2019). Contrarily, this works argues that elements of algorithmic authority justify the claim to legitimacy of systems such as Bitcoin, which is likely to explain why these systems are being supported. Then, algorithmic authority favors some governance and management processes rather than others (see infra). After having examined the previous accounts of the notion of algorithmic authority found in the literature, it is necessary to spend a few words on the philosophical underpinnings of distributed consensus systems before providing a definition.

In the context of blockchains and distributed ledgers, discretion and ambiguities are seen as undesirable features of current arrangements of authority. Since 2008, this philosophical stance was

made clear by Nakamoto: "We proposed a system for electronic transactions without relying on trust" (Nakamoto, 2008, p. 8). Trust entails risk, and uncertainty. What makes trust a risky business is, in the mind of blockchains proponents, the possibility of manipulation that results from the discretionary nature of traditional institutions. The problem is sometimes considered as 'time inconsistency' to signify that the goals of institutions or a third party can diverge from the goals of the users of the system (Craig & Kachovec, 2019). Hence, according to this position discretion is a bug, not a feature. The solution is then straightforward, design a system of hard-coded rules individuals can submit to. Ethereum's Joseph Lubin justified this conclusion by stating that "[t]here will be ways to manipulate people to make bad decisions, but there won't be ways to manipulate the system itself"[45]. With this philosophical stance in the background, we are now in the position to provide a more precise definition valid for our purpose.

Algorithmic authority is an extension of the pure type of rational-legal authority that grounds the legitimacy of a system of imperative co-ordination on the use of transparent, open, decentralized, tamper-proof algorithms that implement normative rules. Obedience is hard coded in the technical infrastructure and, thus, misbehavior is rendered virtually impossible by the system's architecture. As with other ideal types, algorithmic authority in its pure form is found nowhere in the real-world. However, this is not a valid objection to attempting its conceptual formulation in the more precise way possible. The usefulness of the category of algorithmic authority is, like the classical Weberian pure types, justified by its results in promoting a systematic analysis imperative co-ordination systems. This notion is also s useful methodological tool to study the phenomena at hand which provides relevant insights to answer the question posed in the introduction of this work: why do agents

[45] http://www.theepochtimes.com/n3/665367-bitcoin-2-0/ accessed on the 4th of September 2019.

engage with distributed consensus systems? The next section provides an elucidation of the salient ideas on which the belief in the legitimacy of the rule of algorithms is grounded.

7.2 The Elements of Algorithmic Authority

Since the beginning, blockchains and distributed ledgers have proposed a novel way to solve the cooperation problem by disintermediation or decentralization. The narrative often compares powerful, old, and untrustworthy intermediaries as a nexus of centralized power versus new, distributed networks where trust has been replaced by reliability in the technology (De Filippi, 2018). The underlying assumption is that intermediaries or trusted third party impose an unacceptable cost on individuals along with other risks (Locher, Obermeier, & Pignolet, 2018). For example, Bitcoin promises money without banks and a mechanism to allow individuals to escape inflationary monetary policies, and credit bubbles. Beyond decentralization and disintermediation, there are other important elements for the current analysis. The aim of this section is to expose such elements by exploring the ideas that ground the belief in the authority of algorithmic systems.

The first is that decentralized is better than centralized because centralization is inherently risky and results in the hindrance of individuals' goals and rights (Baldwin, 2018). The second idea is that the flattening of power structures is a consequence of the network topology. In other words, the architecture of the network reflects the political distribution of power. The assumption here is that a structural form without a center, i.e., the distributed network, enables a similar distribution of biopower (Galloway, 2004; Pagallo, 2008). This idea traces back to the early P2P movement and has risen to prominence again with the advent of blockchains. According to this position, "since new communication technologies are based on the elimination of centralized command and hierarchical

control, it follows that the world is witnessing a general disappearance of control" (Galloway, 2004, p. 8). However, power persists and in the case of algorithmic authority it is exerted via the protocol.

There are no formal structures outside the system, no legal entities, and no body of representatives, the impersonal order is implemented by the network. Users are only bound to the network by the protocol. This form of authority is exerted impersonally, obedience is always guaranteed by the inexorable execution of the network's operation, and it is never impersonated. Accordingly, algorithmic authority does not have offices or a bureaucracy; it is self-enforcing. Obedience is only granted to the protocol. For this reason, systems that have legal entities tasked with the development and marketing – as in the case of Ethereum - are to be considered more distant to the pure form of algorithmic authority rather than other systems, e.g. Bitcoin. Another idea is that individuals are not forced to join the system, nor the authority of algorithms is imposed against anyone's will. Contrary to the real-world, where individuals cannot escape the subjection to authority, this type of imperative co-ordination is always chosen. This mitigates the fact that the operations of algorithmic authority cannot be reverted, and no mechanisms are in place to remedy its outcomes.

The fourth idea is that the exercise of power is deterministic. Algorithmic authority is as algorithmic authority runs. In its pure form, discretion is removed, that is, the operations and outcomes can be determined ex-ante and do not require ex-post adjudication. In this sense, obedience is trustless for there is no uncertainty; individuals are put in the position to know in advance all the possible outcomes. Complexity is thus reduced by substituting trust with control (Luhmann, 1979). Consequently, algorithmic authority requires full transparency of its protocols. All the rules of the network must be 'out there' for individuals to inspect. Algorithmic authority is a transparent box. Everyone is allowed to witness the operations of the network when it comes to transactions or computations; in this sense, a record of all the activities of the network is necessary. This is achieved by allowing everyone with an internet connection to read the content of the network. Full transparency is another idea on which algorithmic authority rests. Transparency, however, might be undesirable

for individuals. Therefore, this type of authority heavily relies on cryptography to protect individuals' identity and privacy. In its pure form, algorithmic authority does not need to know who everyone is because its operations are agnostic to it. Users are entrusted with the keys [in the sense of public-key cryptography] to access the network and enforcement occurs not on individuals but on hexadecimal strings. The protocol does not need to know who everyone is, everyone can join or leave the network at will. There is no process of recognition, no requirements needed to participate because the network is solely concerned with pseudonymous identities.

The pure form of algorithmic authority does not require administration in the form of a bureaucratic staff. The work needed to maintain and update the network is purely voluntary. Everyone is allowed to propose changes and participate in the maintenance of the network. Coordination is achieved loosely and without central intervention. There is no training required to participate in the contribution process in a formal sense. However, specialized knowledge is often needed to make meaningful contributions due to the highly technical nature of the discourse. The maintenance process does not follow a hierarchical structure, and there is no right of appeal and who disagrees can 'vote with their CPU' and abandon the network or create a new one. The same applies for the update process. There is no clear sphere of competence among developers and privileges are earned on the basis of meritocracy. The normative sources of systems of algorithmic authority are core protocols written in computer code. While natural language may often be used to coordinate the community computer code is the ultimate source of rules. What cannot be executed lies outside algorithmic authority in its pure form. The network enforces only the rules written in computer code; therefore, ambiguity and uncertainty are considerably reduced. In this sense, code is the only source of law, not a concurring constraint on individual choices.

The previous paragraphs outlined the ideas on which the acceptance of algorithmic authority rests. It appears that the imperative co-ordination by/with algorithms is diverse enough to be distinguished it from the Weberian pure types of traditional, charismatic and rational-legal authority.

With regard to the phenomenon of distributed consensus systems, algorithmic authority better captures the rationale used to cultivate the belief in the legitimacy of using a distributed network to regulate individuals' behavior. To better understand the success of blockchains networks it is useful to dedicate a few words on the history of algorithmic authority by examining the attempts to create a digital version of cash. Cash is taken as an example of how some of the core ideas, on which algorithmic authority rests, develop. Arguably, the same process is unfolding with regard to crucial legal constructs, namely, contracts and corporations.

7.2.1 The roots of algorithmic authority

It is not clear if there is a link between the release of Bitcoin and the 2008 financial crisis. However, in the literature, this is often suggested. For example, Baldwin argues that"[t]he bailout of the banks in response to the crash of 2008 - a socialist solution to a capitalist problem - is suggested to be crucial in the impetus behind bitcoin" (Baldwin, 2018, p. 3). Hutten seems to take the link for granted when he writes "It [Bitcoin] was developed as a peer-to-peer payment system to challenge central bank control and the incumbents of the global financial system" (Hütten, 2018, p. 1).

The fact that the genesis block of Bitcoin contains the headline from the Financial Times of the 3rd of January 2009 also seems to support this view[46]. However, the project of a currency for the a-political internet had been in the works long before Bitcoin's release (Popper, 2015). On this basis, it appears that the foundations of algorithmic authority were put in place long before the financial crisis. The idea that technology is a legitimate way of exerting power, monetary power in this case,

[46] To be precise the Bitcoin genesis block contains the following string The Times 03/Jan/2009 Chancellor on brink of second bailout for banks.

goes back a long way before the first blockchain system was implemented. This is the root of algorithmic authority.

Cyber-libertarians attempted to create a digital version of cash since the '80. David Chaum spearheaded the efforts which led to the creation of digicash, while Wei Dai speculated the creation of Digigold. In the end, none of the previous efforts turned out to be successful until Bitcoin, which - unsurprisingly - heavily borrows on previous attempts. The roots of a new type of authority where already in place, governments and institutions couldn't be trusted to fully guarantee property rights and safeguard financial privacy with the advent of the digital revolution (Chaum, 1997) . An 'escape' from politics was needed: technology appeared to provide the answer. In fact, the roots of algorithmic authority go back to the libertarian ideology that perceives technology as a solution to pre-existing institutional arrangements (Golumbia, 2016). A common thread is the attempt to eliminate ambiguities and ensure that decisions are not made but executed. It was believed that technology could then remove control from existing institutions and put it in a transparent, predictable, infrastructure. What Hayek sought to achieve by privatizing money issuance, that is, remove governments' monopoly over money issuance, cyber-libertarian did by using technology (Von Hayek, 2009). However, while Hayek argument builds on economic reasons, the push to adopt technology to ‘regulate’ the issuance of money rests on different grounds, although it must be noted that there is some overlap.

According to cyber-libertarianism, governments and other institutions cannot be trusted to act in the interests of the citizens, for example Nakamoto writes "[t]he central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they land it out in waves of credit bubbles with barely a fraction in reserve" (Nakamoto, 2009). The central point is that p2p open-source technology cannot act against the interests of the people who subject themselves to its control. On the contrary, governments and institutions might act in their self-interest which might be misaligned with

citizens. More importantly, however, their self-interest could be hidden from public discourse. Therefore, as long as the technology is distributed among a p2p network, transparent, accessible, and secure, it can be considered as the foundation of a new legitimate exercise of power: algorithmic authority. In the following section, it will be examined if the core ideas on which algorithmic authority hinges are uphold in the context of current distributed consensus systems. As noted in the previous chapter, current systems establish their imperative co-ordination also on elements proper of traditional, charismatic and rational-legal types of authority; this is necessary because crucial ideas on which algorithmic authority rests are simply violated by current systems. So that one observes a paradox, namely, proponents of these systems advocated their use and adoption also on the basis of the characteristics that these systems ought to have but currently do not possess.

7.3. The Current Situation

This section aims to analyze how current systems are failing to uphold the ideas on which the pure type of algorithmic authority rests. The first idea under consideration is decentralization.

7.3.1 Decentralization

The first idea that current blockchains struggle to uphold is decentralization. Distributed consensus systems, and in particular blockchains, are portrayed as decentralized systems while, in reality, they are not. Nonetheless, advocates of the technology still contend that decentralization is what allows Bitcoin to substitute an army of computers for an army of accountants, investigators, and lawyers. The fact that decentralization is a vital element of blockchains has been pointed out in the

academic literature as well, Walch writes "[t]he concept of 'decentralization' is a foundational, infrastructural one for blockchains" (Walch, 2019a). There is a lot of confusion about decentralization out there. It is known that the notion of decentralization is hard to define (UNDP, 1999). The next paragraphs attempt to establish a first definition of this essentially contested concept.

Mr. Buterin adopts a tripartite distinction which offers a good starting point, not because it is particularly correct or insightful but because it represents the multifaceted understanding of this concept within blockchain communities. Buterin distinguishes three types of decentralization: architectural, logical, and political. Accordingly, architectural decentralization means "how many physical computers is a system made up of?", political is intended as "how many individuals or organizations ultimately control the computers that the system is made up of?", and - lastly - logical decentralization depends on knowing if "the interface and data structures that the system presents and maintains look more like a single monolithic object, or an amorphous swarm?" (Buterin, 2017).

To simplify our discourse, we can think of only two facets of decentralization: technical and political. The former concerns the technical aspect of the network, that is, the protocol, and it comprises both architectural and logical decentralization. The latter refers to the human-touch needed for protocol management. To recall a distinction introduced earlier in this work, technical decentralization operates at the level of the governance by/with the network while political decentralization at the governance of the network level (see chapter 4).

Most blockchains are logically decentralized. Byzantine fault tolerance implies that systems must be able to tolerate nodes joining and leaving the network unpredictably. Split Bitcoin in half and the system will continue to function, the same goes for other popular blockchains. As per the number of physical computers, it depends on each network. In the case of the most popular systems, it is fair to say that they are, indeed, architecturally decentralized. At the time of writing, there are 9.297 reachable Bitcoin nodes, 7.348 Ethereum nodes, and 1.199 Litecoin nodes to take a few prominent

examples[47]. Another critical aspect of architectural decentralization is geographical distribution because full decentralization seems to imply a broad geographical distribution. Most popular blockchains appear to be geographically distributed enough to be considered decentralized in this sense. Thus, it is possible to conclude that blockchains are technically decentralized systems. So far so good.

However, problems arise when examining the political decentralization of blockchains. Different elements are relevant in this regard. First, there is the distribution of mining power which, in most blockchains, is not decentralized. The distribution of mining power is correlated to the facet of political decentralization because miners play a key role in the governance of networks, hence, a highly concentrated mining distribution might rule out political decentralization (Wang, Chu, & Yang, 2019; Wu et al., 2019). Second, the distribution of coins while difficult to assess precisely, appears to be heavily concentrated so that a few entities control most of the coins in circulation. Third, most of the contributions to the codebase of blockchains have been submitted by a few individuals (Azouvi, Maller, & Meiklejohn, 2018). The same is true for the developers that have commit access to the official repository of major blockchains. Fourth, some systems such as Zcash, and EOS were developed by for-profit legal entities, a circumstance that appears to rule out full political decentralization. These dimension of centralization, neatly excluded by Buterin's account, are essential to account for the real degree of decentralization of a distributed consensus system. Decentralization, both technical and political, does not seem impossible to achieve with proper techniques as, for example, secondary rules of change and perhaps of recognition of the principle of decentralization. However, it might be necessary to trade-off a certain degree of decentralization to

[47] Data collected on the 24th of October 2019 from the following sources. https://bitnodes.earn.com/; https://www.ethernodes.org/; https://litenodes.org/.

ensure the effectiveness of distributed consensus systems. A tentative proposal, along with a further analysis of the proper dimensions of decentralization is postponed to the next chapter.

7.3.2 Network

Another crucial idea on which the belief in the authority of algorithmic systems rests is that the topology of networks demands a specific arrangement of power, i.e., a centralized network entails a centralized governance structure while a distributed one disperses power among its peers. The belief that the technical infrastructure of the network leads to a similar arrangement of the power structures that govern it has been successfully subject to various critiques. Since Galloway, it has been clear that political distribution is not a consequence of distributed networks. Similarly, a centralized network might not be the result of centralized power. In other words, it appears that the topology of networks is not correlated with the distribution of power that governs them, in fact, it would be surprising if the opposite were true. Therefore, it seems that the claim of distribution of powers through architectures does not stand critical scrutiny, both empirical and theoretical.

With respect to the theoretical level, it appears that architectures are not capable of encompassing the full spectrum of individuals' interactions. The points of contact between the networks and other social systems (such as the market and the law) can become nexus of centralized power. In the case of blockchains, contrasts between the code of blockchains and off-chain activity might lead to undermine an entire system (DuPont, 2017). It seems necessary to recognize that, at the theoretical level, the network topology is not capable to completely constrain the aggregation of powers 'on' the network.

Concerning the empirical level, it is enough to note that technically distributed – and perhaps decentralized – systems can become subject to centralized control as in the case with most distributed consensus systems. Think for example, of the internet and how a distributed network enabled an unprecedent concentration of power in a few companies. Architectures alone are not capable of imposing power structures for the real issue is who sets the rules of the network. Then, it is crucial to ensure that off-chain mechanisms are put in place to prevent or manage undesired dispersions or accumulations of power.

7.3.3 Politics

A third idea on which algorithmic authority rests is that the technology is politically agnostic, that is, technical systems are not conducive to specific ideologies, rather they are just tools for co-ordination impervious to political ideals. Accordingly, blockchains and distributed ledgers are a neutral technology. In the context of the governance of blockchains in Europe, Finck states that "[i]n and of themselves, blockchains are a neutral technology. Just like any technology, they can therefore be manipulated to be operated for good or for bad" (M. l. Finck, 2018, p. 33) However, some authors argue that blockchains are inherently political (De Filippi & Loveluck, 2016; Herian, 2018a; Scott, 2015; Velasco, 2017). To address this contrast some background is needed.

In 1980 Langdon Winner posited the idea that technical things - or artifacts - possess political qualities (Winner, 1980). He provided an example of how architecture was used to discriminate access to Jones Beach by urban planner Robert Moses and how McCormick's molding machines were used to destruct the workers' union to show how technological artifacts embody political dimensions. He also argued that some technological devices are inherently political due to their characteristics, in this regard he gave the example of the centralized, rigidly hierarchical chain of command demanded

by the existence of the atom bomb. Concordantly, concerning a given technology two scenarios are possible. On the one hand, some technologies could enable means of establishing patterns of power and authority when deployed. On the other hand, some other technologies demand specific arrangements of power and authority. This is often due, as in the case of the atom bomb, to the characteristic of the technological artifacts. The question then becomes if algorithmic authority in the context of distributed ledgers demands a specific arrangement of power or not.

The answer is negative. When it comes to blockchains, it is clear that we are not dealing with a technology of "intractable properties [...] strongly, perhaps unavoidably, linked to particular [...] patterns of power and authority" (*ibidem*, 134). Blockchains are distributed P2P networks akin to the TCP/IP architecture of the internet. However, the internet, as a technological artifact does not demand any particular arrangement of authority. Case in point, it enabled the libertarian dreams of the early P2P movement as well as allowing for the establishment of quasi-monopolistic players that have come to dominate the internet economy, and the so-called surveillance capitalism. Along the same lines, the belief on which algorithmic authority rests enable different patterns of power and authority and demand none. So that, different technical infrastructures can cultivate their legitimacy on the same ideas without necessarily sharing the same political commitment. This is because the focus is on the operations of systems rather than its political qualities, thus patterns of power and authority depend on design choices and implementations of technical solutions along with governance structures. However, the previous argument does not imply that blockchains and other distributed consensus systems are not conducive to particular patterns of power and authority, perhaps inspired by a specific ideology. Therefore, even if these technologies are not linked to a predetermined pattern of power and authority it does not follow that they are just neutral. This is apparent in the case of Bitcoin.

Brett Scott highlights the ambivalent nature of the 'disintermediation' by Bitcoin. He writes "[t]hose with a left-wing, anarchist bent, who perceive the state and banking sector as representing

elite interests, may recognise the potential within Bitcoin for collective direct democratic governance of the currency. However, it also really appeals to conservative libertarians who perceive Bitcoin as a commodity-like currency, free from the evils of a central bank and regulation" (Scott, 2015, p. 2). The ambivalent allure of Bitcoin, argues Scott, is not of a realm lacking the rules imposed by the state but of one imposing its own rules, hence, his perspective corroborates the claim that particular implementations of blockchain technology embody different political visions represented by their distinct sets of rules implemented in their protocols.

Golumbia argues that Bitcoin embodies the principle of cyber-libertarianism. He writes, "Bitcoin and the blockchain technology on which it rests satisfy needs that make sense only in the context of right-wing politics" (Golumbia, 2016, p. 16). In his writing, Bitcoin and the blockchain code right-wing political values directly into the software itself. Therefore, the blockchain is regarded as an inherently political technology suited for right-wing ideologues with a propensity to conspiracy thinking. Toward the end of his book, Golumbia seems to acknowledge that the problem does not lie with the technology but rather with a particular design, he writes "[t]his is not to say that Bitcoin and the blockchain can never be used for non-rightist purposes, and even less that everyone in the blockchain communities is on the right" (*ibidem*, p. 57). It seems that the jury is not out on the ideology that blockchains like Bitcoin embody. At the time of writing, distributed consensus systems are politically underdetermined. For example, Eich writes: "[b]lockchain algorithms are made and reflect the political intentions of their authors. There is nothing inherent in blockchain technology that rules out centralization, regulatory oversight, or democratic governance, be it by central banks, commercial banks, or other providers that benefit from network effects"(Lianos, Hacker, Eich, & Dimitropoulos, 2019, p. 85).

Systems of algorithmic authority do not demand a specific arrangement of power. Consequently, it is delusional to expect that a distributed P2P network with an undefined governance structure will result in an egalitarian utopia, as it has already been noted in the context of P2P network

(Pagallo, 2008). Then, the normative value of distributed consensus systems depends on the content and operations of their algorithms as well as sound governance processes. In conclusion, the issue becomes the development of principles to which each system ought to adhere.

7.4. The Law of Algorithmic Systems of Authority

Distinct beliefs in the legitimacy of a system of imperative co-ordination shape their legal structures. Weber described this influence in the context of his three types of legitimate authority. He wrote that the effectiveness of rational-legal authority rests on the acceptance of the validity of the idea that "every body of law consists essentially in a consistent system of abstract rules which have normally been intentionally established. Furthermore, administration of law is held to consist in the application of these rules to particular cases; the administrative process in the rational pursuit of the interests which are specified in the order governing the corporate group within the limits laid down by legal precepts and following principles which are capable of generalized formulation and are approved in the order governing the group, or at least not disapproved in it." (Weber, 2012, p. 330). Before proceeding, it is useful to describe the other modes of law enabled by the pure types of Weberian origin, namely, traditional and charismatic authority to show precisely how different beliefs in the legitimacy of a system influence its legal structures.

Regarding traditional authority, formal principles are not present. While it is possible for law or administration to be enacted by legislation, the process differs from the rational-legal deliberative one. Weber stated: "[w]hat is actually new [law or administration] is thus claimed to have always been in force but only recently to have become known through the wisdom of the promulgator. The only documents which can play a part in the orientation of legal administration are the documents of tradition; namely, precedents." (Weber, 2012, p. 342). Interestingly, concerning the scalability issue

of Bitcoin new proposed solutions are often claimed to be 'always been there' in the philosophy of Nakamoto, a fact that points to the shift of Bitcoin from the algorithmic to the traditional type of authority.

Systems of charismatic authority also have distinct legal characteristics. Weber notes how charismatic authority is "specifically outside the realm of everyday routine and the profane sphere. In this respect, it is sharply opposed to both rational, and particularly bureaucratic, authority, and to traditional authority, whether in its patriarchal, patrimonial, or any other form." (Weber, 2012, p. 361) Therefore, the typical legal system established by it has the following properties. First, there is no definite sphere of authority and competence, and no appropriation of official powers on the basis of social privileges. Second, there is no system of formal rules or abstract legal principles formalized in general provisions. So that, no process of adjudication is oriented to the enforcement of norms. In his words: "[f]ormally concrete judgments are newly created from case to case and are originally regarded as divine judgments and revelations" (Weber, 2012, p. 361). Accordingly, the next section attempts to describe the normative structures proper of systems based on algorithmic authority.

7.4.1 ≠ Techno-Regulation

The normative functions of algorithmic authority are merely executed by a network of computers. In this sense, the binding norms correspond with protocols and algorithm, i.e., code. Therefore, they might be described as techno-regulatory orders. However, these systems differ from state-led techno-regulatory initiatives because a core idea of systems based on the authority of algorithms is that individuals are always free to escape it because it is never imposed, and full transparency is a vital feature. However, a brief outlook of techno-regulation is in order to distinguish it from the law of algorithmic systems of authority.

According to Roger Brownsword: "the ideal-type of techno-regulation is instantiated regulators, having identified a desired pattern of behaviour (whether morally compliant or not), secure that pattern of behaviour by designing out any option of non-conforming behaviour. Such measures might involve designing regulatees themselves, their environments, or the products that they use in these environments, or a combination of these elements. Where techno-regulation is perfectly instantiated, there is no need for either correction or enforcement." (Brownsword & Yeung, 2008, p. 247). The core idea is removing the space of non-conformity by using technology. The same aspiration is found in the claim of algorithmic authority on the determinism of its operations with a crucial difference. In this case non-conformity is designed out both for regulators and regulatees alike. For example, Bitcoin's protocol is said to protect users from central banks.

In this sense, distributed consensus systems are techno-leviathans that bind both the structure that exert power, i.e. the protocol, and the users. So that, in the context of blockchains and distributed ledgers, techno-norms do not aim to secure "desired pattern of behaviour" on regulatees; rather, regulatees can implement limitations in the architecture so that power is limited. Based on this conceptual shift, it is interesting to examine if the same concerns voiced by Brownsword in the context of state-led techno-regulation still apply to systems of algorithmic authority.

According to Brownsword, techno-regulation may undermine moral communities. He argues that the legitimacy of techno-regulation comes down to respect for human rights and human dignity. Because the aspirations of a moral community hinge on the autonomy of choice. Then, techno-regulation poses the threat of "seemingly abandoning the importance that we attach to the dignity of choice and, with that, much of the basis on which our thinking about responsibility, as well as rights, is premised" (Brownsword & Yeung, 2008, p. 47). The stakes are clear: techno-regulation might hinder the cultural environment in a way that is undesirable for a moral community and which may lead to a moral void. The risks outlined by Brownsword are real when it comes to state-led techno-regulation. However, this is not the case in the context of systems of algorithmic authority.

It seems that individuals retain their moral determination by choosing among different systems of technological rules and by retaining the possibility to choose among different techno-regulatory solutions. It is important to note that the participation in a system of algorithmic authority is always voluntary, so that the dignity of choice is preserved by allowing individuals not to non-conform but to choose in advance their set of constraints under the conditions of transparency and deterministic execution, two characteristic that are central to the belief in the legitimacy of systems such as blockchains and distributed ledgers. Therefore, it might be argued that Brownsword's main concern for the legitimacy of techno-regulation does not apply because autonomy of choice is preserved by allowing individuals to choose their set of constraints. There are other risks related to techno-regulation.

Hildebrand noted that "self-rule, disobedience, and contestability are the hallmarks of law in a constitutional democracy", so that in her view techno-regulation is a "form of administration or discipline rather than law" (Hildebrandt, 2011, p. 248). She focuses her analysis on the deployment of techno-regulation from State and private parties. In this context, she developed the methodology of legal protection by design, that is, "a way to ensure that the technological normativity that regulates our lives: first, is compatible with enacted law, or even initiated by the democratic legislator; second, can be resisted; and third, may even be contested in a court of law" ((Hildebrandt, 2015, p. 218). In her view, the fundamental requirements of 'resistability' and contestability must be translated into technical requirements. Her argument holds some water in the context of algorithmic authority, but conditions apply.

Algorithmic authority is built on individuals' ability to choose their set of rules and on voluntarily subjection, i.e., "lego-Mindstorms for building economic and social institutions" (Buterin, 2014). So that the requirements of resistability and contestability might be shifted to an earlier moment compared to state-led techno-regulation. This is possible because all the rules are transparent, their formation is open to all, and agents are always free to leave these systems. What is more is that

blockchains architecture seem to allow for rules developed according to some of the elements of legal protection by design. It is also important to know that the spirit of blockchains has always been democratic and participatory in nature so that freedom to choose among different systems as well as the ability to fork are crucial in explaining why agents believe in the authority of algorithmic systems. Having examined why risks posed by traditional techno-regulation are not particularly problematic in this context it is interesting to describe, from a legal perspective, the type of techno-regulatory norms implemented within systems such as blockchains and distributed ledgers.

Leenes distinguishes between state techno-regulation from non-state techno-regulation. He regards state-led techno-regulation as a legitimate instrument to achieve policy goals "under condition of paying adequate respect to human rights, offering choice, providing for transparency, and adhering to accountability" (Leenes, 2011, p. 159). Techno-regulation by/with blockchain does not fall into this category, yet. Therefore, distributed consensus systems fall in the context of non-state techno-regulation. Leenes writes: "[w]hen it comes to private rulemaking, which is what non-state techno-regulation is about, regulatory power has to be passed from the sovereign state to private parties" (*ibidem*, p. 161). Leenes then considers contracts as a suitable legal mechanism to provide the legal basis of non-state techno-regulation. However, he recognizes that a legal basis for techno-regulation might be absent altogether; this is the case in our context. When users decide to join a network, it seems that no contractual basis can be inferred to justify the use of techno-regulation, in particular, because it is not clear at all who will be the other(s) party(ies) of the contractual relation. Additionally, the two other instruments for the transfer of powers from the State to private parties discussed by Leenes do not apply to blockchains. For no terms-of-use are generally in place, and undoubtedly legislation does not transfer the power to regulate to blockchains and distributed ledgers. This is not an issue. The justification for the techno-regulation of distributed consensus systems is found in the individuals' autonomy.

For Leenes, one crucial element is the distinction between "is" and "ought" in private techno-regulation. He contends that transparency of the norms is essential and that, consequently, "given the fact that the norms often seem to be opaque, their validity also seems questionable" (*ibidem*, p. 165). Yet, transparency is a paramount principle of algorithmic authority. Then, such systems offer users the possibility to opt in transparent and deterministic techno-norms, thereby safeguarding the option of individual choice. Leenes also notes, and I agree, that "[p]rivate regulators may earn legitimacy by the regulated community by engaging this community in deliberate discourse. This requires a free flow of unhindered vital information" (*ibidem*, p. 167). In conclusion, according to Leenes' perspective blockchains and similar systems are private techno-regulators that, consistently with the beliefs that cultivate their legitimacy, can constrain agents with techno-regulation on the basis of their autonomy of choice. Importantly, a flow of information is needed to earn legitimacy (in the legal sense of validity). On this basis, the next section examines the literature on the techno-regulatory structure of distributed consensus systems, i.e. the law of blockchains.

7.4.2 Perspectives from the literature

This section provides a brief review of the literature on the law of blockchains as determined by the belief in the authority of algorithms. The terminology around this concept is, as expected, imprecise. Some authors refer to the law of algorithmic authority as lex criprographica while others use the term cryptolaw albeit with different meanings.

De Filippi and Wright studied the normative operations of blockchains (Wright & De Filippi, 2015). They considered the legal structure enabled by blockchains as a form of private ordering that they named lex cryptographica. In their account, blockchains enable order without law by implementing private regulatory frameworks that individuals can choose to deploy to regulate legal

relationships among themselves. From a theoretical perspective, lex cryptographica is akin to contract law as it allows individuals to regulate aspects of their legal affairs without relying on legislation. De Filippi and Wright, argued that lex cryptographica is different because "blockchain-based applications do not depend on these rules [law] to structure their functions; instead they depend on lex cryptographica to organize economic and social activity" (De Filippi, 2018, p. 6). Because of the properties of blockchains, they continue, lex cryptographica is distinguishable from the code is law of Lessigian origin. They write: "lex cryptographica shares certain similarities with the more traditional means of regulation by code. Both purport to regulate individuals by introducing a specific set of affordances and constrains embedded directly into the fabric of a technological system. Lex cryptographica, however, distinguishes itself from today's code-based regimes in that it operates autonomously - independently of any government or other centralized authority." (*ibidem*, p. 207). However, it is difficult to understand how this instance differs from other code-based private regulatory efforts as, for example, the ones carried out by popular internet platforms. Surely, one cannot argue that the autonomous nature of lex cryptographica operates unbound by any legislation. This confusion is likely the result of their attempt to establish a concept similar to that of lex Informatica developed by Reidenberg along with subsequent integrations and modifications (Reidenberg, 1997). Yet at the end of their work, De Filippi and Wright recognize that "[b]lockchain-based systems can be controlled in areas where they intersect with regulated entities - such as individuals, network operators, and all those intermediaries who either develop or support the technology. New intermediaries servicing blockchain-based networks are already beginning to emerge [...] So long as these intermediaries remain subject to the rule of law [...] governments will be able to enforce their laws, either directly or indirectly" (De Filippi, 2018, p. 208). On this basis, it is not clear what distinguishes lex cryptographica from lex Informatica.

Reyes uses the term cryptolaw when discussing the normative structures of blockchains and distributed ledgers. She defines cryptolaw as "the new jurisprudence that will emerge as a result of

implementing and delivering the law of any subject matter through smart-contracting, semi-autonomous, intelligently developing cryptographic computer code" (Reyes, 2017, p. 399). In her view, cryptolaw will emerge as a new form of legislation when governments use distributed ledgers technologies to make law: "[c]onceptualizing cryptolaw requires envisioning a world in which law is created first through legislation or regulation written in words and then implemented through cryptographic, smart-contracting computer code" (*ibidem,* 400). Therefore, cryptolaw is an accessory to traditional law as it is conceptualized as an enforcement mechanism to supplement current legal structures and norms. This is clear when examining the three ways in which Reyes believes cryptolaw will arise (a) by private legal structures adopted by governments, (b) through direct development of crypto-legal structures by governments or (c) by the international development of crypto-legal structures. I am skeptical of this account of crypto law as it presupposes for its very existence, the necessity of governments' adoption of blockchain-based technology. In the current landscape, it is not clear that such an event will occur and, moreover, blockchains do not appear applicable in many areas of law (Low & Mik, 2019; Mik, 2017).

Among the publications of the Crypto Law Review, one finds a different account of cryptolaw, i.e., the normative structure of distributed consensus systems. According to this perspective cryptolaw is "the body of on-chain and off-chain enforcement, execution, implementation rules for these new digital instruments and new types of digital markets [blockchains]" (CleanApp, 2018b). Cryptolaw builds on the quasi-legal notion of smart contracts intended as legal obligation formed on some blockchain process; these automatic processes are perceived as faster, cheaper, and more predictable than ambiguous contracts. In this sense, cryptolaw "is an attempt by some actors to distill and crystallize an objective & deterministic body of crypto legal forms and crypto rules" (*ibidem*). Zamfir identifies another aspect of cryptolaw. He believes that legal systems are protocols for the management of disputes, therefore, since disputes arise within blockchains, cryptolaw exists, and it coincides with the protocols adopted for managing them (Zamfir, 2018).

On this basis, the next section departs from the previous formulations to provide a distinct account of the normativity of systems of algorithmic authority. In the rest of this work, the term cryptolaw will be adopted to describe, at a conceptual level, the characteristic of the law of systems that establish their authority on the elements outlines above in section 7.2. In other words, the next section describes the elements of the pure-type of cryptolaw.

7.4.3 Elements of normativity

There are four salient features of cryptolaw divided in two categories. The first category concerns the execution of norms. In this category, there are two elements, namely, determinism, and reduction of ambiguities. The former refers to the possibility of precisely determine ex-ante the law of the system. The idea behind this first category is to allow agents to adopt 'predictable' rules. Emblematic in this regard are smart contracts. When deploying smart contracts, parties are in the position to precisely determine ex-ante how their future legal relationships will be managed. There is no need for ex-post adjudication, nor for third-party execution. Contracts become self-executing because there is nothing to decide or adjudicate; all the elements for the performance are already in the contracts. Therefore, the reasoning goes, the risk is reduced, and the costs of enforcement are eliminated. Accordingly, the law of algorithmic authority is predictable because it computes in a deterministic fashion.

Naturally, determinism requires the reduction or elimination of ambiguities for they introduce non-determinism in the operations of the system. Moreover, ambiguities are reduced because of the particular medium in which this form of law is expressed, that is, computer code. Code is the only language that does what it says. Therefore, there is no room for open standards such as due diligence, best effort, or other open concepts used abundantly in the legal practice. Generally, what cannot be

expressed at a reasonable cost in binary logic does not belong to cryptolaw. The medium in which the law is expressed, then changes from writing in natural language to computer code in the human readable form (before the code is compiled).

Another element proper of Cryptolaw are cryptographic assets, i.e. crypto-assets. These come mostly in the form of cryptographic 'unique' digital tokens that are created and exists only onto distributed consensus systems. The typical example is the standard contracts developed by the Ethereum community, so-called ERC standards[48]. ERC specify contracts under cryptolaw by providing standards for users to regulate their legal relationships. These standards are the typical contracts under cryptolaw, examples include ERC-20 or standard interface for tokens, ERC-721 for non-fungible token standard, and ERC-1155 for the management of multiple token types. Other types of assets created by crypto legal forms are cryptocurrencies, however, the trend toward the tokenization of physical assets points to the fact that cryptolaw is increasingly being used to manage an increasing number of assets.

Transparency and voluntary subjection belong to the second conceptual category. The first element is a corollary of the previous category for determinism requires the ability to inspect cryptolaw both in its source code (human-readable) and compiled code (machine-readable). Transparency of the normative operations of blockchains and distributed ledgers follows from the fact that this idea is foundational in the cultivation of the legitimacy of these systems. Further, transparency is required for the operations of cryptolaw and its execution, not for its subjects which are normally pseudonymous entities, in accordance with the openness of these networks. Further, the process of 'enacting' cryptolaw is carried out on platforms that enable version control and allow anyone to submit proposals and to comment on ongoing initiatives.

[48] ERC stands for Ethereum request for comments.

The last element of cryptolaw is voluntary subjection. In this sense, cryptolaw is never imposed but only chosen by autonomous and pseudonymous agents. Voluntary subjection is a crucial element of cryptolaw because due to its mode of operations, the execution of norms cannot be stopped or modified by any party. This is necessary because as Luhmann noted "obedience to all laws, all of the time, would paralyse self-determination" (Luhmann, 2004 p. 50), then self-determination within cryptolaw is anticipated to the moment in which individuals decide to bind themselves to deterministic, open, and transparent norms. Norms cannot be violated because deviant behavior is prevented at the protocol level, and the violation and its consequences cannot be contested anywhere because of the material impossibility of the violation.

7.5 Conclusion

This chapter aimed to qualify the pure-type of algorithmic authority with a focus on its core elements and legal operations, i.e. cryptolaw. It appears that the characteristics described above are the reasons why agent consider blockchains and similar systems as legitimate. The next chapter further explores the notion of cryptolaw before turning its attention to the subject of decentralization to exemplify how systems of algorithmic authority ought to preserve their legitimacy.

8. Implications

Blockchains and distributed ledgers are among the technologies that challenge our understanding of legitimate authority by exerting power via algorithms. The rise in the belief of the legitimacy of algorithmic systems of rules raises several issues. These issues belong to existing systems such as Bitcoin and Ethereum but may also affect new initiatives such as the European Blockchain Service Infrastructure. While it is not clear if blockchains are here to stay, it is likely that core ideas on which the belief in the authority of algorithms rests are, e.g. distribution of power via networks, transparency of algorithms, decentralization and so on. Therefore, one may wonder if decentralization is and end in itself or, as it seems, should be regarded as a way of distributing power when certain conditions are met. Moreover, to what extent decentralization ought to be pursue is a question that needs to be addressed. Is, for example, the carbon footprint of Bitcoin justifiable because it enables decentralization?

Critical challenges for blockchains and distributed ledgers appear social rather than technical. Some might object to this statement as it is not uncommon for developers and designers to consider the issues troubling blockchain and distributed ledgers as purely technical. In fact, most of the focus has been put to improve the technical aspects of systems while little attention has been put to the social aspect of these technologies (Casino et al., 2018). That said, while there is no shortage of technical improvements for blockchains, existing systems have not changed significantly since their first implementations. The next pages examine two aspects that are likely to have a significant impact in blockchains' development with the goal of providing suggestions and future research directions.

This chapter deals first with cryptolaw in the context of blockchains. The notion of tokenization will be explored then, the idea that cryptolaw is a distinct body of law will be discussed. Later this chapter addresses the question of decentralization by examining to what extent this concept

should be preserved and made the goal of blockchains and distributed ledgers. It will be argued that there are limits to decentralization and that a further dimension, namely, the legal one, ought to be considered.

8.1 Cryptolaw

The previous chapter described the specific understanding of norms and structures within systems of algorithmic authority as examined by the literature on blockchains. The normative operations of blockchain systems include but are not limited to agreements between parties, decentralized autonomous organizations, management of disputes, governance structures, and creation, transfer, modification of cryptographic assets. In other words, cryptolaw is to blockchains what law is to nation states. Some have argued that the normative operations of blockchains, that is cryptolaw, are "the new jurisprudence that will emerge as a result of implementing and delivering the law of any subject matter through smart-contracting, semi-autonomous, intelligently developing cryptographic computer code" (Reyes, 2017, p. 399). Others contend that cryptolaw, under the terminology of lex cryptographia, refers to a new body of law detached from existing legal systems (Agnikhotram & Kouroutakis, 2018; Wright & De Filippi, 2015). This work takes a different perspective. It will be argued that cryptolaw is neither a new body of law nor the mechanism by which the delivery of law will occur, rather cryptolaw refers to normative structures proper of blockchains and distributed ledgers such as creation of digital assets and dispute resolution within existing systems. More importantly, cryptolaw must adhere to existing legal principle as it is not a substitute for law. At best, some of the core ideas of cryptolaw could be adapted to complement legal norms. This is because cryptolaw appears to be founded on untenable assumptions.

At its core cryptolaw is deterministic, transparent, and never imposed. The term cryptolaw does not refer to legal issues raised by cryptocurrencies and blockchains but to how norms are understood and implemented within blockchain systems to perform some of the functions of the law. The argument unfolds as follows. First, critical differences between law and cryptolaw will be discusses. Then, this section aims to expose the core assumptions on which the concept of cryptolaw rests. Finally, it will be argued that cryptolaw ought to be restrained to specific areas, and that extending it to others is not desirable.

The first difference between modern law and cryptolaw is the medium in which they are embodied. Hildebrand stresses the link between concepts of law and different mediums. According to her perspective, "[m]odern law centers on text and printed matter."(Hildebrandt, 2015, p. 141). In other words, modern law hinges the technology of printing. So that, when the law is expressed in another fashion, as for example orally, it enables some legal structures rather than others. For example, memory and face-to-face communication are more prominent when the medium of the law is not recorded. On the contrary, Hildebrand explains, the transposition of the law to printed matter enabled it to share the affordances of the medium, i.e., the script. Therefore, Hildebrand writes, "[t]he legal dimension of society acquired an extended mind in written manuscripts [...] The era of the manuscript entailed much larger societies than that of an oral culture. The reach of written text is far more extensive in time and space that of the spoken word." (*ibidem*, p. 175). When it comes to cryptolaw, norms are expressed is computer code, this is the first difference between law and cryptolaw. The former exists in print, while the latter in computer code; thus, cryptolaw shares the affordances and the limitations of computer code. One significant consequence is the reduction of the relevance of interpretation. Since code is a performative medium, there is no room for debates on the meaning of words, what is legal in cryptolaw is what machines execute. So that, normative structures of cryptolaw only exist – in the context of distributed consensus architectures - on-chain, thereby inheriting the limitation of current architectures such as the difficulties in gathering outside data and

halting when outcomes do not reflect the intention of the stakeholders. There are attempts to bridge this gap by bringing on-chain, i.e. under cryptolaw, normative structures outside of some systems, this is the case in EOSIO where users are required to put a cryptographic reference to the EOS constitution into their transactions; so that, it is hoped that the off-chain constitution is moved on-chain.

Another difference is that cryptolaw operates ex-ante because blockchain systems are usually resistant to interference. If one takes the example of smart contracts, a normative concept proper of cryptolaw, contract formation and execution may occur at the same time if the smart contract is deployed on a public system (Levy, 2017). And since there is no one in charge of the systems, there is no easy way to prevent smart contracts from executing, this is because cryptolaw pretends to do away with ex-post adjudication in favor of ex-ante determinations. Since cryptolaw aims to be deterministic and because reliance or control replace trust in interactions, there is no need to establish third party enforcement. Of course, this element of cryptolaw is more aspirational than concrete because it rests on an untenable assumption that will shortly be discussed.

A further difference is that open legal concepts tracing back to roman law do not find much space in cryptolaw. This is likely because open concepts introduce uncertainty and they require ex-post adjudication in the form of jurisprudence, elements that are explicitly expunged by this concept of normativity. This entails that cryptolaw is drastically reduced to areas in which the reduction of uncertainty is attainable at an affordable cost. In some sense, cryptolaw is best suited when every possible outcome can be accounted for and precisely define, so that one is left to wander what is its purpose in the first place. Things change, however, if one does not believe that cryptolaw is a new form of law or jurisprudence, which is the position taken in this work. The reasons for rejecting the maximalist accounts of cryptolaw are mostly related to two assumptions that appears to ground it.

The first assumption is that access to the source code is enough to understand cryptolaw. This assumption is untenable for the following reasons. First, it is further assumed that by reading the source code, it is possible to fully grasp the operations of, for example, a cluster of smart contracts. However, bugs in the software, along with poor development practices, invalidate this assumption. For example, a bug might lurk in the compiler so that it will be undetectable by examining the source code. A critical aspect follows from this observation, namely, that developers do not express themselves in source code. Then, the case might arise when what the developers said is not what the smart contracts end up doing. In this case, one of the parties involved will likely invoke the law to resolve the conflict (J. G. Allen, 2018) The previous issue is not theoretical, empirical research found that "ICO software code and ICO investor disclosures often do not match" which means that "[o]nly 37 of the 46 auditable issuers promised vesting in their marketing documents or white papers. Of those that promised to vest, the vast majority (29 of 37) apparently did not use smart contracts to encode those rights (Hoffman, 2018, pp. 2,4). Additionally, it is impossible to code for every possible outcome and bugs are simply a reality of software programming. So that, the assumption that source code is enough to bind people only to cryptolaw is untenable. Consequently, cryptolaw cannot exist by itself nor will be the only mechanism by which future regulations will be implemented.

The second assumption is that hard-forking and the voluntary nature of cryptolaw justify the lack of possibility to contest and resist it. Then cryptolaw systems are a modern version of the social contract of Hobbesian origin by which people subject themselves to a technological version of the Leviathan, i.e. the Techno-Leviathan (Scott, 2015). However, hard-forking might not be a viable mechanism to resist norms within blockchains due to prominent network effects. The argument to treat core maintainers of the major cryptocurrencies as fiduciaries hints at the fact that merely forking is not a viable option (Walch, 2019c). Therefore, cryptolaw must be paired with strong norms to guarantee that there are other ways to resist its operations. This might be done at the level of the governance of blockchain networks or by litigation in courts. In any case, this second assumption is

directly linked to the previous one. Because to claim to voluntary subject oneself to the norms of cryptolaw entails necessarily the ability to understand them, however, this is jeopardized by the existence of bugs and unforeseeable behavior of the software, so that, cryptolaw must be paired with other normative constructs such as legal contracts or existing regulations.

On this basis, cryptolaw must be considered as a form of private ordering that implements, for the most part, techno-regulatory norms. Each blockchain or distributed ledger systems can be considered, from the legal perspective, as a private regulator. Therefore, it must operate within the limits of existing regulations. Pace cryptomaximalist. However, there are some areas in which some of the notions of cryptolaw deserve some merit. In these cases, the core ideas underlying the notion of cryptolaw such as transparency, voluntary subjection, and determinism should not be dismissed. One of such areas is tokenization, i.e., the process of associating a cryptographic token to a real-world asset (Li et al., 2019; Weingärtner, 2019).

The goal of tokenization is to legally transfer the token in lieu of the asset represented. The embodiment of an asset into digital form is not new from the legal perspective, think, for example, of the de-materialization of state bonds required before the introduction of the Euro in the EU. In this case, the concepts of cryptolaw such as token standards might prove useful if the law will mandate that the transfer of the token might have the effect of transferring the rights associated with the real-world tokenized asset. This would open the door to the financialization of the tokenized assets so that careful analysis should be carried out before such a possibility is introduced. For now, the transfer of the token does not entail, from the legal perspective, the transfer of the tokenized assets unless a contractual agreement says so.

To sum up, this section concluded that cryptolaw is not a distinct concept of law nor a new jurisprudence. Cryptolaw is a form of private ordering within the framing of current legal systems.

Then, crypto legal structures must be developed to keep blockchains legal and avoid an existential risk to the persistence of these experiments in algorithmic governance.

8.2 New Perspectives on Decentralization

There are three types of decentralization discussed in the blockchain space. Buterin distinguishes between logical, architectural, and political decentralization (see chapter 7). To recall, logical decentralization refers to the integrity of the system from a functionality perspective; architectural decentralization, instead, points to the numbers of computers that make up the network; lastly, political decentralization is concern with the number of entities that run the nodes. The notion of decentralization is fuzzy, yet it is one of the core ideas on which blockchains' authority is cultivated. The current section aims to add a fourth dimension to the notion of decentralization currently missing, namely, legal (de)centralization. This aspect of decentralization refers to the presence or absence a legal entity behind a given distributed consensus systems. The addition of this dimension arguably helps to elucidate the differences among systems who claim to be decentralized.

The dimension of legal decentralization is necessary because decentralization is a central concept in blockchains and distributed ledgers. The importance of decentralization as one of the core tenets that drives the adoption of this class of technologies has been clear since the inception of Bitcoin. In this context, Nakamoto wrote "[i]t is completely decentralized with no server or central authority" (Nakamoto, 2009). As further evidence of the relevance of this concept lies in claims made about the systems that followed. For example, Ethereum original whitepaper's subtitle: "A Next-Generation Smart Contract and Decentralized Application Platform" while TRON self describes as

"Advanced Decentralized Blockchain Platform" (TRON, 2018; Wood, 2014) .Another case in point is that the perceived centralization of some systems is used to critique them, Mr. Buterin in the occasion of the scaling Bitcoin conference held in Hong Kong in 2015, provocatively tweeted: "can we really say that the uncoordinated choice model is realistic when 90% of the Bitcoin network's mining power is well-coordinated enough to show up together at the same conference?."

Baldwin defines this tendency as network-fetishism. He wrote, a propos of Bitcoin, that "[i]nstead of decentralisation being considered as based upon a geopolitical decision, being a contingent choice, serving a specific historical function, and with appropriate cost-analysis, it is claimed to be 'superior', and indeed, a 'step forward in the evolution of systems" (Baldwin, 2018, p. 3). Then, according to this perspective, the problem is that "Decentralised network fetishism conceals relations and systems of domination, exploitation, and alienation. This is arguably what has happened with bitcoin. There is an illusion of circumventing economic power with decentralised nodes but what has emerged upon closer scrutiny is the corporate occupation of cyberspace in powerful and deep nodes" (*ibidem*, 6).

This leads us to the scope of this section. It aims to highlight the relevance of the fourth dimension of legal decentralization concerning distributed ledgers and blockchains. Accordingly, the next paragraphs explore the legal relevance of decentralization. Then a method for decentralize effectively in the context of distributed consensus systems will be put forward. It turns out that Pope Pius XI might have fleshed out the principle to support the decentralization effort of blockchains and distributed ledgers long before their invention.

8.2.1 Re-defining decentralization

Defining decentralization has real legal consequences. Perhaps, the most remarkable effect of decentralization is found in the U.S. legal system. More precisely, decentralization has been used as an argument in determining whether cryptocurrencies and other cryptographic tokens are an 'investments contract' and therefore constitute a security. Under U.S. law, the Howey test determines if there is an investment contract if four conditions are met. These conditions are (1) the presence of a contract, transaction, or scheme (2) whereby a person invests money, (3) in a common enterprise, and (4) is led to expect profits solely from the efforts of others. In this context, the SEC director William Hinman used the notion of decentralization in a speech delivered on the 14th of June 2018. It is important to note that Mr. Hinman did not define the concept of decentralization, however, it is reasonable to suppose that he draws from the notions described above, that is, logical, architectural and political decentralization of existing blockchains. Hinman's argued that "[i]f the network on which the token or coin is to function is sufficiently decentralized - where purchasers would no longer reasonably expect a person or group to carry out essential managerial or entrepreneurial efforts - the assets may not represent an investment contract [...] As a network becomes truly decentralized, the ability to identify an issuer or promoter to make the requisite disclosures becomes difficult, and less meaningful." Hence, Hinman concludes that "when I look at Bitcoin today, I do not see a central third party whose efforts are a key determining factor in the enterprise. The network on which Bitcoin functions is operational and appears to have been decentralized for some time", moreover, he continues "[b]ased on my understanding of the present state of Ether, the Ethereum network and its decentralized structure, current offers and sales of Ether are not securities transactions." However, if he would have considered the dimension of legal decentralization the argument would have taken another direction. This is because Ethereum is less legally decentralized than Bitcoin for the presence

of the Ethereum foundation incorporated in Switzerland, whose efforts appear to a relevant extent managerial or entrepreneurial.

Further, legal decentralization addresses a possible concern related to data protection and blockchains (Daoui, 2019; lyons, courcelas, & timsit, 2018; Ramsay, 2018). In the context of the application of the GDPR to blockchains, a recent study suggested that "the GDPR is based on the underlying assumption that in relation to each personal data point there is at least one natural or legal person - the data controller - whom data subjects can address to enforce their rights under EU data protection law. Blockchains, however, often seek to achieve decentralisation in replacing a unitary actor with many different players. This makes the allocation of responsibility and accountability burdensome, particularly in light of the uncertain contours of the notion of (joint)-controllership under the regulation." (Finck, 2019, p. 4). This account is defensible only if the elements of decentralization that are taken into consideration are the logical, architectural and political one. Instead, by adding the axis of legal centralization the problems of allocating responsibility and accountability is reduce to a handful of systems which do not have legal entities backing the network's own efforts. Moreover, legal (de)centralization explains why closed blockchains are not considered problematic from the legal viewpoint. In this case, even if systems might be architecturally, politically, and logically decentralized, they are not legally decentralized because one legal entity controls the development of the systems. This is true even if this legal entity does not run any of the nodes! On the contrary, some open blockchains might be decentralized along all four dimensions, that is, logical, architectural, political, and legal. However, this is the exception rather than the norm. Among the top systems by market capitalization, only Bitcoin would have to be considered decentralized among all the four axis described above, on the contrary, systems such as Ethereum, TRON, EOSIO, Zcash, and others which are run by a for-profit company or backed by a legal entity would be quickly identified as not entirely decentralized, and, therefore, subject to the enforcement of legal norms without much difficulty.

The section contends that the added dimension of legal decentralization is more relevant than the logical, architectural and political one. This is because it will be shown that most existing systems can hardly be considered decentralized beyond the logical and architectural aspects. Yet, this is true for existing distributed systems implemented long before the advent of blockchains and distributed ledgers.

8.2.2 Awdy?

The title of this subsection refers to apparent anxiety present in the crypto world as well as the URL of a website that tracks decentralization metrics across the most popular systems. It is the acronym of are we decentralized yet? These metrics track easily measurable aspects of blockchain networks such as mining distribution, and the number of full nodes. It comes to no surprise that blockchain communities are actively worrying about being sufficiently decentralized, for – as it has been discussed in the previous chapter – the aspiration of being decentralized is arguably one of the main motives to use blockchains and distributed ledgers in the first place. The next paragraphs show that concerns about the degree to which current systems are decentralized are, indeed, justified.

On the one hand, the mining of cryptocurrencies cannot be considered decentralized. This is true regardless of the consensus algorithm adopted. It holds for both PoW or PoS/DPoS system along with hybrids of the two. More precisely, mining is not decentralized with regard to the distribution of mining power or stakers in PoS systems. On the other hand, exchanges of cryptocurrencies have become dominant players and it is possible to assume that most transactions are carried out via their platforms. This is likely because blockchains are not user-friendly. Therefore, exchanges exert a significant amount of pressure on blockchain systems often influencing the value of their cryptographic tokens. Exchanges are problematic because there are few safeguards in place or best

practices to guard users against the risks associated with the business of exchanging cryptocurrencies for fiat. Their short history is littered with mismanagement, hacks, and frauds. Think, for example, to the MtGox demise or the recent QuadrigaCX case.

The empirical data reported above in chapter 7 showed how logical and architectural dimensions of decentralization are insufficient to produce truly decentralized systems, arguably, the most important dimensions of decentralization are the legal and political one. Then, this section continues by proposing a principle to help blockchains and distributed ledgers orient their efforts toward building more decentralized systems. As in the case of the issue of governance explored in chapter 4, legal theory can help. After all, the question of decentralization is not new because it entails distributing power among different levels of government.

8.2.3 How to decentralize

First, we need to consider that absolute decentralization appears both impossible and undesirable as it corresponds with anarchy. Therefore, designers ought to aim at the highest degree of decentralization while preserving the effectiveness of the system along with other values. For example, if a serious security vulnerability is discovered, it seems necessary to prefer swift action by a group of experts rather than a more protracted deliberation involving the entire community. Then, the desirable degree of decentralization changes with regard to different functions. However, this nuanced approach to the concept of decentralization appears seldom considered in the blockchain discourse, if at all. This section argues that a version of the subsidiarity principle appears well-suited to guide blockchains' architects to build meaningfully decentralized systems. For the principle of subsidiarity dictates the appropriate level at which authority ought to be exercised. It originated within the Catholic Church and was later adopted as a general principle of European Law.

The origin of the principle of subsidiarity is found in two encyclicals, Rerum Novarum and Quadragesimo authored by Pope Leo XIII and Pope Pius XI respectively (XI, 1931; XIII, 1891). Arguably devised to tame the struggle between the opposing forces of socialism and liberalism the principle of subsidiarity seeks to provide practical and moral guidance, to organize a system of *herrschaft* to recall Weber's terminology. Defined as "the most weighty principle" of social philosophy by Pius XI, subsidiarity is defined in the encyclical Quadragesimo in the following way: "[j]ust as it is gravely wrong to take from individuals what they can accomplish by their own initiative and industry and give it to the community, so also it is an injustice and at the same time a grave evil and disturbance of right order to assign to a greater and higher association what lesser and subordinate organizations can do" (XIII, 1891). In other words, subsidiarity decentralizes authority up to the point in which decentralization cannot effectively execute a given function.

Past its Catholic origins, subsidiarity is a core principle of European law. The Maastricht Treaty established the principle of subsidiarity, then the principle was incorporated in the Lisbon Treaty into Article 5(3) of the TEU which states that "[u]nder the principle of subsidiarity, in areas which do not fall within its exclusive competence, the Union shall act only if and in so far as the objectives of the proposed action cannot be sufficiently achieved by the Member States, either at the central level or at regional and local level, but can rather, by reason of the scale or effects of the proposed action, be better achieved at Union level." Furthermore, the Lisbon Treaty established a new protocol (Protocol No 2) on the application of the principle of subsidiarity along with proportionality. Chiefly, it established the new role of national parliaments in ensuring compliance with the aforementioned principles. The compliance with the principle of subsidiarity is ensured by the retrospective review of the Court of Justice following the adoption of a legislative act, see for example the judgments in Cases C-84/94, C-233/94, and C-547/14. What is crucial for our purposes is that subsidiarity can be used to prevent excessive centralization of powers by guarantee independence of a lower authority. To a relevant extent, subsidiarity prevents centralization about

specific actions if more decentralized levels of authority can attain the objectives of such actions. Therefore, it is unsurprising that a joint UNDP-Government of Germany report on decentralization recognizes the relevance of the principle of subsidiarity. In the report, subsidiarity is considered as guiding the national frameworks for decentralization, "[t]he constitutional/statutory basis defining the systems, the levels, their respective jurisdictions and their complementary roles according to the principle of subsidiarity." (UNDP, 1999, p. 16). On this basis, this section contends that subsidiarity might guide the decentralization efforts of blockchains and distributed ledgers more effectively than blind adherence to an ill-defined idea of decentralization.

It is unclear that a single formulation of the subsidiarity principle for blockchains would fit all blockchains and distributed ledgers. More precisely, it might be that different systems would agree on distinct versions of the principle of subsidiarity. Perhaps, one community might decide to limit its reach to matters of security of the network while another might extend it to cover all the development process. This is because, subsidiarity must be considered with regard to goal(s) and action(s) proposed to achieve it, so that, deliberation is needed to precisely delimit its operational reach. Then, crypto communities ought to specify the goals and objectives of their technical infrastructure so that the actions proposed to achieve them could be assessed with the subsidiarity principle in order to understand the proper level of intervention. An example might clarify the argument. Let us take Ethereum and assume that there is enough agreement within the community to establish the improvement of its performance as a primary goal. Then, one needs to assess whether this objective can be sufficiently achieved in a decentralized way, i.e., by the EIP procedures or, as it seems likely if it would be better achieved by a dedicated body or crypto-institution to attain it.

Additionally, when a vulnerability is discovered, the subsidiarity principle justifies the swift intervention by a small group of developers. In this way, the core value of decentralization is preserved whilst recognizing that some actions demand some degree of centralization to be performed effectively. Moreover, a subsidiarity principle might ensure that blockchain systems maintain a

sufficient amount of legitimacy when decentralization appears unfit to reach some of the actions needed to ensure blockchains' development.

If the subsidiarity principle is implemented in blockchains and distributed ledgers, it will offer some justification of the current centralized aspects of many systems or it might expose them as untenable. In conclusion, this section contends that the principle of subsidiarity would benefit distributed consensus systems because it will likely (a) promote sensible decentralization by acknowledging that some actions are better performed with some degree of centralization (b) help to justify the presence of centralized aspects of current systems.

9. Conclusion

This dissertation examined blockchains and distributed ledgers. More precisely, it studied the claims that support the adoption of these systems in a variety of domains, ranging from online payments to distributed organizations. In other words, it aimed to understand on what basis blockchains, and distributed ledgers are being adopted beyond purely technical motives. The analysis was structured as follows.

Chapter 2 examined the phenomenology of blockchains and other consensus systems using Heidegger's methodology to define the object under study precisely. Several levels of the software stack of these systems have been examined, from the scripting language to consensus algorithms. Then, chapter 3 examined the claim that blockchains are 'trust machines' finding that it falls short because these systems appear to increase reliability nor trust by introducing control. The claim that blockchains are a new mode of governance was examined later in chapter 4. The conclusion is that blockchains are, for the most part, incomplete systems of rules and that, therefore, their adoption does not appear justified on this basis.

Then, I argued that the reason why blockchains and distributed ledgers are adopted is because these technologies are perceived to have a valid claim to *herrschaft* in the Weberian sense. To understand the origin and scope of this claim, chapter 5 fixed the appropriate level of abstraction, namely that of descriptive legitimacy, to understand the nature and attribute of the claim to rule of blockchains and distributed ledgers. Accordingly, chapter 6 examined if the framework elaborated by Max Weber is sufficient to explain the authority of blockchains and why people use and argue for the adoption of this class of technologies. It found that the three pure types of imperative co-ordination (traditional, charismatic, and rational-legal) are only capable to partly explain why people grant authority to these systems. Therefore, chapter 7 attempted to outline the core ideas on which

blockchains' authority hinges. It found that blockchains appear to cultivate their belief in their authority on a computational extension of the pure type of rational-legal authority. Chapter 7, then, took a general viewpoint to study the elements on which the authority of algorithmic authority hinges. Later, it examined the facets of the claim to authority of blockchains by studying the concept of cryptolaw as well as the current state of affairs with regard to the core idea of decentralization. To conclude, the main findings of this work are summarized as follows.

The first finding is that no such thing as The Blockchain, The Distributed ledger, or The Blockchain Technology exist. Systems should be examined on a case-by-case on the following axis. Access to the network (open vs. closed), computational complexity (Turing complete vs. Turing incomplete), access to network functions, and legal structures (presence of a legal entity). This leads us to the principle that blockchains and other distributed ledgers should not be treated as a single entity, rather as different mechanisms to achieve distinct goals.

The second finding is that blockchains and distributed ledgers are not trustless systems. In the case of direct access to endogenous assets, these systems replace trust with reliance. In other cases, trust is still necessary, but it is reduced by the introduction of control by/with the protocol. Therefore, the second main finding is that the interplay of trust, reliance and control demands careful consideration when dealing with old systems as well as designing new ones. The shift from trust to control in the reduction of complexity might have relevant effects that should be studied cautiously. The third finding is that the governance of blockchains and distributed ledgers needs secondary rules, preferably written in natural language and off-chain. The fourth main finding is that some of the ideas on which the authority of blockchains and distributed ledgers rests should be adopted to design other systems that exert power via computations. These ideas are voluntarily subjection, transparency of the source code, and transparency of the systems' operations.

The fifth finding is that cryptolaw is not a parallel legal system. Rather, it is a form of private ordering of techno-regulatory norms. Therefore, cryptolaw demands careful consideration of when and how it should be permitted. Lastly, decentralization within blockchains and distributed networks ought to be driven by a version of the subsidiarity principle so that, actions should be decentralized only in so far as the objectives of the proposed action can be sufficiently achieved in a decentralized fashion.

In conclusion, it is possible to draw a few general remarks from the analysis carried out in the previous pages. It is useful to recall that the effects of blockchains and distributed ledgers on trust and governance do not support their adoption. Instead, other factors outside this study may explain the rise in the blockchain phenomenon. I argued that the conviction, according to which power is better exercised via (some) computational processes is the answer to the question addressed in this work, namely, why do agents engage with blockchains and distributed ledgers. This appears to be mostly based on the core ideas explored in chapter 7, further, these ideas will likely survive the obsolescence of blockchains and distributed ledgers. Against this backdrop, this work contributes to future studies on how to exert power legitimately byways of computation in a manner that is distinct from the previous iterations of techno-regulatory systems. Open questions remain such as whether limits ought to be put in place concerning the areas in which power via computation could be legitimately exercised or to the appropriate governance structures to ensure human flourishing. Moreover, questions also raise in the context of the proper level in which power with computations could be exercised legitimately.

10. 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.

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

Agnikhotram, S., & Kouroutakis, A. (2018). Doctrinal Challenges for the Legality of Smart Contracts: Lex Cryptographia or a New, Smart Way to Contract. *Journal of High Technology Law*(2), 300-328.

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

Alberini, A., & Pfammatter, V. (2019). Blockchains, Smart Contracts, Decentralised Autonomous Organisations and the Law. In *Blockchain and data protection*.

Allen, D. W. E., Berg, C., Lane, A. M., & Potts, J. (2018). Cryptodemocracy and its institutional possibilities. *The Review of Austrian Economics*. doi:10.1007/s11138-018-0423-6

Allen, J. G. (2018). Wrapped and Stacked: 'Smart Contracts' and the Interaction of Natural and Formal Language. In *European Review of Contract Law* (Vol. 14, pp. 307).

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., . . . Manevich, Y. (2018). Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. *arXiv preprint arXiv:1801.10228*.

Antonopoulos, A. M. (2014). *Mastering Bitcoin: unlocking digital cryptocurrencies*: " O'Reilly Media, Inc.".

Arruñada, B., & Garicano, L. (2018). *Blockchain: The birth of decentralized governance*. Retrieved from https://EconPapers.repec.org/RePEc:upf:upfgen:1608

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.

Auinger, A., & Riedl, R. (2018). Blockchain and Trust: Refuting Some Widely-held Misconceptions.

Aust, H. (2018). 'The System Only Dreams in Total Darkness': The Future of Human Rights Law in the Light of Algorithmic Authority.

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

Baird, L. (2016). The Swirlds hashgraph consensus algorithm: fair, fast, byzantine fault tolerance. In (Vol. SWIRLDS-TR-2016-01). Swirlds Tech Reports.

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

Bano, S., Sonnino, A., Al-Bassam, M., Azouvi, S., McCorry, P., Meiklejohn, S., & Danezis, G. (2017). Consensus in the Age of Blockchains. *arXiv preprint arXiv:1711.03936*.

Barlow, J. P. (1996). Declaration of Independence for Cyberspace. In.

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

Bartoletti, M., & Pompianu, L. (2017). An empirical analysis of smart contracts: platforms, applications, and design patterns. *arXiv preprint arXiv:1703.06322*.

Benčić, F. M., & Žarko, I. P. (2018). Distributed Ledger Technology: Blockchain Compared to Directed Acyclic Graph. *arXiv preprint arXiv:1804.10013*.

Bensman, J. (1979). Max Weber's concept of legitimacy: an evaluation. *Conflict and control: Challenge to legitimacy of modern governments, 7*, 325-371.

Bentham, J. (1996). *The collected works of Jeremy Bentham: An introduction to the principles of morals and legislation*: Clarendon Press.

Bentov, I., Lee, C., Mizrahi, A., & Rosenfeld, M. (2014). Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake. *IACR Cryptology ePrint Archive, 2014*, 452.

Berg, A., Berg, C., & Novak, M. (2018). *Blockchains and Constitutional Catallaxy*. Paper presented at the Annual Australasian Public Choice Conference, Melbourne.

Berg, C. (2017). What Diplomacy in the Ancient Near East Can Tell Us About Blockchain Technology. *2017, 2*, 10. doi:10.5195/ledger.2017.104

Berg, C., Davidson, S., & Potts, J. (2018a). Blockchains as Constitutional Orders. In R. E. Wagner (Ed.), *James M. Buchanan: A Theorist of Political Economy and Social Philosophy* (pp. 383-397). Cham: Springer International Publishing.
Berg, C., Davidson, S., & Potts, J. (2018b). Crypto Constitutionalism
Bhargavan, K., Swamy, N., Zanella-Béguelin, S., Delignat-Lavaud, A., Fournet, C., Gollamudi, A., . . . Sibut-Pinote, T. (2016). *Formal Verification of Smart Contracts*. Paper presented at the Proceedings of the 2016 ACM Workshop on Programming Languages and Analysis for Security - PLAS'16.
Bian, Y., Mu, W., & Zhao, J. L. (2018, 2018/6). *Online Leadership for Open Source Project Success.* Paper presented at the Evidence from the GitHub Blockchain Projects.
Botsman, R. (2012). The currency of the new economy is trust. *Ted Talks*.
Bratman, M. E. (2013). *Shared agency: A planning theory of acting together*: Oxford University Press.
Brown, R. G., Carlyle, J., Grigg, I., & Hearn, M. (2016). Corda: an introduction. In. https://docs.corda.net/_static/corda-introductory-whitepaper.pdf: R3.
Brownsword, R. (2019). Regulatory Fitness: Fintech, Funny Money, and Smart Contracts. *European Business Organization Law Review*. doi:10.1007/s40804-019-00134-2
Brownsword, R., & Yeung, K. (2008). *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes*: Bloomsbury Publishing.
Buterin, V. (2014). DAOs, DACs, DAs and More: An Incomplete Terminology Guide.
Buterin, V. (2017). The Meaning of Decentralization.
Buterin, V., Hitzig, Z., & Weyl, E. G. (2018). Liberal Radicalism: Formal Rules for a Society Neutral among Communities. *arXiv preprint arXiv:1809.06421*.
Cachin, C., Schubert, S., & Vukolić, M. (2016). Non-determinism in byzantine fault-tolerant replication. *arXiv preprint arXiv:1603.07351*.
Cachin, C., & Vukolić, M. (2017). Blockchains Consensus Protocols in the Wild. In *arXiv preprint arXiv:1707.01873* (Vol. 31st International Symposium on Distributed Computing).
Camp, L. J. (2003). *Designing for Trust*, Berlin, Heidelberg.
Camp, L. J., Nissenbaum, H., & McGrath, C. (2002). *Trust: A Collision of Paradigms*, Berlin, Heidelberg.
Campbell-Verduyn, M. (2018). *Bitcoin and Beyond Cryptocurrencies, Blockchains, and Global Governance* (M. Campbell-Verduyn Ed.). New York: Routledge.
Casanovas, P. (2012). A note on validity in law and regulatory systems (position paper). *Quaderns de filosofia i ciència, 42*(2012), 29-40.
Casino, F., Dasaklis, T. K., & Patsakis, C. (2018). A systematic literature review of blockchain-based applications: current status, classification and open issues. *Telematics and Informatics*.
Castelfranchi, C., & Falcone, R. (2000). Trust and control: A dialectic link. *Applied Artificial Intelligence, 14*(8), 799-823. doi:10.1080/08839510050127560
Castelfranchi, C., & Falcone, R. (2010). *Trust theory: A socio-cognitive and computational model* (Vol. 18): John Wiley & Sons.
Catalini, C. a. G., Joshua S. (2017). Some Simple Economics of the Blockchain. *Rothman School of Management Working Paper No. 2874598; MIT Sloan Research Paper No. 5191-16, Available at SSRN: https://ssrn.com/abstract=2874598 or http://dx.doi.org/10.2139/ssrn.2874598*.
Chapron, G. (2017). The environment needs cryptogovernance. *Nature, 545*(7655), 403.
Chaum, D. (1997). David Chaum on Electronic Commerce How much do you trust Big Brother? *IEEE Internet Computing, 1*(6), 8-16.
Chohan, U. (2017). The Decentralized Autonomous Organization and Governance Issues. *Availeble at SSRN https://ssrn.com/abstract=3082055 or http://dx.doi.org/10.2139/ssrn.3082055*.
CleanApp. (2018a). Blockchain Governance Bibliography. Retrieved from https://medium.com/cryptolawreview/blockchain-governance-bibliography-360efc52d3f9
CleanApp. (2018b). Crypto Legal Theory.
Coleman, J. A. (1997). Authority, power, leadership: Sociological understandings. *New Theology Review, 10*(3).
Conte de Leon, D., Conte de Leon, D., Stalick, A. Q., Stalick, A. Q., Jillepalli, A. A., Jillepalli, A. A., . . . Sheldon, F. T. (2017). Blockchain: properties and misconceptions. *Asia Pacific Journal of Innovation and Entrepreneurship, 11*(3), 286-300.

Craig, B. R., & Kachovec, J. (2019). Bitcoin's Decentralized Decision Structure. *Economic Commentary*(2019-12).
Crain, T., Gramoli, V., Larrea, M., & Raynal, M. (2017). *Blockchain Consensus.* Paper presented at the ALGOTEL 2017-19èmes Rencontres Francophones sur les Aspects Algorithmiques des Télécommunications.
Crepaldi, M. (2019). *Why blockchains need the law: Secondary rules as the missing piece of blockchain governance*. Paper presented at the Proceedings of the Seventeenth International Conference on Artificial Intelligence and Law.
Cuccuru, P. (2017). Beyond bitcoin: an early overview on smart contracts. *International Journal of Law and Information Technology, 25*(3), 179-195. doi:10.1093/ijlit/eax003
Cutts, T. (2019). Smart contracts and the average joe. *West Virginia Law Review*.
Daoui, S., Fleinert-Jensen, T. & Lempérière, M. . (2019). GDPR, Blockchain and the French Data Protection Authority: Many Answers but Some Remaining Questions. *Stanford Journal of Blockchain Law & Policy, Retrieved from https://stanford-jblp.pubpub.org/pub/gdpr-blockchain-france*.
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. (2018). *Blockchain and the Law: The Rule of Code*: Harvard University Press.
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
De Vido, S. (2019). All that Glitters is not Gold: The Regulation of Virtual Currencies in the New EU V Anti-Money Laundering Directive. *DPCE Online, 38*(1).
Debler, J. (2018). Foreign Initial Coin Offering Issuers Beware: The Securities and Exchange Commission is Watching. *Cornell International Law Journal, 51*(1), 245-272.
Deleuze, G. (1988). *Foucault*: U of Minnesota Press.
Dierksmeier, C., & Seele, P. (2016). Cryptocurrencies and Business Ethics. *Journal of Business Ethics*. doi:10.1007/s10551-016-3298-0
Dietvorst, B. J., Simmons, J. P., & Massey, C. (2015). Algorithm aversion: People erroneously avoid algorithms after seeing them err. *Journal of Experimental Psychology: General, 144*(1), 114.
Dinh, T. T. A., Liu, R., Zhang, M., Chen, G., Ooi, B. C., & Wang, J. (2017). Untangling Blockchain: A Data Processing View of Blockchain Systems. *arXiv preprint arXiv:1708.05665*.
Dodd, N. (2017). The social life of Bitcoin. *Theory, Culture & Society*.
Dos Santos, R. P. (2017). On the Philosophy of Bitcoin/Blockchain Technology: Is it a Chaotic, Complex System? *Metaphilosophy, 48*(5), 620-633. doi:10.1111/meta.12266
Douceur, J. R. (2002). *The sybil attack.* Paper presented at the International workshop on peer-to-peer systems.
DuPont, Q. (2014). The politics of cryptography: Bitcoin and the ordering machines. *Journal of Peer Production, 1*(4), 1-10.
DuPont, Q. (2017). Experiments in algorithmic governance: A history and ethnography of "The DAO," a failed decentralized autonomous organization. In *Bitcoin and Beyond* (pp. 157-177): Routledge.
DuPont, Q. (2018). Social and Technical Opportunities and Risks of Cryptocurrencies and Blockchains. *Available at SSRN*.
Durante, M. (2010). What Is the Model of Trust for Multi-agent Systems? Whether or Not E-Trust Applies to Autonomous Agents. *Knowledge, Technology & Policy, 23*(3), 347-366. doi:10.1007/s12130-010-9118-4
Durante, M. (2015). Sicurezza e fiducia nell'età della tecnologia. *Filosofia politica, 6*(3), 439-458.
Dworkin, R. (1986). *Law's empire*: Harvard University Press.
Estella de Noriega, A. (2002). *The EU principle of subsidiarity and its critique*.
Eyal, I., & Sirer, E. G. (2018). Majority is not enough: Bitcoin mining is vulnerable. *Communications of the Acm, 61*(7), 95-102.
Fabienne, P. (2010). Political legitimacy. *Stanford Encyclopedia of Philosophy, 29*.
Falcone, R., & Castelfranchi, C. (2001). Social Trust: A Cognitive Approach. In C. Castelfranchi & Y.-H. Tan (Eds.), *Trust and Deception in Virtual Societies* (pp. 55-90). Dordrecht: Springer Netherlands.
Fallon Jr, R. H. (2004). Legitimacy and the Constitution. *Harvard Law Review, 118*, 1787.

Fenwick, M., Kaal, W. A., & Vermeulen, E. P. (2016). Regulation Tomorrow: What Happens when Technology Is Faster than the Law?
Feynman, R. P., & Leighton, R. (2001). *" What do you care what other people think?": further adventures of a curious character*: WW Norton & Company.
Finck, M. (2018). Blockchains: Regulating the Unknown. *German LJ, 19*, 665.
Finck, M. l. (2018). *Blockchain Regulation and Governance in Europe*. Cambridge: Cambridge University Press.
Finck, M. l. (2019). *Blockchain and the General Data Protectgion Regulation - Can distributed ledgers be squared with European data protection law?* https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf: European Parliament.
Floridi, L. (2008). The method of levels of abstraction. *Minds and machines, 18*(3), 303-329.
Floridi, L. (2010). *Information: A very short introduction*: OUP Oxford.
Floridi, L. (2011). *The philosophy of information*: Oxford University Press.
Floridi, L. (2018). Soft Ethics and the Governance of the Digital. *Philosophy & Technology, 31*(1), 1-8.
Floridi, L., Cath, C., & Taddeo, M. (2019). Digital Ethics: Its Nature and Scope. In C. Öhman & D. Watson (Eds.), *The 2018 Yearbook of the Digital Ethics Lab* (pp. 9-17). Cham: Springer International Publishing.
Frantz, C. K., & Nowostawski, M. (2016). *From institutions to code: towards automated generation of smart contracts.* Paper presented at the Foundations and Applications of Self* Systems, IEEE International Workshops on.
Fulmer, N. (2019). Exploring the Legal Issues of Blockchain Applications. *Akron Law Review, 52*(1), 5.
Galen, D., Brand, N., Boucherle, L., Davis, R., Do, N., El-Baz, B., . . . Lee, J. (2018). Blockchain for social impact. In (in collaboration with RippleWorks ed.). Stanford: Stanford Graduate School of Business.
Galloway, A. R. (2004). *Protocol: How control exists after decentralization*: MIT press.
Gambetta, D. (1988). *Trust: Making and breaking cooperative relations*: B. Blackwell New York, NY.
Gencer, A. E., Basu, S., Eyal, I., van Renesse, R., & Sirer, E. G. (2018). Decentralization in Bitcoin and Ethereum Networks. *arXiv preprint arXiv:1801.03998*.
Gerard, D. (2017). *Attack of the 50 foot blockchain: Bitcoin, blockchain, Ethereum & smart contracts*: David Gerard.
Gilcrest, J., & Carvalho, A. (2018, 10-13 Dec. 2018). *Smart Contracts: Legal Considerations.* Paper presented at the 2018 IEEE International Conference on Big Data (Big Data).
Girasa, R. (2018). Regulation of Cryptocurrencies and Blockchain Technologies: National and International Perspectives. In: Springer.
Glaser, F., & Bezzenberger, L. (2015). *Beyond cryptocurrencies-a taxonomy of decentralized consensus systems*. Paper presented at the 23rd European Conference on Information Systems (ECIS),, Münster, Germany.
Golumbia, D. (2016). *The politics of Bitcoin: software as right-wing extremism*: University of Minnesota Press.
Gonzalez Rivas, A., Tsyganova, M., & Mik, E. (2018). Smart Contracts and their Identity Crisis.
Goodwin, M., Koops, B.-J., & Leenes, R. (2010). *Dimensions of technology regulation*: Wolf.
Governatori, G., Idelberger, F., Milosevic, Z., Riveret, R., Sartor, G., & Xu, X. (2018). On legal contracts, imperative and declarative smart contracts, and blockchain systems. *Artificial intelligence and law, 26*(4), 377-409. doi:10.1007/s10506-018-9223-3
Greene, A. R. (2017). Legitimacy without Liberalism: A Defense of Max Weber's Standard of Political Legitimacy. *Analyse & Kritik, 39*(2), 295-324.
Grigg, I. (2015). On the intersection of Ricardian and Smart Contracts. In.
Grodzinsky, F. S., Miller, K. W., & Wolf, M. J. (2011). Developing artificial agents worthy of trust: "Would you buy a used car from this artificial agent?". *Ethics and Information Technology, 13*(1), 17-27. doi:10.1007/s10676-010-9255-1
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*.
Hanson, R. (2003). Shall we vote on values, but bet on beliefs? *Journal of Political Philosophy*.

Hanson RT., R. A., Staples M. (2017). Distributed Ledgers, Scenarios for the Australian economy over the coming decades. *Canberra*.
Hart, H. L. A., & Green, L. (2012). *The concept of law*: Oxford University Press.
Hawlitschek, F., Notheisen, B., & Teubner, T. (2018). The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy. *Electronic Commerce Research and Applications, 29*, 50-63.
Hayes, A. (2019). The Socio-Technological Lives of Bitcoin. *Theory, Culture & Society, 36*(4), 49-72. doi:10.1177/0263276419826218
Hearn, M. (2015). Why is Bitcoin forking.
Heidegger, M. (1996). *Being and time: A translation of Sein und Zeit*: SUNY press.
Heidegger, M., & Lovitt, W. (1977). *The question concerning technology, and other essays*: Harper & Row New York.
Herian, R. (2018a). The Politics of Blockchain. *Law and Critique, 29*(2), 129-131. doi:10.1007/s10978-018-9223-1
Herian, R. (2018b). Regulating Disruption: Blockchain, GDPR, and Questions of Data Sovereignty. *Journal of Internet Law, 22*(2), 1.
Hershovitz, S. (2003). LEGITIMACY, DEMOCRACY, AND RAZIAN AUTHORITY. *Legal Theory, 9*(3), 201-220. doi:10.1017/S1352325203000090
Hildebrandt, M. (2011). Legal protection by design: objections and refutations. *Legisprudence, 5*(2), 223-248.
Hildebrandt, M. (2015). *Smart technologies and the end (s) of law: novel entanglements of law and technology*: Edward Elgar Publishing.
Hoffman, D. (2018). Regulatin Initial Coin Offering (ICOs). *Penn Wharton Public Policy Initaitive, 59*.
Hsieh, Y.-Y., & Vergne, J.-P. (2017). Bitcoin and the Rise of Decentralized Autonomous Organizations.
Hütten, M. (2018). The soft spot of hard code: blockchain technology, network governance and pitfalls of technological utopianism. *Global Networks*.
Iansiti, M., & Lakhani, K. R. (2017). The Truth About Blockchain. *Harvard Business Review, 95*(1), 118-127.
Ibáñez, L.-D., O'Hara, K., & Simperl, E. (2018). *On Blockchains and the General Data Protection Regulation*. University of Southampton.
Idelberger, F., Governatori, G., Riveret, R., & Sartor, G. (2016). *Evaluation of logic-based smart contracts for blockchain systems.* Paper presented at the International Symposium on Rules and Rule Markup Languages for the Semantic Web.
Ishmaev, G. (2017). Blockchain Technology as an Institution of Property. *Metaphilosophy, 48*(5), 666-686. doi:10.1111/meta.12277
Jeong, S. (2013). The Bitcoin Protocol as Law, and the Politics of a Stateless Currency. *SSRN, Available at SSRN: https://ssrn.com/abstract=2294124 or http://dx.doi.org/10.2139/ssrn.2294124*.
Joerges, B. (1999). Do Politics Have Artefacts? *Social Studies of Science, 29*(3), 411-431.
Käll, J. (2018). Blockchain Control. *Law and Critique, 29*(2), 133-140. doi:10.1007/s10978-018-9227-x
Kelsen, H. (1967). *Pure theory of law*: Univ of California Press.
Khan, V., & Goodell, G. (2019). Libra: Is it Really About the Money? *Available at SSRN 3441707*.
Kim, T. W., & Zetlin-Jones, A. (2019). The Ethics of Contentious Hard Forks in Blockchain Networks With Fixed Features. *Frontiers in Blockchain, 2*(9). doi:10.3389/fbloc.2019.00009
Krause, M. J., & Tolaymat, T. (2018). Quantification of energy and carbon costs for mining cryptocurrencies. *Nature Sustainability*, 1.
Lamport, L., Shostak, R., & Pease, M. (1982). The Byzantine generals problem. *ACM Transactions on Programming Languages and Systems (TOPLAS), 4*(3), 382-401.
Larimer, D. (2018). Decentralized Blockchain Governance.
Leenes, R. (2011). Framing techno-regulation: An exploration of state and non-state regulation by technology. *Legisprudence, 5*(2), 143-169.
Lehdonvirta, V. (2016). The blockchain paradox: Why distributed ledger technologies may do little to transform the economy.
Lemieux, V. (2017). *Blockchain and Distributed Ledgers as Trusted Recordkeeping Systems: An Archival Theoretic Evaluation Framework.*
Lessig, L. (2006). Code: Version 2.0. *New York*.

Levy, K. E. (2017). Book-smart, not street-smart: blockchain-based smart contracts and the social workings of law. *Engaging Science, Technology, and Society, 3*, 1-15.
Li, X., Wu, X., Pei, X., & Yao, Z. (2019). *Tokenization: Open Asset Protocol on Blockchain.* Paper presented at the 2019 IEEE 2nd International Conference on Information and Computer Technologies (ICICT).
Lianos, I., Hacker, P., Eich, S., & Dimitropoulos, G. (2019). *Regulating Blockchain: Techno-Social and Legal Challenges*: Oxford University Press.
Libra Association. (2019). Libra White Paper. In. https://libra.org/en-US/white-paper/: Libra Association.
Locher, T., Obermeier, S., & Pignolet, Y.-A. (2018). When Can a Distributed Ledger Replace a Trusted Third Party? *arXiv preprint arXiv:1806.10929*.
Logg, J. M., Minson, J. A., & Moore, D. A. (2019). Algorithm appreciation: People prefer algorithmic to human judgment. *Organizational behavior and human decision processes, 151*, 90-103.
Low, K. F., & Mik, D. E. (2019). Pause the Blockchain Legal Revolution. *Forthcoming, International & Comparative Law Quarterly*.
Luhmann, N. (1979). *Trust and Power*: John Wiley & Sons.
Luhmann, N., Kastner, F., & Schiff, D. (2004). *Law as a social system*: Oxford University Press on Demand.
Lupton, D. (2014). *Digital sociology*: Routledge.
Lustig, C. (2018). *Algorithmic Authority of the Bitcoin Blockchain*.
Lustig, C., & Nardi, B. (2015, 5-8 Jan. 2015). *Algorithmic Authority: The Case of Bitcoin.* Paper presented at the 2015 48th Hawaii International Conference on System Sciences.
Lustig, C., Pine, K., Nardi, B., Irani, L., Lee, M. K., Nafus, D., & Sandvig, C. (2016). *Algorithmic authority: the ethics, politics, and economics of algorithms that interpret, decide, and manage.* Paper presented at the Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems.
lyons, t., courcelas, l., & timsit, k. (2018). *Blockchain and the GDPR*. Retrieved from
Maiyya, S., Zakhary, V., Amiri, M. J., Agrawal, D., & El Abbadi, A. (2019). *Database and Distributed Computing Foundations of Blockchains.* Paper presented at the Proceedings of the 2019 International Conference on Management of Data.
Mallard, A., Méadel, C., & Musiani, F. (2014). The paradoxes of distributed trust: peer-to-peer architecture and user confidence in Bitcoin. *Journal of Peer Production*(4), 10.
Marian, O. Y. (2013). Are Cryptocurrencies' Super'Tax Havens?
Mattila, J., & Seppälä, T. (2018). Distributed Governance in Multi-sided Platforms: A Conceptual Framework from Case: Bitcoin. In A. Smedlund, A. Lindblom, & L. Mitronen (Eds.), *Collaborative Value Co-creation in the Platform Economy* (pp. 183-205). Singapore: Springer Singapore.
McKnight, J. C. (2012). A failure of convivencia: Democracy and discourse conflicts in a virtual government. *Bulletin of Science, Technology & Society, 32*(5), 361-374.
Meijer, D., & Ubacht, J. (2018). *The governance of blockchain systems from an institutional perspective, a matter of trust or control?* Paper presented at the Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age, Delft, The Netherlands.
Merkle, R. C. (2016). DAOs, democracy and governance. *Cryonics Magazine, July-August, 37*, 4.
Michal Araszkiewicz, P. C. (2016). On Legal Validity. *Frontiers in Artificial Intelligence and Applications, 294 Legal Knowledge and Information Systems*, 125-130.
Mik, E. (2017). Smart contracts: terminology, technical limitations and real world complexity. *Law, Innovation and Technology*, 1-32.
Mutti, A. (2004). The resiliency of systemic trust. *Economic Sociology: European Electronic Newsletter, 6*(1), 13-19.
Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. In.
Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies: a comprehensive introduction*: Princeton University Press.
Narayanan, A., & Clark, J. (2017). Bitcoin's Academic Pedigree. *Queue, 15*(4), 20.
Natoli, C., Yu, J., Gramoli, V., & Esteves-Verissimo, P. (2019). Deconstructing Blockchains: A Comprehensive Survey on Consensus, Membership and Structure. *arXiv preprint arXiv:1908.08316*.
Naves, J., Audia, B., Busstra, M., Hartog, K. L., Yamamoto, Y., Rikken, O., & Heukelom-Verhage, S. v. (2019). Legal Aspects of Blockchain. *Innovations: Technology, Governance, Globalization, 12*(3-4), 88-93. doi:10.1162/inov_a_00278

Nickel, P. J., Franssen, M., & Kroes, P. (2010). Can We Make Sense of the Notion of Trustworthy Technology? *Knowledge, Technology & Policy, 23*(3), 429-444. doi:10.1007/s12130-010-9124-6
Nissenbaum, H. (2001). Securing trust online: Wisdom or oxymoron. *BUL Rev., 81*, 635.
Nissenbaum, H. (2004). Will Security Enhance Trust online, or supplant it?
Notheisen, B., Cholewa, J. B., & Shanmugam, A. P. (2017). Trading real-world assets on blockchain. *Business & Information Systems Engineering, 59*(6), 425-440.
OECD. (2019). *State of the art in the use of emerging technologies in the public sector*. Retrieved from
Ølnes, S., & Jansen, A. (2018). *Blockchain technology as infrastructure in public sector: an analytical framework.* Paper presented at the Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age.
Oren, O. (2018). ICO's, DAO's, and the SEC: A Partnership Solution. *Columbia Business Law Review*, 617.
Oshodin, O., Molla, A., & Ong, C. E. (2016). An information systems perspective on digital currencies: a systematic literature review.
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. (2013). *The laws of robots: crimes, contracts, and torts* (Vol. 10): Springer.
Pagallo, U. (2016). *Even Angels Need the Rules: AI, Roboethics, and the Law*. Paper presented at the ECAI.
Pagallo, U. (2017a). 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. (2017b). LegalAIze: Tackling the Normative Challenges of Artificial Intelligence and Robotics Through the Secondary Rules of Law. In M. Corrales, M. Fenwick, & N. Forgó (Eds.), *New Technology, Big Data and the Law* (pp. 281-300). Singapore: Springer Singapore.
Pagallo, U. (2019). Network Theory and Legal Information "for" Reality: A Triple Support for Deliberation, Decision Making, and Legal Expertise. In *Law, Public Policies and Complex Systems: Networks in Action* (pp. 267-280): Springer.
Pagallo, U., Bassi, E., Crepaldi, M., & Durante, M. (2018). *Chronicle of a Clash Foretold: Blockchains and the GDPR's Right to Erasure.* Paper presented at the Legal Knowledge and Information Systems: JURIX 2018: The Thirty-first Annual Conference.
Pagallo, U., Casanovas, P., & Madelin, R. (2019). The middle-out approach: assessing models of legal governance in data protection, artificial intelligence, and the Web of Data. *The Theory and Practice of Legislation*, 1-25.
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
Pasquale, F. (2011). Restoring transparency to automated authority. *J. on Telecomm. & High Tech. L., 9*, 235.
Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*: Harvard University Press.
Pflaum, I., & Hateley, E. (2013). A bit of a problem: National and extraterritorial regulation of virtual currency in the age of financial disintermediation. *Georgetown Journal of International Law, 45*, 1169.
Pitt, J. C. (2010). It's Not About Technology. *Knowledge, Technology & Policy, 23*(3), 445-454. doi:10.1007/s12130-010-9125-5
Popov, S. (2018). *The Tangle*. IOTA Foundation https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvsIqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iota1_4_3.pdf.
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.
Přibáň, J. (2011). Self-Reference of the Constitutional State: A Systems Theory Interpretation of the Kelsen-Schmitt Debate. *Jurisprudence, 2*(2), 309-328.
Rajagopalan, S. (2018). Blockchain and Buchanan: Code As Constitution.
Ramsay, S. (2018). *The General Data ProtectionRegulation vs. The Blockchain: A legal study on the compatibility between blockchain technology and the GDPR*. Thesis. Faculty of Law. Stockholm University.
Rawls, J. (1955). Two concepts of rules. *The philosophical review, 64*(1), 3-32.

Rawls, J. (2001). *Justice as fairness: A restatement*: Harvard University Press.
Raz, J. (2001). Liberty and trust.
Reidenberg, J. R. (1997). Lex informatica: The formulation of information policy rules through technology. *Texas Law Review, 76*, 553.
Reijers, W., O'Brolcháin, F., & Haynes, P. (2016). Governance in Blockchain Technologies & Social Contract Theories. *Ledger, 1*, 134-151.
Reijers, W., Wuisman, I., Mannan, M., De Filippi, P., Wray, C., Rae-Looi, V., . . . Orgad, L. (2018). Now the Code Runs Itself: On-Chain and Off-Chain Governance of Blockchain Technologies. *Topoi*. doi:10.1007/s11245-018-9626-5
Reyes, C. L. (2017). Conceptualizing Cryptolaw. *Nebraska Law Review*(2), 384-445.
Rogers, R. (2013). *Digital methods*: MIT press.
Sartor, G. (2008). Legal Validity: An Inferential Analysis. *Ratio Juris, 21*(2), 212-247. doi:10.1111/j.1467-9337.2008.00388.x
Schmitt, C. (2005). *Political theology: Four chapters on the concept of sovereignty*: University of Chicago Press.
Schneider, N. (2019). Decentralization: An Incomplete Ambition.
Scholz, L. H. (2016). Algorithmic Contracts. *Stanford Technology Law Review, Forthcoming*, Available at SSRN: https://ssrn.com/abstract=2747701.
Scott, B. (2015). Visions of a Techno-Leviathan: The Politics of the Bitcoin Blockchain.
Searle, J. R. (2005). What is an institution? *Journal of Institutional Economics, 1*(1), 1-22. doi:10.1017/S1744137405000020
Shahaab, A., Lidgey, B., Hewage, C., & Khan, I. (2019). Applicability and Appropriateness of Distributed Ledgers Consensus Protocols in Public and Private Sectors: A Systematic Review. *IEEE Access*.
Shakow, D. J. (2018). The Tao of The DAO: Taxing an Entity That Lives on a Blockchain.
Shermin, V. (2017). Disrupting governance with blockchains and smart contracts. *Strategic Change-Briefings in Entrepreneurial Finance, 26*(5), 499-509. doi:10.1002/jsc.2150
Sicilia, M.-A., & Visvizi, A. Blockchain and OECD data repositories: opportunities and policymaking implications. *Library Hi Tech, 0*(0), null. doi:doi:10.1108/LHT-12-2017-0276
Siems, M. M. (2009). The taxonomy of interdisciplinary legal research: finding the way out of the desert. *Journal of Commonwealth Law and Legal Education, 7*(1), 5-17.
Sigrid Seibold, G. S. (2016). Consensus. In *Immutable agreement for the Internet of Value*: KPMG LLP.
Sklaroff, J. M. (2017). Smart Contracts and the Cost of Inflexibility.
Stoll, C., Klaaßen, L., & Gallersdörfer, U. (2019). The Carbon Footprint of Bitcoin. *Joule*. doi:10.1016/j.joule.2019.05.012
Swan, M. (2015). *Blockchain: Blueprint for a new economy*: " O'Reilly Media, Inc.".
Swan, M., & De Filippi, P. (2017). Toward a Philosophy of Blockchain: A Symposium: Introduction. *Metaphilosophy, 48*(5), 603-619. doi:10.1111/meta.12270
Szabo, N. (1997). Formalizing and securing relationships on public networks. *First Monday, 2*(9).
Taddeo, M. (2009). Defining trust and e-trust: from old theories to new problems. *International journal of technology and human interaction (IJTHI), 5*(2), 23-35.
Taddeo, M. (2010a). Modelling Trust in Artificial Agents, A First Step Toward the Analysis of e-Trust. *Minds and machines, 20*(2), 243-257. doi:10.1007/s11023-010-9201-3
Taddeo, M. (2010b). Trust in technology: A distinctive and a problematic relation. *Knowledge, Technology & Policy, 23*(3-4), 283-286.
Taddeo, M., & Floridi, L. (2011). The case for e-trust. *Ethics and Information Technology, 13*(1), 1-3. doi:10.1007/s10676-010-9263-1
Tai, E. T. T. (2017). Formalizing contract law for smart contracts. In *Tilburga Private Law Working Paper Series* (Vol. No. 06/2017). https://ssrn.com/abstract=3038800: Tilburg University.
Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the technology behind Bitcoin is changing money, business, and the world*: Penguin.
Teutsch, J., & Estsblishment, T. (2017). On decentralized oracles for data availability.
Thurimella, R., & Aahlad, Y. (2018). The Hitchhiker's Guide to Blockchains: A Trust Based Taxonomy.
TRON. (2018). TRON Advanced Decentralized Blockchain Platform. In. https://tron.network/static/doc/white_paper_v_2_0.pdf: TRON Foundation.

Tschorsch, F., & Scheuermann, B. (2016). Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies. *IEEE Communications Surveys & Tutorials, 18*(3), 2084-2123. doi:10.1109/COMST.2016.2535718

UNDP, G. o. G. (1999). *Decentralization: A Sampling of Definitions*. http://web.undp.org/evaluation/documents/decentralization_working_report.PDF: UNDP.

Unsworth, R. (2019). Smart Contract This! An Assessment of the Contractual Landscape and the Herculean Challenges it Currently Presents for "Self-executing" Contracts. In M. Corrales, M. Fenwick, & H. Haapio (Eds.), *Legal Tech, Smart Contracts and Blockchain* (pp. 17-61). Singapore: Springer Singapore.

van Klink, P., & Taekema, S. (2008). A dynamic model of interdisciplinarity: Limits and possibilities of interdisciplinary research into law. *SSRN, Tilburg University Legal Studies Working Paper No. 010/2008; Tilburg Working Paper Series on Jurisprudence and Legal History No. 08-02*.(Available at SSRN: https://ssrn.com/abstract=1142847 or http://dx.doi.org/10.2139/ssrn.1142847).

Vaz, J., & Brown, K. (2018). *Cryptocurrencies, institutions and trust*. Monash Business School. Australian Center for Financial Studies.

Velasco, P. R. (2017). Computing Ledgers and the Political Ontology of the Blockchain. *Metaphilosophy, 48*(5), 712-726. doi:10.1111/meta.12274

Victoria Louise, L. (2016). Trusting records: is Blockchain technology the answer? *Records Management Journal, 26*(2), 110-139. doi:10.1108/RMJ-12-2015-0042

Vigna, P., & Casey, M. J. (2018). *The Truth Machine: The Blockchain and the Future of Everything*: St. Martin's Press.

Von Hayek, F. A. (2009). *Denationalisation of money: The argument refined*: Ludwig von Mises Institute.

Walch, A. (2017). Blockchain's Treacherous Vocabulary: One More Challenge for Regulators.

Walch, A. (2019a). Deconstructing'Decentralization': Exploring the Core Claim of Crypto Systems. *Crypto Assets: Legal and Monetary Perspectives (OUP, forthcoming 2019)*.

Walch, A. (2019b). Deconstructing 'Decentralization': Exploring the Core Claim of Crypto Systems. In *Crypto Assets: Legal and Monetary Perspectives*: Oxford University Press.

Walch, A. (2019c). In Code (Rs) We Trust: Software Developers as Fiduciaries in Public Blockchains.

Wang, C., Chu, X., & Yang, Q. (2019). Measurement and Analysis of the Bitcoin Networks: A View from Mining Pools. *arXiv preprint arXiv:1902.07549*.

Wattenhofer, R. (2016). *The science of the blockchain*: CreateSpace Independent Publishing Platform.

Weaver, N. (2018). Risks of cryptocurrencies. *Communications of the Acm, 61*(6), 20-24.

Weber, B. (2014). Bitcoin and the legitimacy crisis of money. *Cambridge Journal of Economics, 40*(1), 17-41.

Weber, M. (1978). *Max Weber on law in economy and society (20th century legal philosophy series)*: Berkeley: University of California Press.

Weber, M. (2012). *The Theory of Social and Economic Organization* (A. M. H. a. T. Parsons, Trans.): Martino Publishing.

Weingärtner, T. (2019). Tokenization of physical assetsand the impact of IoT and AI. In. EU Blockchain Observatory Forum.

Werbach, K. D. (2017). Trust, But Verify: Why the Blockchain Need the Law. *Berkley Technology Law Journal*.

Werbach, K. D. (2018). *The Blockchain and the New Architecture of Trust*: MIT Press.

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

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

Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper, 151*(2014), 1-32.

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

Wu, K., Peng, B., Xie, H., & Huang, Z. (2019, 12-14 July 2019). *An Information Entropy Method to Quantify the Degrees of Decentralization for Blockchain Systems.* Paper presented at the 2019 IEEE 9th International Conference on Electronics Information and Emergency Communication (ICEIEC).

XI, P. P. (1931). On Reconstruction of the Social Order. *Encyclical of Pope Pius XI, 15*.

Xiao, Y., Zhang, N., Lou, W., & Hou, Y. T. (2019). A Survey of Distributed Consensus Protocols for Blockchain Networks. *arXiv preprint arXiv:1904.04098*.

Xie, R. (2019). Why China Had to Ban Cryptocurrency but the US Did Not: A Comparative Analysis of Regulations on Crypto-Markets between the US and China. *Washington University Global Studies Law Review, 18*, 457.
XIII, P. L. (1891). Rerum novarum. *Encyclical of Pope LEO XIII*.
Xu, B., Luthra, D., Cole, Z., & Blakely, N. (2018). EOS: An Architectural, Performance, and Economic Analysis. In. https://blog.bitmex.com/wp-content/uploads/2018/11/eos-test-report.pdf.
Yeung, K. (2019). Regulation by Blockchain: the Emerging Battle for Supremacy between the Code of Law and Code as Law. *The Modern Law Review, 82*(2), 207-239. doi:10.1111/1468-2230.12399
Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where Is Current Research on Blockchain Technology?-A Systematic Review. *PLoS One, 11*(10), e0163477. doi:10.1371/journal.pone.0163477
Zachariadis, M., Hileman, G., & Scott, S. V. (2019). Governance and control in distributed ledgers: Understanding the challenges facing blockchain technology in financial services. *Information and Organization*. doi:https://doi.org/10.1016/j.infoandorg.2019.03.001
Zamfir, V. (2017). Against on-chain governance. Retrieved from https://medium.com/@Vlad_Zamfir/against-on-chain-governance-a4ceacd040ca
Zamfir, V. (2018a). Blockchain Governance 101.
Zamfir, V. (2018b). My Intentions for Blockchain Governance.
Zamfir, V. (2019). Against Szabo's Law, For a New Crypto Legal System.