EconomEtica

Centro interuniversitario per l'etica economica
e la responsabilità sociale di impresa
promosso dalla Fondazione Italiana Accenture

N.76 November 2019

Blockchains' twilight zones. A reasoned literature review for a critical primer

Plinio Limata

Blockchains’ twilight zones

A reasoned literature review for a critical primer

Abstract

This literature review focuses on certain critical aspects of blockchain technology. Trust, (de)centralization and law are pivotal to the functioning of markets and society in general; blockchain promises to deeply transform both, and their correlated institutions. Technology and behaviors have a reciprocal influence. Results show several issues that must not be underestimated in order to develop the applications of the blockchain properly, and therefore reach shared benefits and avoid unintentional negative impacts at both micro (individual) and macro (societal) level.

Keywords: blockchain, trust, law, decentralized governance

1. Introduction

The blockchain is currently commanding high media attention, and many people are showing enthusiasm for the potential outcomes deriving from the use of this technology and its role in driving the decentralization of society and rendering the need for central authorities and intermediaries obsolete, which could be replaced by the “4 Cs” of code, connectivity, crowd, and collaboration (Fenwick et al., 2018). Yet, its potential to facilitate new forms of governance remains largely unexplored (Rozas et al., 2018). Much attention has been dedicated to the positive or disruptive changes that would change our society with the full adoption of this technology. Aside from technological issues, less attention has been given to the challenges it may pose. Very little research has focused on blockchain technology and its ability to address societal needs (Ølnes et al., 2017), being predominantly concentrated on technological matters and business-related topics while neglecting applications, value creation, and governance to address broader societal, political or judicative questions (Risius and Spoher, 2017). Essentially, the research in question has merely taken the technological features for granted, looking at the possible implications of the blockchain implementation in different industries. For example, Faber and Jonker (2019) explore how the blockchain may work in relation to the paradigm of sustainability and circularity, but they overlook blockchain claims, failing to question them in their functioning and consequences. Moreover, the relation between what is made possible by technology in its practical application could differ from what is envisaged or desirable from a societal or legal perspective. The development of technologies such as blockchain is indicative of a type of politics, understood as interactions between social discourses and social imaginaries (Reijers and Coeckelbergh, 2016).

The debate is currently hinging on two leading positions: techno-determinism and market-driven values versus those who consider central institutions as inherently necessary in fostering democratic forms of governance (Rozas et al., 2018). However, institutions are social technologies, and technological evolution not only affects production but also social organization (Berg et al., 2018). Therefore, as Rozas et al. (2018) point out, can we build perspectives of blockchain-based governance that go beyond markets and states?

Different approaches have been developed to analyze the blockchain according to the scientific or industrial sector involved[1], and several definitions have been generously given.[2] A number of literature reviews have been published to photograph the state of the art: Yli-Hummo et al. (2016) provided a systematic review of the blockchain as a technology; Conoscenti et al. (2016) scrutinized the application of Blockchain for the Internet of Things; Risius and Spohrer (2017) published a research framework; Hawlitschek et al. (2018) focused on blockchain and trust in the sharing economy; Reyna et al. (2018) investigated how blockchain could potentially improve the IoT. All of these studies brought the pros and cons of this technology to the surface in certain potential fields of applications, while not placing a specific focus on the potential consequences and changes that will be required for the large-scale implementation of this technology to fulfill its potential.

Reijers et al. (2016, p. 147) claim that the blockchain reflects the idea expressed by Hobbes of a totalitarian sovereign in terms of rule-enforcement, coupled with Rousseau's concept of decentralized governance and Rawls's theory of equal rights and liberties for all. Is it true? Will the pairing of blockchain technology with institutions envisage and be loyal to such principles?

We are facing a society in transition, which means a fundamental rearrangement of institutions that assure societal functions (Faber and Jonker, 2019). Government, governance[3], and classical socio-economic paradigms could be challenged by the possibilities that may arise from the development of non-centralized political and socio-economic systems, which in turn could revolutionize interaction in society "We are in a phase of human development where the power to develop codes and select algorithms has – and it will increasingly have – major implications in contemporary society: this power entails assertion of authority, calling into question the egalitarian nature of technology and networks" (Atzori, 2015, p. 27). At the same time, a "hypothetical global society only run through organizational patterns based on individualism […] would inherently lack legitimate mechanisms to regulate the convergence of the particular into the general, which is the traditional role of centralized political institutions" (Atzori, 2015, p. 25). This role has been played considering the objectives that a society envisages for itself. The mistrust of these institutions today (De Filippi, 2018), and the birth of a technology that allows for the creation of autonomous networks, poses serious challenges in striving for a just, inclusive and sustainable society.

[1] E.g., *through a Schumpeterian lens of ICT productivity* or *through an institutional lens of efficient governance* (Davidson et al., 2016), as an *institutional technology of coordination* (Berg et al., 2019; Davidson et al., 2018), in terms of *competition* (Lianos, 2018) or *innovation* (Catalini and Gans, 2017); in light of an *entangled political economy approach* (Allen et al., 2018).

[2] E.g., as a *non-discriminative technology* (Koletsi, 2019), as *a foundational technology* (Werbach, 2018), as *an innovative technology in search of use cases* (Glaser, 2017), as *a new and foundational mode of configuring reality* (Swan and De Filippi, 2017), as *a coordinating institution for creating new economies* (Berg and Berg, 2017), as *a new institutional technology of governance* (Davidson et al. 2016b), as *a new type of economy* (Davidson et al., 2016), a *catallaxy* (Davidson et al., 2016b), as a narrative technology (Reijers and Coeckelbergh, 2016), as a *new general purpose technology* (Evans, 2014).

[3] Governance can be intended as the manner in which power is exercised, e.g. in the management of a country's economic and social resources for development (World Bank, 1992).

Our research aims to highlight the importance of questioning how this technology will impact social aspects, freedom, and people's interaction in general. Blockchains are a technology for the distribution, maintenance, and verification of social facts (Berg et al., 2019), creating the chance to reshape "the ways and means through which individuals, enterprises and bureaucracies interact in the pursuit of gains achieved economically, socially or politically" (Novak, 2018, p. 6). We decided to prioritize the concepts which should receive attention for evaluating the impact on the development and functioning of societies by the application of the blockchain on a large scale. In a literature review, we therefore aim to bring those aspects into the discussion which, to date, have been identified as the most uncertain or problematic: i) trust, ii) (de)centralization, and iii) law. We will focus on the identified primary aspects, considering them as founding elements of societal functioning. Other critical aspects, such as those based on technology, were not taken into consideration, as they were not functional in the scope of this research. The chapters that follow present the issues addressed singularly to reach conclusions. The final remarks are dedicated to possible future patterns of research.

2. A primary on the blockchain

The advent of the blockchain has been compared to the invention of double-entry bookkeeping in fourteenth century Italy (Abadi and Brunnermeier, 2018) or of the Internet (Akgiray, 2019), showing the potential for groundbreaking transformations within many industries (Beck and Muller-Bloch, 2017). The financial sector is seen as a primary user of the blockchain concept (Akgiray, 2019; Nofer et al., 2017) since, in 2008, Satoshi Nakamoto's paper, "Bitcoin: A Peer-to-Peer Electronic Cash System," underlined the basis of modern blockchain-based cryptocurrency innovation. According to Yermack (2018, p. 8), although a first analogical example of this technology was given by Haber and Stornetta's work (1991), which proposed a distributed ledger published in public media outlets (e.g., newspaper) for time-stamping the creation of intellectual property, Nakamoto's attempt was the first to provide a trusted non-territorial digital currency that was not dependent on centralized financial institutions such as banks; "a peer-to-peer electronic cash system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party" (Catalini and Gans, 2017, p. 1).

The first stage was the creation of a cryptocurrency (i.e., bitcoin) to which other altcoins[4] followed. Developments were so vast that, as highlighted by Davidson et al. (2016b, p. 5), Babbitt and Dietz (2015) defined *cryptoeconomy* "as an economy unconstrained by geography and political and legal institutions in which blockchains rather than trusted third parties constrain behavior and all transactions are recorded on a decentralized public ledger." However, the potential application of blockchains are much broader than currencies (Allen et al., 2017), and go well beyond financial services (Tapscott and Tapscott, 2016). "Blockchain was the under-the-hood invention that enabled the digital currency and payments system to work without the need for a trusted central authority by

[4] "Altcoin" is a combination of two words: "alt" and "coin"; alt signifying 'alternative' and coin signifying (in essence) 'cryptocurrency.' Altcoins are the alternative cryptocurrencies to the digital currency Bitcoin. See: https://www.investopedia.com/terms/a/altcoin.asp

using a distributed, cryptographically secure, and crypto-economically incentivized consensus engine" (Davidson et al., 2016 p. 2).

A decade later, the blockchain technology has moved beyond cryptocurrencies, but little remains known about its promised disruptive potential (Beck and Muller-Bloch, 2017). The fundamental characteristics of this technology enables the implementation of a wide range of processes for asset registry, inventory, and information exchange, both hard assets such as physical property, and intangible assets such as votes, patents, ideas, reputation, intention, health data, information, etc. (Swan, 2015 quoted in Ølnes et al., 2017, p. 357). The blockchain opens the door to the liquification of the physical world, to the economy of real-time micro-transactions and smart data sharing (Waelbroeck, 2018, p. 1). Its applications are foreseen in almost every human field; it is recognized as an alternative to ownership ledgers based on traditional double-entry bookkeeping (Yermack, 2017). As mentioned by Werbach (2018), according to Max Weber, double-entry bookkeeping was the foundation of modern capitalism. Markey-Towler (2018, p. 3) also remarks on the concept, since "the basis for our market economies is the law of contract and property, and these rely on the keeping of verifiable records, our entire economic system relies on the keeping of verified public records." The purpose of a ledger is to record and verify facts in their economic, political, or social manifestations (Davidson et al., 2018). In contemporary society, trusted intermediaries generally occupy this function. While "the goal of the Blockchain technology is to create a decentralized environment where no third party is in control of the transactions and data. […] The information about every transaction ever completed in Blockchain is shared and available to all nodes." (Yli-Hummo et al., 2016, p. 2).

In short, it is a public record kept without the requirement of a public authority (Markey-Towler, 2018), a shared database that allows its users to make transactions of valuable assets in public and pseudonymous setups without having to rely on an intermediary or central authority (Glaser, 2017; Risius and Spohrer, 2017; Hawlitschek et al., 2018). It is an instrument for recording and transmitting digital goods over the Internet, with the assurance that these goods cannot be copied or multiplied (Swan and De Filippi, 2017, p. 2). The blockchain makes use of three primary features to ensure these results: distributed ledgers, consensus, and smart contracts (Werbach, 2018, p. 10). These are all independent technologies that can be used independently in stand-alone applications, or jointly within any combination with the other technologies (Akgiray, 2019).

Therefore, in spite of the common characteristics there is no unique implementation of "the blockchain", since it may come in many different forms and with different properties (Ølnes et al., 2017, p. 360). "Blockchain technology can be deployed in various ways to create platforms with different features, including with regard to: (i) who can propose new transactions to be added to the ledger; (ii) who stores a copy of the ledger; (iii) who can add new blocks to the ledger; (iv) who can view the ledger; (v) whether users are identifiable; and, (vi) who controls the platform's underlying software" (Bacon et al., 2017, p. 49).

By the different combination that the above-mentioned elements can achieve, Beck and Muller-Bloch (2017) categorized the blockchain in two different ways; "public and private, also called unpermissioned and permissioned." However, there is a third possibility to be considered, the so-called "consortium model," which is "partially decentralized" (Reyna et al., 2018). The three types have varying configurations of permission, by which the economic properties of rivalry and excludability differ (Waelbroeck, 2018, p. 7).

"From an economic perspective, a private permissioned system merely resembles an intra- or inter-group technology upgrade[5] […] A hybrid *(consortium)* blockchain can be considered a club good. Users are excludable from the system, but the admitted users have no further restrictions with respect to the usage of the systems services. A public blockchain, on the contrary, resembles a public good. That is, users are non-excludable from its services, and there is no rivalry among users. If a rivalry should exist for some reason, it could be considered a common good" (Glaser, 2017, p. 1548).

Public blockchains are distributed systems without a single owner that can freely govern the network (Risius and Spoher, 2017); anyone can operate a mining node and maintain a copy of the shared ledger. Permissioned ledgers are a different story, in which elements of control dictate the rules of the game and decide which grade restricts the rights of members. Moreover, "private blockchains and public blockchains differ in three other dimensions: the effectiveness of the validation process[6], the governance[7] of the blockchain and the issue of legal responsibility[8]" (Waelbroeck, 2018, p. 11).

In summary, this technology has attracted high expectations. The variety of approaches and definitions corresponds with the innumberable expectations that have been raised by the blockchain (Avital et al., 2016). However, there remains a paucity of knowledge regarding where and how blockchain technology is effectively applicable and where it can provide notable societal effects (Risius and Spoher, 2017, p. 1).

3. Literature Review: Methodology

The present literature follows Vom Brocke et al. (2009) and Webster and Watson (2002), as shown in fig.1 below. We focused on scholarly literature featuring the lens of the civil economy.[9] Except for one literature review, written by Yli-Hummo et al. (2016), articles focusing on technological and cryptocurrency issues were discarded. We queried scientific databases, such as JSTOR, Scopus, SSRN, Science Direct, Ideas, and G-Scholar, using the following keywords: blockchain, blockchain + trust, blockchain + law, blockchain + rights, blockchain + governance; identifying 475 articles. The work was carried out in four steps. The first layer (1) of analysis referred to titles, abstracts and keywords, to proceed to the exclusion of those articles not directly focused on the issues investigated or mentioning them in a superficial context (2). A snowball analysis (3) was then performed to extend the coverage of the research. This additional step was conducted in order to process 48 additional articles. Lastly, we selected 105 articles, and a classification (4) was performed that divided the materials into the specific topic concerned.

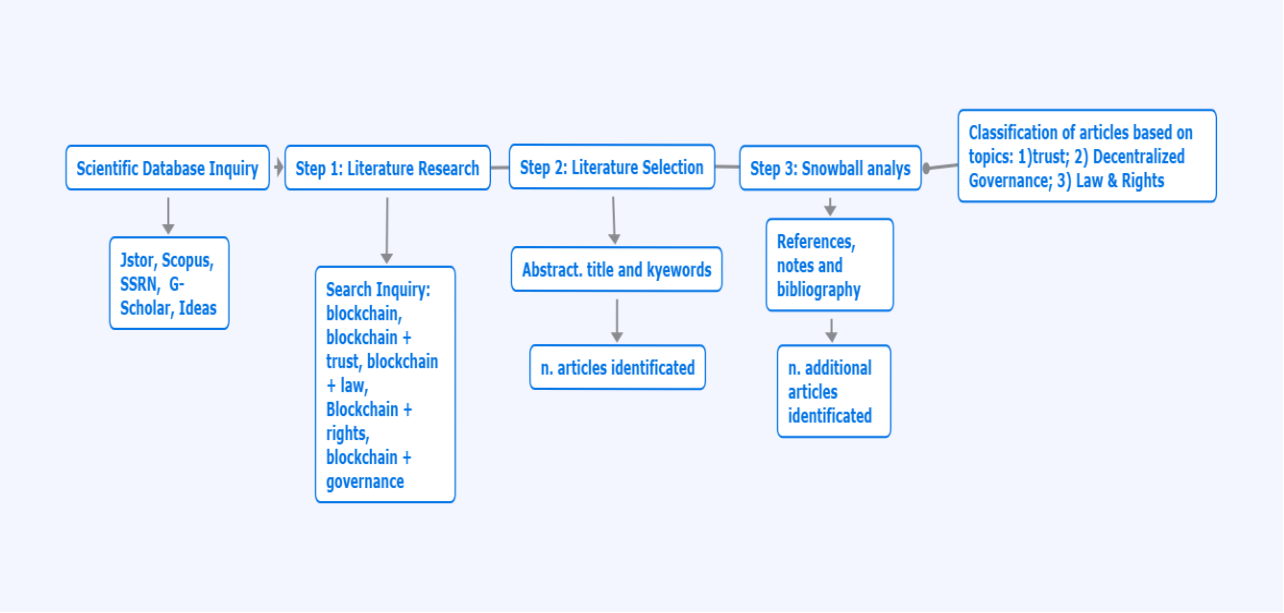
[5] In this case, the blockchain can be considered a private good.

[6] The author refers to different types of *consensus*, whereby an increase in the speed of block validation can come at the cost of security, for example.

[7] Governance includes questions such as who dictates the rules, maintains the system, how the rules are executed, and how a Blockchain system would be closed out. The established governance structure should also be responsible for ensuring adherence to the guiding principles and design philosophy of the project (Lapointe and Fishbane, 2019).

[8] It could be much easier to establish responsibilities in the case of a private (and national) blockchain, while the question is under debate in international public blockchain (Waelbroeck, 2018, p. 11).

[9] The civil economy shifts the primacy from rights and contracts to the social bonds and civic ties upon which democracies and market economies depend, portraying market relationships as relations of mutual assistance, hence neither impersonal nor anonymous.


Scientific Database Inquiry
Jstor, Scopus, SSRN, G-Scholar, Ideas
Step 1: Literature Research
Search Inquiry: blockchain, blockchain + trust, blockchain + law, Blockchain + rights, blockchain + governance
Step 2: Literature Selection
Abstract. title and kyewords
n. articles identificated
Step 3: Snowball analys
References, notes and bibliography
n. additional articles identificated
Classification of articles based on topics: 1)trust; 2) Decentralized Governance; 3) Law & Rights

4. Discussion about the findings of the literature review

The literature review was conducted to identify several issues that should be studied in greater depth in order to provide a more accurate assessment of the impact of blockchain implementation and application on a societal level, in the light of the intrinsic characteristics of this technology; e.g., anonymous, trustless, immutable, transparent. These features present a wealth of technical challenges and limitations that must be addressed (Yli-Hummo et al., 2016). If not ,the blockchain may not fulfill the enormous expectations placed on it (Avital et al., 2016); "Its implications are significant because the applications that the technology affords can reconfigure economic, legal, institutional, monetary and ultimately broader socio-political relationships" (Reijers et al., 2016, p. 147). It is vital that researchers investigate the associated costs of blockchain systems for individuals and society (Risius and Spoher, 2017), since new technology applications "amplify" each other, increasing their social impact and effects (Fenwick and Vermeulen, 2018), often resulting in a change in human behavior that in turn influences technology applications (DeSanctis and Poole, 1994, quoted in Ølnes et al., 2017, p. 362). As stressed by Koletsi (2019) in recalling Heidegger, any technology cannot be ideologically, socially or culturally neutral, since its essence is not merely technological but a deep reflection of human thought and action to control and understand the surrounding physical environment. De Filippi and Hassan (2016) strengthen this concept; technology is not neutral, but inherently political since its design will ultimately dictate the type of actions that might be enabled or prevented by its proliferation.

Furthermore, as Hacker et al. (2019) affirm, "technological development and innovations profoundly rely on the social forces that promote their use, being accompanied by a narrative of a broader change of the social, economic and legal processes that govern value generation." Reijers and Coeckelbergh (2016) and Koletsi (2019) confirm these dynamics within the blockchain narrative. It is to be noted that these social forces may represent different social groups which each have varying interpretations of technology, changing its design accordingly and thereby influencing (if not dictating) human behaviors.

The blockchain seems to promise the liberation of individuals and value creation, but, as highlighted by Wright and De Filippi (2015), increased automation could result in decreased freedom and autonomy, giving birth to a highly prescriptive and deterministic type of *algorithmic governance*, leaving the mere illusion of freedom to ordinary people. Besides, blockchains still have significant technical, operational and scaling shortcomings (Fenwick et al., 2018). "Faith in technology should take into consideration blockchain's operational risks in large-scale application: "(i) software has bugs, (ii) software is vulnerable to attack, (iii) software is ever-changing through new releases, and (iv) few people understand how software works" (Walch, 2015, quoted in Kakavand and De Sevres, 2016, p. 25). There is much to be considered, especially for a technology defined as disruptive and applicable to everything.

a) Is the blockchain a trust-free environment?

In every human transaction, there must be an element of trust. Trust is arguably the primary input in economic cooperation, and in economic theory is usually understood as being exogenously provided (Berg et al., 2018). "Trust is a psychological state comprising the intention to accept vulnerability, based upon positive expectations of the intentions or behavior of another […] Trust is neither a behavior (e.g., cooperation) nor a choice (e.g., taking a risk), but an underlying psychological condition that can cause or result from such actions" (Rousseau et al.,1998). Trusting relations, which consist of the qualities of vulnerability, risk, expectation, or uncertainty (Davidson et al., 2018), are the foundational resource of any economy and institutions that can engender trust facilitating extensive economic cooperation and therefore value creation (Berg et al., 2018). Trust is a fundamental precondition underpinning exchange and economic coordination, but it is costly to maintain[10] (Davidson et al., 2018). Moreover, it is not transitive[11] (Werbach, 2018).

"An essential quality a ledger must possess is trust in the ledger itself. A high trust ledger creates a low transaction cost economy, which is a precondition for economic efficiency and prosperity" (Nooteboom, 2002, quoted in Davidson et al., 2016, p. 5). "The blockchain technology will fundamentally transform the way trust is built" (Hawlitschek et al., 2018, p. 51). Distributed ledger technology allows participants to trust the outcome of a system without trusting the individual participants (Werbach, 2018, p. 6), reducing the cost of opportunism, and galvanizing trust with respect to data integrity (Davidson et al., 2018).

The blockchain reaches the endogenization of trust thanks to the combination of three underlying technologies: cryptography, smart contracts, peer-to-peer networks, and distributed ledger design (Akgiray, 2019). The ledger is based on cryptographic techniques [namely the *hash function* and the *digital signature* (Ishmaev, 2017, p. 674)], combined with game theory[12] (Catalini and Gans, 2017),

[10] In the same research, the authors estimated that about 35 per cent of employment in the United States relates to activity aimed at upholding trustful economic relationships (Davidson et al., 2018).

[11] For example, I may trust my bank, but that does not mean I trust yours! (Werbach, 2018, p. 21).

[12] Game theory can be used to analyze the strategies of the consensus nodes as well as the interactions between them. Through an analysis base on game theory, the nodes can learn and predict the mining behaviors of others, and then develop optimal reaction strategies based on an equilibrium analysis. Moreover, game theory can be utilized to develop incentive mechanisms that discourage the nodes from executing misbehaviors or launching attacks. As such, game theory is natural in the decision making of all the consensus nodes in the blockchain networks. See: https://arxiv.org/pdf/1902.10865.pdf

capable of solving the so-called double-spending problem and the Byzantine Generals problem[13]. While the double-spending is a potential problem unique to digital currencies and assets since digital information can be reproduced relatively easily, the latter is endemic to distributed systems (Berg et al., 2019) and questions how distributed computer systems could reach a consensus without relying on a central authority, in such a way that the network of computers could resist an attack from ill-intentioned actors (Wright and De Filippi, 2015, p. 5). Although theoretical solutions were highlighted in a 1982 paper by Leslie Lamport, Nakamoto's implementation of Blockchain technology was the first to provide a de facto Byzantine-Fault-Tolerant consensus[14] (Huckle and White, 2016, p. 5).

The combination of security and transparency is what makes the blockchain a so-called *trust-free technology* (Beck et al., 2016), a *trustless system*, a *trust machine,* which can constitute the foundation for genuinely *trust-free economics* (Glaser, 2017, p. 1543). "Introduced by Greiner and Wang (2015), the notion of trust-free systems proposes the utilization of the capability of blockchain technology to automatically create an immutable, consensually agreed, and publicly available record of past transactions that is governed by the whole system to mitigate trust issues in peer-to-peer systems" (Hawlitschek et al., 2018, p. 58). Within the blockchain, the creation of the immutable, consensually agreed, and publicly available record of past transactions takes place through the so-called *Consensus*; it means that participants in a network have confidence that their ledgers are both accurate and consistent (Werbach, 2018, p. 12). The distributed consensus protocol (which can have several forms such as majority voting, priority voting or having a minimal number of votes) ensures the data integrity of the transactions (Ølnes et al., 2017). Of course, the way a consensus can be reached may vary depending on the rules and the type of blockchain being implemented (i.e., public, private, or hybrid). As will be shown, for example, public blockchains can be almost impossible to alter (if the will of the majority of its participants is lacking), while private blockchains are not. The nature of the network has consequences on the rights of its participants (as shown by Bacon et al., 2017), and consequently on their trust with respect to data integrity or the ledger itself as well. This aspect must not be underestimated, since "in the context of the digital revolution, who, what, when, and how people "trust" is changing" (Fenwick and Vermeulen, 2018). Therefore, researchers must fully understand what this means. "If the blockchain endogenizes the manufacture of trust, lowering the

[13] The problem of the Byzantine Generals describes a class of engineering failures in which a system needs to reach a consensus but fails to do so because of inconsistencies in communication (a Byzantine fault). "The description of the problem in Lamport, Shostak, and Pease (1982) is as follows: the Byzantine army surrounds an enemy castle. The army is divided into divisions, each of which is led by a general. The generals need to come to a consensus over a plan to attack the castle. However, not all of the generals are loyal – a certain number of the generals are traitors, who either wish to prevent consensus or for the generals to come to a consensus on a bad plan. The messengers that pass information between the generals could be killed – and information therefore does not get through or is late. This is described as asynchronous messaging. In the simplest set up of the problem, consider an army with three generals and a binary decision about whether to attack or retreat. Each general sends a message to the other two generals concerning their proposed action and wait for messages from the other. If the traitorous general shares contradictory messages (that is, recommending to one that they attack, and the other that they retreat) then coordination will fail, risking subsequent defeat in battle. In order to tackle the fact that a 'bad plan' is hard to formalize, they designated one general as a commanding general who was tasked with formulating the plan and distributing orders to the others. Any general, commander or lieutenant, can be a traitor. Thus, the problem of the Byzantine Generals is that 1) all loyal generals need to obey the same order, and 2) if the commanding general is loyal, then all loyal generals obey the order of the commanding general. Metaphorically speaking, traitorous generals are unreliable components that report inconsistently to other distributed components, impeding consensus. Lamport, Shostak, and Pease (1982) sought to discover the proportion of loyal/traitorous generals that a distributed system could handle. Their finding was that, contrary to prior belief, under the simplest set up, three generals were not tolerant of one of their members being traitorous" (Berg et al., 2019, p. 3).

[14] However, as it will be shown further, this robustness can be overcome by the so-called "51% Attack".

cost of trust" (Davidson et al., 2018) and constituting a new type of trust (Wright and De Filippi, 2015), what kind of trust will it be? How will it influence users' behavior? Therefore, the central question is not how to regulate blockchains (Werbach, 2018, p. 1) but how blockchains will regulate human behaviors and trust. Technologies can operate as a kind of law, regulating the behavior of their users (Werbach and Cornell, 2017, p. 1). The set-up of the blockchain allows actors to trust the technology, which originates from the need to trust involved actors (Finck, 2017). Is the need to trust other people in a blockchain network eliminated using the technology or is trust just displaced onto other parties? (Walch, 2017b, p. 4).

Clear evidence exists that inter-organizational and interpersonal trust differ because the focal point also differs (Rousseau et al.,1998). In an analysis of the sharing economy, Hawlitschek et al. (2018) categorized trust in i) peers, ii) platform, and iii) product, applying the same distinction to blockchains, as recalled by Keymolen (2013, p. 135); "In analyzing trust online, one has to take into account the specific workings of the online technology, its mediation (Verbeek 2011b), to see if and how measures have to be taken to ensure trustworthy online interaction". For example, the varying nature of the blockchain has consequences on the trust needed among its participants, e.g., private blockchains can make use of more lightweight consensus mechanisms than public blockchains by relying on a certain level of trust in participants (Buterin, 2015, cited in Risius and Spoher, 2017, p. 8).

According to certain scholars, a new form of *algorithmic trust* is created with the blockchain that distinguishes it from the more traditional typology of trust that initially existed only between human agents (Swan and De Filippi, 2017), representing "a shift from trusting people to trusting math" (Antonopoulos, 2014 quoted in Atzori, 2015, p. 2). At the bare minimum, trust must be placed in the underlying cryptography (Hileman and Rauchs, 2017, p. 17) that allows all participants to scrutinize each operation (Wright and De Filippi, 2015). This transparency and the confidence placed in "the security and auditability of the underlying code" (Wright and Filippi, 2015) is what appears to be enough with which to claim the superfluity of trust and correlated institutions.

As seen above, trust concerns the expectations and vulnerability of the parties involved (Rousseau et al., 1998), and can be expensive to manufacture conventionally (Davidson et al., 2018). Conversely, a technological system plays active roles in shaping the way we understand our activities, experiences, and relations with other people (Reijers and Coeckelbergh, 2016). As stated, in distributed ledgers trust is enforced by the rules governing the network; hence, the blockchain seems to operate a shift that replaces trust among participants with the properties of technology. In this process, it seems that there is no space for the willingness of the actors to accept vulnerability. Does this constitute *trustless trust* (Werbach, 2018, p.58)?

The blockchain promises do not lower expectations, generate value, and reduce or remove vulnerability – rendering relations a simple matter of choice and technology[15] (Reijers and Coeckelbergh, 2016) – through immutability and consensus. Will this be enough?

[15] The authors affirm that within a blockchain environment, social relations may become increasingly rigid due to the constraint and the modus operandi of the technology itself. In line with the characteristics of the blockchain, "our social relations are transformed in such a way that they become rigid, irreversible and non-negotiable." See: Reijers and Coeckelbergh, 2016, p. 121

Immutability and Forks

Blockchains are permanently distributed spreadsheets or ledgers in which information can only be added and never deleted (Gabison, 2016, p. 328). Information on a blockchain is seen as “immutable” or “indelible” (Yermack, 2018, p. 14), which serves as one of the primary selling features of blockchain technology (Walch, 2017, p. 736). Data accuracy and immutability are the two features that have shaped the blockchain as an alternative trust-reinforcing mechanism in our societies and economies (Akgiray, 2019).

There is an active debate on how immutability in blockchain systems is created (Walch, 2017). However, as with “trustlessness”, absolute immutability does not exist, due to the fact that blocks comprising transactions can be reversed, in theory, if enough nodes decide to collude (Hileman and Rauchs, 2017, p. 17). This particular feature is strictly intertwined with the “nature” of the implemented blockchain, i.e., public, private, or hybrid. For example, while public blockchains can be considered immutable in the sense that it is costly to rewrite history on a blockchain and there is no single point of failure[16] - SPOF (Abadi and Brunnermeier, 2018), private blockchains could simplify reversing transactions (Hileman and Rauchs, 2017).

Immutability may also refer to the resilience of the distributed system, which, in missing the single point of failure, may not be easily attacked or shut down, thus becoming invulnerable. However, “Blockchain-based systems are not invulnerable. […] Nakamoto’s solution to the Byzantine Generals problem is remarkably robust, but a “51% attack” can overcome it” (Werbach, 2018, p. 25); this could occur if a party or colluding group controls at least 51% of the computing power of the network, having the authority to determine what is recorded and what is not, and even potentially to revise the existing records[17] (Walch, 2017, p. 739). Moreover, the chance exists that a blockchain can be partly rewritten if the majority of a community supports a (*hard*) *fork* (Yermack, 2018, p. 14).

Real-world events have demonstrated that the unchangeable nature of a blockchain record is always limited by the decisions taken by its human governors to change it (Walch, 2017, p. 713). Blockchain coordination changes and adapts not only to the technological limitations of the available protocols but to the mutual expectations and influence of interacting stakeholders (Berg at al., 2018) by reaching a consensus. If a consensus fails to form, as for the adoption of new rules, either temporarily or persistently, we describe the event as a “fork” (Atik and Gerro, 2018, p. 7). Generally speaking, forking is an event that occurs in an open-source project when the code base is copied and changed, creating a new project (Berg et al., 2018, p. 4), but on a blockchain, a fork is created whenever the rules governing that blockchain are changed. We speak of a *soft* fork when some users on a single blockchain may continue to use the old rules without using the features in the new software; a hard fork occurs when part (or all) of the community decides to change the rules governing the blockchain (Abadi and Brunnermeier, 2018). It concerns the split of a unique system in two, where each one will have its own independent rules and functioning. The transactions that occurred before the hard fork will be found on both blockchains (Shakow, 2018, p. 2).

Practically, forks are blockchain-specific events that evoke elements of both “exit” and “voice” in the sense of the Exit-or-Voice reaction paradigm first set out by Alfred O. Hirschman (Atik and Gerro,

[16] A single point of failure (SPOF) is a part of a system that will prevent the entire system from working, should it fail.

[17] The chances of suffering a 51% attack decrease or increase depending on the size of the network (e.g., major public networks are considered large enough to resist a 51% attack since it would prove too costly to represent (or convince) 51% of the network and also very expensive to recalculate all the blocks).

2018, p. 2). Forking can be considered a form of group secession (exit) that takes an existing set of institutions and creates a new 'society' with a shared history but divergent futures (Berg and Berg, 2017), eliminating the inefficiencies arising from switching costs in centralized record-keeping systems (Abadi and Brunnermeier, 2018). If certain participants do not like the output of a governance process, they can choose a hard fork, starting their own independent chain (Barrera and Hunder, 2018). Practical examples are provided by the bitcoin forks[18] that have occurred in previous years or the 2016 DAO case[19].

Although the blockchain could be considered "censorship-resistant" (Werbach, 2018, p. 22), since information can be published and distributed across hundreds of thousands of computers, rendering it virtually impossible for any single entity to censor (Wright and De Filippi, 2015, p. 13), as shown, it is not immutable. Especially in the case of public blockchains, it is subject to the will of its participants and their appreciation of the outcomes. Thus, the possibilities offered by this technology make it "more feasible for individuals to exit political-socio-economic systems at the level of the system itself, and elect to accede freely to institutional systems which formulate, promulgate, keep and verify institutions and public records without a centralized authority" (Markey-Towler, 2018, p. 1). This process could result in controversial situations in which converging and conflicting private interests into the common interest will not always be possible without the leadership of a central and recognized authority.

Therefore, we suggest that the current state of the art of blockchain implementations, apart from the noise claims, has not yet proved that this technology will be able to completely replace the role of institutions when it comes to trust. As seen, trust comprises vulnerability, risk, and expectation; in the blockchain environment, there appears to be no space for vulnerability. Conditions are set ex-ante, and moreover, as in the case of forks, these can be changed by the majority of the community. This process does not ensure that the rights of all participants will be weighted in the same manner and these rights will be respected. In this process, there is no space for compromise, in which people are given the simple option of leaving the network (fork). The same logic is applicable both at micro and macro level. Will it be possible to fork from community and society?

b) Will the blockchain enable decentralized governance?

To interact in society, we must be guaranteed certain reciprocity and security concerning exchange and property (Markey-Towler, 2018, p. 6). Traditionally this has been made possible by the centralized state. Decentralized architectures are currently gaining popularity to protect one's privacy against the pervasive surveillance of states and corporations (De Filippi, 2016). There is a progressive disengagement of citizens in local politics, and growing distrust in existing institutions (De Filippi, 2018); it is a question of public trust (Maupin, 2017) to which the blockchain responded as a social and economic movement that aims to provide transparency, self-regulation, and efficiency (Koletsi, 2019). Blockchain technology may disrupt any centralized system that coordinates information by providing a more efficient decentralized alternative compared to the conventional combination of

[18] The first hard fork splitting bitcoin occurred on the 1st August 2017, resulting in the creation of Bitcoin Cash. Many other examples can be found at: https://bitcoinexchangeguide.com/bitcoin-blockchain-forks-history/

[19] References to this case can be found in Walch (2017), Sulkowski (2018); Ishmaev (2018), among many others.

firms, markets, and states (Davidson et al., 2016), giving an opportunity for individuals to coordinate common activities, interact directly with one another, and govern themselves in a more secure and decentralized manner (De Filippi, 2018b).

The possible decentralization operated by blockchain-based systems has the advantages of missing a single point of failure (Atzori, 2015) with the provision of a complete, transparent, and intrinsically valid historical transaction log (Hawlitschek et al., 2018, p. 52). It is claimed that the blockchain provides a technical solution (i.e., a cryptographic consensus) to the problem of cooperation in joint or group production at scale[20], while still maintaining the benefits of commons-type (i.e., polycentric) institutional governance (Davidson et al., 2016b, p. 13). It may bring trust and coordination to shared resource pools and facilitate new models of non-hierarchical governance in which intelligence is expanded to the edges of the network instead of being concentrated in the center (Wright and De Filippi, 2015, p. 38). On these bases, it can be considered a hyper-political tool, capable of managing social interactions on a large scale and rendering traditional central authorities obsolete (Atzori, 2015, p. 1). It may foster 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 and De Filippi, 2015).

Blockchain technologies open a discussion on the necessity or possibility of a new type of social contract (Koletsi, 2019). A first and intriguing analysis of the philosophical background that may lay behind the blockchain is provided by Reijers et al. (2016), who examine how blockchain technologies can produce models of governance and how these models of governance are justified. The authors start from the consideration that the social contract for blockchain technologies can be understood as the underlying model for the governance of blockchain-based interactions. Reijers et al. conclude that blockchain governance justification relies on a Hobbesian conception of human nature; while blockchain governance reflects Rousseau's idea of sovereignty[21] that is implemented in a decentralized manner.

Atzori (2015, p.21) states that the reason for the original creation of the central coordination of public institutions was to protect the common good and collective rights in the long term from transitory individual interests and any reckless logic of profit. Thus, if the centralized institutions are working for the general interest, it is natural to ask ourselves; "Is decentralization a good idea? Is it economically feasible? What are the social consequences of decentralization?" (Narayanan et al. 2016, quoted in Oh and Wallsten, 2018).

Even if some skeptics argue that no one knows the meaning of 'decentralization' (Walsh, 2019), according to Kaal (2019) the four general types of decentralization refer to; 1. Technology; 2. Organization; 3. Market; 4. Society. These types of decentralization are subject to iterative decentralization processes and affect each other by way of feedback effects. This pattern may alternatively be described as follows; (1) the blockchain is considered a viable substitute for central ledgers; (2) in the long-run the historical effect of blockchain technology is to disrupt the economic

[20] The authors refer to the to the eight core design principles for the efficacy of groups identified by Wilson, Ostrom and Cox in 2013. See: Wilson, D. S., Ostrom, E., and Cox, M. E. (2013). Generalizing the core design principles for the efficacy of groups. Journal of Economic Behavior and Organization, 90, S21–S32. doi: 10.1016/j.jebo.2012.12.010

[21] According to Reijers et al. (2016), Rousseau's ideal of a general assembly that encompasses all the members of a community could be technically realized in blockchain governance. For Rousseau, sovereignty can never be alienated from the individuals forming society and, as such, sovereignty is always vested in the will of the people – in a decentralized manner, not residing in a centralized assembly or monarch (as it is for Hobbes).

value of hierarchy (Berg et al., 2018), perhaps with a system of distributed, bottom-up cooperation (De Filippi, 2018); (3) decentralized technology inaugurates new forms of economic exchanges – historical evidence has demonstrated that every time decentralization emerges in a given industry, profit margins disappear (Kaal, 2019); (3bis) the comparative efficacy of blockchains in coordinating information between decentralized agents [which, following Hayek, (1945) is perhaps the most fundamental economic problem of creating an orderly economic system (Allen, 2019, p. 7)] results in new configurations of the market; (4) distributed ledger technology affects industrial capitalism, which is based on centralized ledger technology (Berg et al., 2018), transforming it and thus current societal institutions. Thus, is the blockchain environment capable of leading to the experimentation of new forms of governance and relations (Berg et al., 2018)?

As seen in the case of the fork, “what is revolutionary about this technology is that it makes even yet more viable what Albert Hirschman (1970) called the “exit” response to the decline in organizations” (Markey-Towler, 2018, p. 3). “Blockchain technology is by design a multi-user system. It is designed for continuous, non-centrally governed interaction among (large) heterogeneous groups of participants. Furthermore, it supports the independent development and deployment of autonomous, collaborative, and highly interoperable services by every user of the system” (Glaser, 2017, p. 1550). Blockchain technology is expected to facilitate direct interaction between citizens, providing administration without a governmental administrator and tailoring services provided by governments (Keyser, 2017 quoted in Ølnes et al., 2017, p. 362). It is even believed by some that it represents the coming of a stateless global society (Atzori, 2015) or a *decentralized autonomous society* (DAS) with no space for centralized forms of power and control (Garrod, 2016). DAS supporters start “from the assumption that there is no trust and no community, only individual economic agents acting in self-interest” (O'Dwyer, 2015 cited in Garrod, 2016, p. 67). There is no space for the notion of a social contract (Reijers et al., 2016). The idea to use secure encryption to protect citizens’ freedom and privacy and do away with governments and the surveillance of big corporations can be traced back to the cyberpunk and crypto-anarchist culture of the late 1970s (Atzori, 2015). The blockchain rekindled the cyber-libertarian flame (Werbach, 2018); anarcho-capitalists conjoin decentralization, individualization, and privatization (Flood and Robb, 2017). Conversely, we find some authors, such as Markey-Towler (2018), for whom the blockchain is revolutionary because it could make the anarchist utopia a reality, or Huckle and White (2016), who investigate if the technology is directly applicable to socialism since a public blockchain advocates community ownership.

Nevertheless, does community ownership mean *social* (or socialist) ownership? Can socialism be considered a synonym of community government and governance? According to Kaal (2019), relying on notions of open-source volunteer contributions and greater good perspectives for society, decentralization transcends the traditional economic notions of capitalism and socialism, combining both for the simultaneous generation of profits and redistribution of resources. So, the blockchain could help implement new forms of decentralized models of commons-based management, since it “enables collective organizations and social institutions to become more fluid and promote greater participation, potentially transforming how corporate governance and democratic institutions operate” (Wright and De Filippi, 2015, p. 3).

As will be shown, the widespread adoption of smart-contracts could also make it easier “to create custom legal systems, where people are free to choose and to implement their own rules within their own techno-legal frameworks” (Wright and De Filippi, 2015, p. 40). The development of non-centralized political and socio-economic systems could derive from "polycentric systems (which are) are more likely than monocentric systems to provide incentives leading to self-organized, self-corrective institutional change" (Ostrom, 2010; quoted in Shackelford and Myers, 2017, p. 35). Blockchain technologies can configure specific forms of political organization (Reijers et al., 2016), in which "individuals could find new ways to spontaneously organize and coordinate themselves into transnational cloud communities and even acquire their own self-sovereign identity that subsists independently of any nation-state" (De Filippi, 2018, p.1).

Obviously, the terms of comparison are only possible with previously known or experienced models of society. However, looking at the potential shift from trust in people to trust in technology, thanks to the blockchain, the institutional structure of society could shift to one that is computationally based with a diminished need for human-operated brick-and-mortar institutions[22] (Swan and De Filippi, 2017, p. 4), and thus resulting in something completely new.

Just as the platform economy[23], the Internet of Things[24], and Big Data[25], distributed ledgers pull in online systems and business processes previously conducted offline (Finck, 2017, p. 20), pushed by societal trends towards a networked society[26] and platform-mediated services[27] (Glaser, 2017). Without proper steering, this transformation may lead to significant problems, especially in relation to power dynamics. As Atzori (2015, p. 29) warns; "In a world increasingly reliant on technology and ruled by networks, whoever owns and controls these platforms always has significant power over civil society." How will we deal we this phenomenon? What kind of instrument can we rely on?

As seen, decentralization may work on several levels, having a twofold impact:1) within the economic domain, converting the hierarchical structure of the market into a horizontal one; 2) the disruption of public institutions, which have the role of representing the general interest, and thus the introduction of issues with power relations dynamics among individual and network, and network(s) and network(s). We have to understand how to tackle and judge these possible outcomes.

[22] Brick and mortar (also bricks and mortar or Band M) refers to the physical presence of an organization or business in a building or other structure. The term brick-and-mortar business is often used to refer to a company that possesses or leases retail shops, factory production facilities, or warehouses for its operations. More specifically, in the jargon of e-commerce businesses in the 2000s, brick-and-mortar businesses are companies that have a physical presence (e.g., a retail shop in a building) and offer face-to-face customer experiences. See: https://en.wikipedia.org/wiki/Brick_and_mortar

[23] The platform economy is economic and social activity facilitated by platforms. Such platforms are typically online matchmakers or technology frameworks. See: https://en.wikipedia.org/wiki/Platform_economy

[24] The Internet of Things (IoT) is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that is provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. See: https://en.wikipedia.org/wiki/Internet_of_things - Consulted on September 4, 2018

[25] "Big data" is a field that treats ways to analyze, systematically extract information from, or otherwise deal with data sets that are too large or complex to be dealt with by traditional data-processing application software. See: https://en.wikipedia.org/wiki/Big_data -Consulted on September 4, 2018

[26] Network society is the expression coined in 1991 related to the social, political, economic and cultural changes caused by the spread of networked, digital information and communications technologies. See: https://en.wikipedia.org/wiki/Network_society - Consulted on September 4, 2018

[27] A platform-mediated ecosystem can be broadly defined as an industrial architecture with an infrastructure in the center that facilitates value co-creation among different agents (platform owners, supply side, and demand side) and a set of rules (governance) regulating their interdependencies (Tiwana, 2014). See: https://pdfs.semanticscholar.org/4622/6f2bbc80b0dedd75974484e0710b681b9534.pdf- Consulted on September 4, 2018

c) What will the relationship between the blockchain and the law be?

Decentralized networks of cryptography-based economic activities are a relatively new phenomenon, and societies need to understand the potential liberties and restrictions that come with them (Risius and Spoher, 2017). Blockchain systems prompt a reconsideration of two of the central legal devices of modernity: the ledger and the contract (DuPont and Maurer, 2015, p. 2). At the same time, the blockchain has been defined as the emergence of a new species of economic coordination: governments, firms, markets, and relational contracting (Davidson et al., 2016, p. 3). These domains are ruled by the law in order to ensure standards, maintain order, resolve disputes, and protect liberties and rights. Laws, codes, regulations, and norms that exist today have been promulgated for a substantially analogical world (and human being). The situation may change quickly. Will this require a general reconsideration of the way laws are constructed and the goals they aim for? How will the law deal with the blockchain, its implementations, and its repercussions?

There are various ways in which law and technology can influence each other. The two interact through a complex system of dependencies and interdependencies, both contributing to the regulation of individual behaviors (De Filippi and Hassan, 2016). Hence, technological advancements may hold the potential to alter our conception of the law[28] (Werbach and Cornell, 2017), and result in a new subset of law or even function without a legal framework (Sulkowski, 2018). In fact, as Wright and De Filippi (2015) claim; "the blockchain could support and facilitate the deployment of a decentralized alternative to the current legal system, a new digital common body of law, called *Lex Cryptographia,* based on rules administered through self-executing smart contracts and decentralized (autonomous) organizations. An interconnected system of rules interacting with one another, in a reliable and predictable way, without the need of any third-party institution to enforce these rules."

The blockchain is implemented in a space where *code is law*[29]. Lawrence Lessig originally meant 'code is law' as a metaphor, where "code controls behavior as the law might control behavior" (Zetzsche et al., 2017, p. 24). Thus, code – as well as markets and norms – is just one coequal modality of regulation[30] (Werbach, 2018). In following this line of reasoning, it is possible to conceptualize computer code as constitutional rules (Rajagopalan, 2019). Platform-based technological applications such as blockchain possess working rules which convey a sense of constitutionalizing amongst developers and users (Berg et al., 2018). According to Wright and De Filippi (2015, p. 26), over time, law and code may merge so that the only way for people to break the law is to effectively break the code. However, the two languages currently still differ. "Legal code is primarily extrinsic[31]; technical

[28] The Authors refer to Lessig (1999) who claims that "code is law", thus technologies can operate as a kind of law, regulating behavior of their users.

[29] Lessig L., "Code and other laws of cyberspace", New York: Basic Books, 1999.

[30] "According to Lessig (1999) four different forces exist, which all contribute — to a greater or lesser extent — to shaping individual actions, in ways that often remain outside of the control of any given individual alone. 1. Law creates artificial constraints limiting individual actions through legal rules and regulations (e.g., by making it illegal for people to steal, and punishing those who infringe these rules). 2. Social norms regulate cultural behaviors through peer pressure (e.g., by making it socially unacceptable for people to speak loudly in a professional meeting). 3. The market encourages or discourages specific behaviors through the mechanism of supply and demand (e.g., by setting prices for specific goods or services). 4. Architecture (defined by Lessig as "features of the world, whether made or found") imposes a series of constraints by limiting the type of actions that an individual can do (e.g., biology, geography, technology are all, to some extent, constraining people's actions)" (De Filippi and Hassan, 2016).

[31] As will be shown, law needs third parties for enforcement, while code does not.

codes are primarily intrinsic in comparison, meaning when rules are breached the errors are returned, and no activity occurs such that compliance is ensured through the employment of the codes. Technical codes also follow the rules rigidly by nature, such that these are adhered to even where compliance generates undesirable or unforeseen outcomes" (Yeoh, 2017, p. 5). This kind of "inflexibility" will be addressed later with the introduction of smart contracts. However, the relation between code and law is not as straightforward as it may seem; e.g., the differences of the two languages are an obstacle to take into consideration when it comes to the design of blockchain features by developers or norms and regulations by institutions. Nowadays, the relation between the blockchain and the law is substantially threefold; according to Werbach (2018) the blockchain can interact with the legal system:

> 1) as a supplement; there is an existing trust architecture that works appropriately (so no additional work is needed to establish trust), and the blockchain operates as an additional layer subject to established legal rules. In this case, the primary value proposition is the speed and efficiency gain compared to a centralized ledger. The blockchain is used solely to protect the integrity of data on the shared ledger.
>
> 2) as a complement; it may work in scenarios where trust based on the legal system is breaking down or insufficient. Distributed ledgers can complement and extend the existing trust architecture. This is the case when the blockchain powers new markets, being complementary to existing legal arrangements.
>
> 3) as a substitute; there is no backstop of traditional legal enforcement, and it can be envisaged in cases in which legal enforcement is weak.

In our understanding, the first two cases constitute what is being implemented most commonly, while the third hypothesis is the least plausible, since the implementation of a blockchain in an environment with no rule of law is unlikely to solve issues outside the digital realm. However, the situation may evolve so much that there can be no certainty with which to prove this affirmation as necessarily true.

Regulatory challenges

The relationship between technology and law has evolved significantly, as the former is being increasingly used as a complement or a supplement to the latter (De Filippi and Hassan, 2016). Although regulators have long rejected the 'code is law' maxim in its absolute version (Finck, 2017, p. 13), in the digital world technology itself can be regarded as a parallel form of regulation (Wright and De Filippi, 2015). To achieve their massive potential and prevent catastrophic failures, blockchain-based systems will need to integrate with the operations and institutions of the law (Werbach, 2018). Legal theory seeks to harmonize and find an appropriate balance between public order and security with private interest, thereby guaranteeing economic growth, individual autonomy and fundamental rights (Wright and De Filippi, 2015). Will this role of mediating interests still be played? And how?

Moreover, current insufficient technological understanding could be translated into legislative risks (Walch, 2017). Many governments and central banks are now investing in blockchain solutions (Akgiray, 2019), although very few governments have adopted a comprehensive blockchain law[32]

[32] Delaware, a state on the east coast of the United States, has allowed the use of blockchain as a means to create and manage corporate records. A second example is in Arizona where smart contracts and blockchain based signatures have

(Zetzsche et al., 2017). Moreover, in the case of the blockchain implemented on transnational networks, the legitimate claim of jurisdiction over globally-connected, decentralized institutions must be determined by the laws of any one country (Hacker et al., 2019).

Legal challenges posed by blockchains should not be underestimated by regulators (Harwood-Jones, 2016 cited in Yeoh, 2017, p. 7). Certain core features, such as openness, lack of permissioning, and potential anonymity, make public blockchain systems problematic from a legal and regulatory perspective (Millard, 2018, p.845). Broadly speaking, there are three major types of controversy (Werbach, 2018): illegality (involving the use of cryptocurrencies to break the law, or theft of cryptocurrencies through hacking and similar means), classification (involving activity that is basically legitimate but not structured according to the legal requirements of the non-blockchain equivalent), and legal validity (how other legal structures recognize distributed ledgers), which may result in at least three major types of potential liability risk (Zetzsche et al., 2017): i) ledger transparency risks (related to the violation of data privacy, insider trading and market abuse, and identity theft); ii) cyber risks (tampering with data prior to storage, brute force attack and cheating, double spending and distributed denial of service attacks); and iii) operational risks (insufficient coding, key person risk, negligent performance).

The scope of legitimate practices for blockchain-based systems is a governance question at its core, and not a computer science question (Werbach, 2018, p. 6). The policy ecosystem is not fully adapted to this technology, and rules and regulations will have to be modernized (Gabison, 2016). It is crucial for regulators to wait until its benefits (and failures) have been uncovered before moving to pass laws concerning best practices (Schakelford and Myers, 2017). Governments should tackle the increasingly disintermediated global economy by focusing on distributed ledger technologies and individual use cases rather than underlying enabling technologies (Maupin, 2017, p. 1). No 'one-size-fits-all' legal analysis is possible. Instead, each application of blockchain technology will need to be considered on its facts (Bacon et al., 2017). Legal and regulatory issues must be considered in the specific context of individual use cases and evidence of concept and pilots, since the technical complexity and the delivery timeframe will vary, and so will the legal questions (Zetzsche et al., 2017, p. 23).

To fully realize the potential of the blockchain, it is paramount to acknowledge the need to undertake a careful mapping of the respective roles of the "dry code" of cryptography and the "wet code[33]" of law (Werbach, 2018, p. 7), since distributed ledgers could be regulated by both legal and technical codes (Yeoh, 2017, p. 5). As previously noted, the differences between the two codes are evident when it comes to analyzing the language needed to implement them. Blockchain technology still has a fluctuating terminology that can cause difficulties for global regulators seeking to understand and govern the technology appropriately (Walch, 2017).

Much of the regulation involved is a classification exercise - the rules establish status categories, and the regulators police who is subject to those categories (Werbach, 2018, p. 38), e.g., from a technical standpoint, blockchains are only one subset of distributed ledger technologies (Maupin, 2017). The lack of a precise vocabulary around blockchain technology does not help and serves to increase the

been given full legal status. Another country that is leading the "blockchain race" is Estonia (Fenwick and Vermeulen, 2019). Other examples can be found at: https://blockchainlawguide.com/blockchain/

[33] N. Sazbo introduced the distinction between wet code (what lawyers practise) and dry code (operations confined to and executed by computers) in 2008, available at: http://unenumerated.blogspot.com/2006/11/wet-code-and-dry.html

need for regulators to learn from the industry itself, which in turn could increase the risk of errant risk analysis or under-regulation (Walch, 2017). On the other hand, the inherent ambiguity of the legal system — necessary to ensure that the law is justly applied on a case-by-case basis — ultimately gives software developers and engineers the power to embed their own interpretation of the law into the technical artefacts that they create (De Filippi and Hassan, 2016). Synthetically, problematic vocabulary increases the chances of (1) regulatory capture (and the risks that accompany it), (2) inconsistent regulation across subject-matter domains and jurisdictions, and (3) "perverse innovation" (Walch, 2017, p. 729). To address these problems, attempts to create a philosophy (Swan and De Filippi, 2017) and ontology (Tasca et al., 2018) of blockchains have been proposed.

The regulatory dilemmas include the classic conundrum when tackling innovative technologies or practices: finding just the right moment to regulate (Walch, 2017, p. 717). As F. Easterbrook has argued, new technologies do not necessarily call for new legal doctrines when fact patterns are fundamentally unchanged (Werbach and Cornell, 2017, p. 24). This principle seems to fuel certain approaches that have been taken into consideration by regulators. According to Akgiray (2019), there are three types of regulatory positioning: 1. Study-and-Wait-and-See; 2. New legislation and regulation; 3. Guidance and sandboxing.

This classification can be split into a small number of approaches to manage the adoption of the appropriate regulation to be implemented. The first approach is based on *waiting and seeing* how the technology unfolds while continuing to apply existing legal frameworks (Finck, 2017). Most regulators are in this position, considering the blockchain as a comprehensive new business model (Akgiray, 2019). A second instrument is the so-called *safe harbor*. It is a regulatory provision that formally limits legal enforcement. When firms can take enough steps to police themselves, the safe harbor incentivizes them to do so by defining what specific conduct is necessary (Werbach, 2018). The third type of instrument found in the literature is the *recycle box*, which is implemented when minor adaptations to existing national and international regulatory frameworks are required (Maupin, 2017). The *dark box*, instead, employs blockchains or other DLTs to accomplish illegal objectives, per se. They call on regulators to develop more effective globally cooperating regimes for detecting, tracking, and prosecuting blockchain-based illicit activities (Maupin, 2017). And last, but not least, the *regulatory sandbox*[34], which can be defined as a set of rules allowing innovators to test their product or business model in an environment that temporarily exempts them from following some or all of the legal requirements in place (Finck, 2017, p. 14). Some jurisdictions have concluded that it is both premature to bring in new regulation and risky to just wait and see (Akgiray, 2019). In a similar vein to safe harbors, but limited in time and scale (Werbach, 2018), the sandbox uses cases utilize blockchains or distributed ledger technologies to pursue permissible objectives but in ways that entail regulatory risks, which, for reasons concerning the technical properties of blockchains, cannot be addressed without destroying the core value proposition of the existing regulatory regimes (Maupin, 2017, p. 1). The sandbox was first launched in the UK in 2015 and remains the most widely implemented. For the sandbox to be effective, Maupin (2017) identified at least four distinctive features: i) global reach – sandbox must have the capacity to tap competent authorities from any national jurisdiction in the process of evaluating and working towards creative regulatory solutions

[34] In computer security, a "sandbox" is a security mechanism for separating running programs, usually in an effort to mitigate system failures or software vulnerabilities from spreading. It refers to an isolated but fully functional testing environment where software, apps or programs can be tested. If a programmer writes a new piece of code, they may use a sandbox to test it.

for new use cases; ii) cross-sectoral flexibility – it must be able to assemble competent authorities from any sector that might conceivably be impacted by a blockchain; iii) a start-up-friendly operating structure – it must be accessible and useful for small start-ups with extremely small budgets and numbers of staff[35]; iv) use case-tailored parameter-setting practices – it must be capable of tailoring both the experimentation parameters it sets (aspects such as timelines, test customer profiles, etc.) and the oversight and data monitoring requirements it imposes on the specifics of the use case in question.

Excluding the case of the dark box, all of the regulatory approaches above are based on the necessity of assessing the impact of the applications of the blockchain at several levels before bringing its use onto a larger scale. In this way, the blockchain is replicating the regulatory curse of the Internet (Hacker et al., 2019). In keeping with the issues raised in the present paper, the following sub-topics are highlighted as critical within the realm of law regarding large-scale adoption.

Identity and Pseudonymity

If the price of centralization is trust, as users need to trust centralized operators with their data, decentralization comes at the expense of transparency, as interactions of those involved are made visible to each node in the network [36](De Filippi, 2016, p. 1). Transparency can thus be regarded as a means for the network to police itself by enabling users to collectively verify the legitimacy of every network transaction (Bradbury, 2013 quoted in De Filippi, 2016, p. 5). The transparency inherent to these networks is such that anyone could retrieve the history of every performed operation and rely on big data analytics to retrieve potentially sensitive information (De Filippi, 2016). Even if transparency is not necessarily in conflict with privacy (De Filippi, 2016), it is beneficial to data integrity, while also facilitating access to assets through identity theft (Zetzsche et al., 2017). Identity is a crucial component of any economic exchange (Berg et al., 2018), since we rely on having some level of assurance over the identity of the person or firm we are interacting with. Outside digital life, identity is typically social and intersectional (Immorlica et al., 2019). Identity technology represents the *sine qua non* of modern human activity; without it, it is virtually impossible to engage meaningfully in economic, social and political activities[37] (Allen et al., 2018). The definition of 'personal data' is very expansive, as it covers any information that relates to an identifiable person, i.e., a person who can be identified "directly or indirectly" (Bacon et al., 2017). The problem of maintaining control over and preserving transparency of our digital identity becomes urgent since our lives depend more on digital services, in which people have multiple identities depending on the

[35] This is clarified by the author by the fact that "most blockchain start-ups satisfying the sandbox criteria face a chicken-and-egg problem. They cannot scale without obtaining some modicum of regulatory certainty, but they do not have sufficient bandwidth to engage in labyrinthine regulatory processes across multiple jurisdictions whose approvals they would need in order to scale safely" (Maupin, 2017, p. 16).

[36] Decentralized architectures generally rely on the disclosure of each user's interactions for effective coordination amongst a distributed network of peers.

[37] Identity is a coordination problem. More complex or significant transactions demand more formal identification of the parties involved. Identity institutions are crucial and valuable infrastructural technologies of any complex society. Identity technologies are adopted by market participants in order to prove and verify identities as markets gain complexity. (When we write 'identity technologies', this is shorthand for technologies that allow individuals to provide evidence of their identity and counterparties to verify those claims.) This approach to identity views identity as fluid, contextual and subjective. Individuals possess many 'identities' depending on the social, economic, and political context in which they are operating. In the legal-centric theory of identity, contrastingly, identity is singular, uniform and permanent. Governments establish identity in order to extract revenue and distribute rents. To know more, see: Berg, A., Berg, C., Davidson, S. and Potts, J., The Institutional Economics of Identity (May 25, 2018). Available at SSRN: https://ssrn.com/abstract=3072823 or http://dx.doi.org/10.2139/ssrn.3072823

activity in which they are involved[38] (Gabison, 2016). Furthermore, due to its pseudo-anonymous nature blockchain technology is likely to fulfill individuals' desires to maintain a wide range of identities while maintaining their privacy (Berg, 2018 cited in Allen et al., 2018, p. 16). To this end, permissioned blockchains offer clear advantages in security and privacy (Yermack, 2018, p. 16), since in public blockchain it is possible to de-anonymize a user by analyzing network traffic or the blockchain itself. So, even if pseudonymity is not enough to guarantee total anonymity (Conoscenti et al., 2016), and total anonymity is never guaranteed (De Filippi, 2016, p. 15), this pseudonymity also presents significant regulatory challenges (Wright and De Filippi, 2015, p. 21), especially concerning the regulation of behaviors and their consequences among blockchain participants, such as in the cases of agreements or contracts.

Smart contracts

A contract is a promise that can be legally enforced (Rodrigues, 2018, p. 26). "Blockchain can be regarded as a 'paradigm-shifter' in the sphere of contracting; it allows automation of the process of contractual performance of both parties" (Savelyev, 2017, p. 121). Electronic contracts are nothing new, the innovation here comes from "the fusion of two lines of technological development: electronic contracting and cryptography" (Werbach and Cornell, 2017, p. 5). Indeed, Nick Szabo, who clearly did not envisage any form of complicated technology, rather a simple vending machine (Werbach and Cornell, 2017, p. 9) when writing in 1994, defined electronic contracts as "a set of promises, specified in digital form, including protocols within which the parties perform on these promises." Smart contracts can be considered just one example of a larger trend of computerized technologies purporting to displace or replace human decision-making (Werbach and Cornell, 2017, p. 56). This trend of automation is motivated by three well-known difficulties with natural language and human institutions: i) ambiguity; ii) corruption; iii) enforcement (Grimmelmann, 2019).

With smart contracts, a distributed ledger becomes a distributed computer (Werbach, 2018, p. 16), that can theoretically be used to create any number of social contracts[39] (Garrod, 2016, p. 62), threatening the position of a wide range of intermediaries that provide trust or overcome the lack of trust (Arruñada, 2018, p. 6). Smart contracts are believed to offer the hope — or possibly the threat — of circumventing Hobbes' age-old essential role of law[40] (Werbach and Cornell, 2017, p. 3).

Based on the current understanding and properties revealed by smart contracts, Savelyev (2017, pp. 124-127) identifies the following features: (1) *solely electronic nature* – smart contracts can only exist in electronic form; it is not possible to use any other form of contract for them (e.g., a written hardcopy); (2) *software implementation* – contractual terms are manifested in computer code, therefore it is possible to argue that each "smart" contract by is also a computer program by its legal nature; (3) *increased certainty* – a computer language does not allow for discretion in its interpretation by the machine. Smart contract terms are interpreted by machine on the basis of Boolean logic[41]; (4) conditional nature – conditional statements are foundational to computing as they are based on statements such as 'if "x" then "y"'; (5) self-performance – once a smart contract is concluded, its

[38] E.g., how many usernames and passwords do you use?

[39] With the expression "social contract", the author refers to such examples as: non-geographic countries (complete with taxes, benefits, and voting), transnational lending programs, universal basic income schemes, marriage contracts

[40] Hobbes' basic idea—that binding agreements require a system to ensure that counterparties can trust one another to perform—is an intuitive and powerful argument for the essential role of law (Werbach and Cornell, 2017, p. 2)

[41] Boolean logic is a form of algebra in which all values are reduced to either TRUE or FALSE. See: https://www.webopedia.com/TERM/B/Boolean_logic.html - consulted on June, 15 2018.

subsequent performance is no longer dependent on the will of its parties or a third party; (6) self-sufficiency – a smart contract requires no legal institutions to exist.

In taking these characteristics into consideration, the interpretation of smart contracts has become an object of debate, since there remains no universally agreed definition (Savelyev, 2017, p. 120). The very concept of smart contracts may be the result of a series of terminological misunderstandings characterized by the inconsistent and incorrect use of legal terms (Mik, 2017). Thus, can a smart contract be considered a contract?

It is claimed that a blockchain is an economic world of complete contracts (Davidson et al., 2016b, p. 9). However, "no physical representation of an agreement can ever entirely represents the agreement. Though we informally speak of contracts as pieces of paper or text on a screen, contracts are intangible. They are enforceable agreements" (Kolber, 2018, p. 219). The meaning of a legal contract is a social fact (Grimmelmann, 2019), which explains the necessary incompletion of all contracts (Rodrigues, 2018)[42].

According to general opinion, smart contracts are meant to be stand-alone agreements that are not subject to interpretation by outside entities or jurisdictions since they are self-executing (Rodrigues, 2018), in light of their self-performing property. Smart contracts are considered only those based on blockchain technology with electronic assets as their object to ensure its self-enforcing nature (Savelyev, 2017, p. 130). Allen et al. (2018) broadly define smart contracts as agreements — or parts of agreements – that are written into code at the top of a blockchain platform and can be automatically executed when specific conditions are validated. Therefore, smart contracts are more adequately understood as autonomous software agents (Finck, 2017) and algorithmic rules that automatically respond to inputs according to pre-programmed parameters (Howell and Potgieter, 2019).

Therefore, smart contracts are not "contracts" in terms of being legally enforceable promises with binding obligations on two parties seeking to broker a mutually beneficial exchange in the 'real' or 'physical' world (Howell and Potgieter, 2019). A smart contract is merely the code for the execution of the contract (Gans, 2019). A contractual agreement requires an offer and acceptance (to establish mutual consent), consideration (anything of value exchanged) and an intention to create legal relations (Zetzsche et al., 2017, p. 30). Smart contracts do not capture the dynamic processes of stipulating a contract; e.g., searching for partners, negotiation of terms, reaching an agreement, and monitoring and enforcement of performance of the agreed terms, which constitute the economic activity of real-world 'contracting' between human actors (Howell and Potgieter, 2019). A smart contract does not create obligations in a legal sense […] One of the key elements of obligation is (1) its orientation in the future and (2) a 'will' component. (Savelyev, 2017, p. 129). A smart contract, on the other hand, does not commit any party to do anything. It is not an exchange of promises or

[42] An intriguing and futuristic remedy for the incompleteness of contracts thanks to technological features (blockchain + artificial intelligence) is provided by Casey and Niblett (2017), who highlight "self-driving contracts" as a potential alternative to blockchain-based smart contracts. Recognizing the incompleteness of the contracts, the authors propose a "contract that writes its own terms or fills its own gaps. To be more precise, a self-driving contract has three key features. It is an agreement where (1) the parties set only broad ex ante objectives; but (2) the contract uses machine-driven analytics and artificial intelligence to translate the general ex ante objective into a specific term or directive at the time of performance; where (3) those terms are based on information gathered after the parties execute the initial agreement". See: Casey, A. J. and Niblett, A., Self-Driving Contracts (March 1, 2017). Available at SSRN: https://ssrn.com/abstract=2927459 or http://dx.doi.org/10.2139/ssrn.2927459

commitments (Werbach and Cornell, 2017, p. 22). Therefore, smart contracts cannot be considered contracts at all because there is no possibility of uncertainty in their execution and thus no compliance; strictly speaking, they are merely an example of automaticity created by the verification game (DuPont and Maurer, 2015).

A different interpretation is provided by Max Raskin (2017); rather than constituting legal enforcement at all, they are a form of self-help. To Raskin, "[a]utomated execution of a contract is a preemptive form of self-help because no recourse to a court is needed for the machine to execute the agreement" (Werbach and Cornell, 2017, p. 26). The code itself is the ultimate arbiter of the deal it represents (Savelyev, 2017, p. 125), and everything beyond the code is just an explanation (Werbach and Cornell, 2017, p. 29). As stated by Grimmelmann (2019), way to change the consequences of contracts on a blockchain is to change the semantics.

Viewed from this perspective, there is no legal point of intervention[43] as the code is self-contained (Rodrigues, 2018, p. 6). In fact, in contrast to traditional contracts, in which trust is placed in the personality of the other party in the contract, in smart contracts such trust is placed in the computer algorithm behind the agreement ('trustless trust') (Savelyev, 2017, p. 123). "If two parties engage in a contractual agreement using a smart-contract application, performance of contractual terms is guaranteed not by the goodwill of parties or third-party arbitrage but rather by the encoded algorithm" (Ishmaev, 2017, p. 667). Hence, crypto-contracts tend to build social and functional properties *within* the system (DuPont and Maurer, 2015, p. 8); i.e., without the necessity for arbitrating third parties. As shown by the failure of the 2016 DAO, even if no code can anticipate all the problems that could arise (Rodrigues, 2018), smart contracts have been considered good at setting forth anticipated conditions and consequences ex-ante and then ensuring that the effects occur upon the fulfillment of the conditions involved (Werbach, 2018, p. 53). By default, they implement a zero-tolerance policy by which parties have no choice but to execute the contract (Wright and De Filippi, 2015, p. 26), eliminating the act of remediation by admitting no possibility of breach (Werbach and Cornell, 2017, p. 4).

Therefore, the critical distinction between smart contracts and other forms of electronic agreements (and contracts in general) is enforcement (De Filippi and Wright, 2018; Werbach and Cornell, 2017, p. 15). Their distinctive aspect is the fact that they simplify enforcement; in fact, they make enforcement unavoidable (Werbach and Cornell, 2017, p. 28). Enforcement is automatic concerning a "smart contract" and does not depend on the law for enforcement (Rodrigues, 2018, p. 26). However, apart from optimistic claims, smart contracts may nevertheless require enforcers for contract completion, in a more traditional sense (Arruñada, 2018, p. 9). The flaw in the rationale is the failure to distinguish contractual execution from enforcement […] Execution of the agreement is automated, but enforcement is not (Werbach, 2018).

Furthermore, "the core peer-to-peer structure of blockchain faces insurmountable difficulties to reach contractual completion and to interact with the real world, two challenges that regards, respectively, contract (*in personam*) rights and property (*in rem*) rights" (Arruñada, 2018, p. 19). Smart contracts are limited by their nature to those contractual terms that can be specified in computer-readable code,

[43] "In the world of "smart contracting" on the blockchain, there is no place for the law to step in to supply default rules—*no legal intervention point*. The lack of a legal intervention point means that law on the blockchain works in a fundamentally different way from law in the corporeal world" (Rodrigues, 2018).

and still further limited by any constraints imposed by the blockchain system on which the contract operates. The "*fundamental smart contract challenge*" is related to performance obligations that must be verified in interactions with non-digital activities (Gans, 2019). As a result, they are unable to capture the real-world complexity of all but the simplest transactions (Bacon et al., 2017, p. 33). At this point a legal intervention does exist — not in the blockchain environment itself, but rather in the intersection of the blockchain features and the physical world (Rodrigues, 2018).

Moreover, another element of vulnerability is represented by the fact that smart contracts can have errors and security flaws like any other software code (Werbach, 2018, p. 25). Errors in computer code are prevalent and impossible to eradicate, and they increase with increasing code complexity as with conventional contracts (Arruñada, 2018, p. 15). Although proponents of smart contracts claim that many kinds of contractual clauses may thus be made partially or fully self-executing, self-enforcing, or both (Kakavand and De Sevres, 2016), certain contractual terms simply cannot be expressed through formal logic because they imply human judgment (Werbach and Cornell, 2017, p. 43). Several key legal concepts lack a binary nature, such as force majeure, material breach, and good faith, which cannot be translated into computer code (Vatiero, 2018).

Even considering the case of a smart contract operating precisely as designed, it may produce sub-optimal results – either in the minds of one or both parties or as a matter of economic efficiency – due to the fact that it is fixed (Werbach and Cornell, 2017, p. 44). As previously stated, the concept of incomplete contracts acknowledges that it is rarely possible for parties to consider every eventuality in contractual bargaining due to a combination of bounded rationality, transaction costs, verifiability, or other strategic reasons (Allen et al. 2018). Furthermore, "the more complex and unique the transaction, the higher the value at risk, and the harder it is to anticipate and precisely specify contingencies and measure and observe outcomes; the longer the timeframe between agreement and execution, the lower the likelihood that smart contracting will be more efficient than real-world contracting" (Howell and Potgieter, 2019 p. 1). Concerning their inflexibility, smart contracts underestimate a central problem of transaction cost economics: the need for an efficient adaptive mechanism (Vatiero, 2018). Therefore, even if smart contracts may economize on costs of enforcement compared to traditional contracts, they also impose potentially greater costs of negotiating agreements (Allen et al. 2018). Moreover, in preventing ex-post external adaptation, transaction costs may emerge or increase, so that traditional contracts may incur lower transaction costs than smart contracts (Vatiero, 2018).

Even if smart contracts are not intended to be legally enforceable (Werbach and Cornell, 2017, p. 20), there are two differing approaches at present that dispute a resolution for smart contracts: 1. Smart contracts can operate within the existing contract law framework and can be adjudicated by the courts or existing alternative dispute resolution (ADR) procedures (De Filippi and Wright, 2018); 2. Smart contracts are distinct legal tools rather than digital alternatives to traditional legal contracts (Werbach and Cornell, 2017), which may create new legal systems, a new *Lex Cryptographia* (Wright and De Filippi, 2015), or will require a 'distributed jurisdiction' – that is, blockchain-based governance (Allen et al., 2019).

As noted above, smart contracts are subject to significant limitations (Kaal, 2019). There is no reason, however, to suggest that they cannot coexist with the traditional contract (Werbach, 2018). From a practical perspective, it is possible to imagine that the choice between traditional and smart contracts will be a matter of economic efficiency and pragmatism (Howell and Potgieter, 2019). Even if the nexus of smart contracts of the blockchain represents a fundamental challenge to business and contract law more generally (Rodrigues, 2018), it can be stated that smart contracts will not replace contract law because contract law operates as a remedial institution with the aim of adjudicating on the legitimacy of a situation ex-post (Werbach and Cornell, 2017, p. 40), and plays a role in our social system that smart contracts do not even purport to replicate (Werbach and Cornell, 2017, p. 32). At the same time, the impact of these self-executive software agents will be clearer in areas that are intrinsically contractual (Arruñada, 2018), such as corporations and enterprises.

Distributed autonomous organizations (DAO)

Business organizations have always changed as a result of technology. The "decentralization and disintermediation" of business organizations will crucially disrupt traditional hierarchical forms of organization (Fenwick and Vermeulen, 2018), resulting in an expansion of the role of markets (horizontal networks) and the contraction of the role of hierarchy (vertical networks) (Berg et al., 2018). The blockchain is "an institutional technology of governance that competes with other economic institutions of capitalism, namely firms, markets, networks" (Davidson et al., 2016, p. 1), capable of undermining the economic efficiency of hierarchies (which exploit incomplete contracts) and relational contracting (which requires trust between parties) over markets[44] (Davidson et al., 2016b). How? Thanks to smart contracts, which are intended to create certainty for counterparties, simplify and automate business, and remove transaction costs (Kaal, 2019); e.g., Allen et al. (2019) consider the lowering of verification costs and networking costs a plausible outcome. However, the scope of smart-contract applications is wide-ranging, from simple contractual agreements to self-governing organizations (Ishmaev, 2017, p. 667). "Multiple smart contracts can be bound together to form decentralized organizations that operate according to specific rules and procedures defined by smartcontracts and code — thereby transforming Michael Jensen's and William Meckling's theory that firms are nothing more than a collection of contracts and relationships into reality" (Wright and De Filippi, 2015, p. 15). As Davidson et al. (2016, p. 21) state; "Blockchain distributed ledger technology is a rare and special general-purpose technology because it adds a further category to the suite of Williamson's (1985) 'economic institutions of capitalism' – namely, markets, hierarchies and relational contracting – with a new type of economic order": Distributed Autonomous Organizations – DAO (Davidson et al., 2016b), and Decentralized Collaborative Organizations – DCOs (Novak, 2018). Both are built upon two concepts; autonomous agents and decentralized organization (Rodrigues, 2018). As a DAO involves a set of humans interacting with each other according to a protocol specified in code and enforced on the blockchain (Rodrigues, 2018), the standard corporate arrangements of equity, debt, and corporate governance could be encoded as a series of smart contracts (Werbach, 2018, p. 18); in short, a business form conceived as networks of contracts built exclusively on software designed to replace individuals (Finck, 2017, p. 7). The main question is therefore as follows: if a corporation is merely a nexus of contracts, why not encode those agreements into digital self-enforcing agreements (Werbach and Cornell, 2017, p. 18) that are able to self-organize with distributed and decentralized profit margins, management and services (Manski, 2017 quoted in Novak, 2018)?

[44] According to Williamson (1985), a hierarchical organization is a method for controlling opportunism. It is protection against opportunism that gives rise to the transaction cost efficiency of hierarchies and relational contracting over markets. This is possible since the valuable prospect of the blockchain (as smart contracts and DAOs) is precisely to eliminate opportunism in crypto-economic mechanisms by enabling a spot market exchange to carry forward a pure promise indefinitely (Davidson et al., 2016b).

The first challenge to be addressed is the location of the DAO within the range of traditional business entities (Rodrigues, 2018). There are problems related to the nature of this organization that lead to legal indeterminacy due to the requirements needed to operate similarly in real life. The concept of a firm is questioned (Waelbroeck, 2018, p. 14). Moreover, the physical spatial distribution of a DAO, which can be distributed into transnational networks, raises several issues regarding applicable legislation. At the same time, it can be logical to deduce that, until the challenges related to smart contracts find a proper solution, DAOs would suffer from the same weaknesses, therefore resulting that their implementation on a large-scale would be challenging to reach. Perhaps much will depend on the extension of the activities that this "new type of economic order" will be entrusted to.

The rising of such organizations may have the power to reshape the nature of work and the notion of the firm (Waelbroeck, 2018). Will the institution of property be affected as well?

The institution of property within the blockchain

Property relations in society could be replaced by or supplemented with blockchain models and implemented in new domains (Ishmaev, 2017, p. 682). With digitized property registries, digital currencies, and smart contracts, real property could be effectively virtualized, facilitating the transfer of property from one party to another (Wright and De Filippi, 2015). Blockchains offer potential advantages in terms of cost, speed, and data integrity in comparison with classical methods of proving ownership (Yermack, 2018, p. 8). Devices and every tangible property can be registered onto a blockchain and turned into a smart property (Wright and De Filippi, 2015, p. 15) in which the rights associated with objects are attached to the objects themselves (Werbach and Cornell, 2017, p. 18). In this way, “property does not disappear but is instead enforced and exercised in different ways. If rights were previously exercised through norms, laws, markets, and architectures, today they are algorithmically inscribed in the object” (O'Dwyer, 2015 cited in Garrod, 2016, p. 70). This scenario is strongly linked to the radical claims that property rights may vanish in the future, becoming a subset of contract law (Ishmaev, 2017, p. 669). As recalled by Berg et al. (2019), the complex interaction between possession and legal ownership is a core part of the ‘scaffolding’ that sustains the market economy. The blockchain can now promote new ways of organizing and distributing assets in digitalizing them as *smart properties*. These assets (e.g. hard assets such as real estate) can be tokenized, valued, and mobilized in unprecedented fractional forms, giving the opportunity to develop new forms of consumption (Kaal, 2019).

Smart properties and tokenization

Digitalization of physical assets on a blockchain is called *tokenization*; it is the process of digitally representing an off-chain real-world asset (currency, commodity, security, property, etc.) on a distributed ledger (Akgiray, 2019; Hileman and Rauchs, 2017). Tokenization refers to the process of transforming the rights to perform an action on an asset into a transferable data element (i.e., *token*) on the blockchain (Rozas et al., 2018). A token is a quantified unit of value that gives its holder the option to exercise specific digital rights that are embedded in the coded rules of the underlying protocol (Collomb et al., 2018).They may be programmed with certain rules that can be used to define what kinds of activities the token network does or does not support (Tan, 2019).

Tokens can only appear in one entry in the ledger at a time (Gans, 2019); they are rivals, and only one person can use a given token at a given time (Waelbroeck, 2018). The potentially unique economics of each token are not based on legal rights but on their promises (e.g. claims and features) and functions (Lo and Medda, 2019), e.g., i) perks; ii) liquidity; iii) funding (Fenwick et al., 2018).

Taking the functions tokens may perform into consideration, they can be classified into several categories. Taxonomies have been proposed in the literature, e.g.:

a) Hargrave et al. (2018) subdivide tokens into: 1. Currency tokens (which can be used to buy and sell real-world goods); 2. Platform tokens (which can be used as "payment" on a blockchain platform); 3. Asset-backed tokens (which are tied to an underlying physical asset, e.g., real estate or fine art).
b) Collomb et al. (2018) provide a slightly different categorization into four functional categories: (i) utility tokens (giving rights of usage such as payment or access tokens); (ii) participation tokens (giving rights to participate in the governance of a specific distributed process); (iii) investment tokens (giving rights to dividends or other financial returns, based on the profits generated by a project); and (iv) asset-backed tokens (giving rights of ownership over an underlying asset, whether a commodity, a property or so forth).

Technological development has shown that many tokens are likely to fall within one or more of these categories. The interoperability of tokens is an increasingly important characteristic of token designs (Kaal, 2019b), since it affects the rights of the holders, which can be: (i) rights of usage; (ii) rights of participation; (iii) rights to profits; and (iv) rights of ownership (Collomb et al., 2018). Of course, as well as functions these rights are not exclusive to one another.

The mass adoption of tokens for fundraising[45] (Tan, 2019), the interoperability of their functions and rights of the holders, the consequent development of so-called *token economics*[46] (or *tokenomics*) has prompted legislators to begin tackling these issues. Not surprisingly, the many characteristics shown by tokens are reflected by the different regulatory regimes which they may fall under. The debate remains open, but first proposals are currently being made (Hacker et al., 2019):

- currency tokens (primarily designed for payment purposes) under currency and payment services regulation;
- investment tokens –under securities and investment regulation (Fenwick and Vermeulen, 2019);
- utility tokens – under consumer and general contract law.

It has been claimed that the pairing of tokens and blockchains may be able to create institutional orders that can be defined in Hayek's words (1960) as a '*catallaxy*', which was defined as "a special kind of spontaneous order produced by the market by people acting within the rules of the law of property, tort and contract" (Davidson et at., 2016b). We underline *within* the rules of the law of property, tort, and contract; and thereby not outside these realms of the law. Blockchain developments, as in the case of ICOs, have often been developed in a shadowy zone, where code is law until the moment the stakes are not too high. As seen in the case of smart contracts, it seems that

[45] We refer here to the so-called Initial Coin Offering (ICO), or "token sale", or "token generating event", which can be described as "a means of fundraising whereby tokens giving their owners certain rights are sold in exchange for cryptocurrencies or fiat money" (Collomb et al., 2019).

[46] Token economics designs the model used to influence the use of tokens in a decentralised ecosystem, through incentive mechanisms and a defined token environment. Token economics is the foundation of tokenised ecosystems. It looks at the long-term and short-term goals and drivers of the ecosystem (Tan, 2019).

the law is called upon to intervene when behaviors in the cybersphere do not respect the *recognized* rights of those involved in such operations. A point of legal intervention may exist wherever the blockchain has an intersection with human beings and their institutions. Among many, the institution of private property has played a major role. The potential switch that may derive from the tokenization of mobilizing properties (and their use) in fractional forms has to be taken seriously into account by practitioners and scholars, bearing in mind the statement of Berg et al., (2019, p. 2) recalling Hodgson[47]; "the elision in the property rights literature about the distinction between 'economic' property rights – those derived from possession and the ability to use or dispose goods one possesses – and 'legal' property rights – the ability to have those rights recognized in law, using their legal property as collateral." This second aspect seems to be underestimated at times in the narrative of blockchain development. Property rights are not the resource itself that is owned but the rights to use the resource (Tan, 2019). Should this be viewed as correct?

Property Rights

In academic research, the concept of property is anything but simple (Ishmaev, 2017) and property rights are in the sphere of public ordering (Arruñada, 2018, p. 21).

The essence of property is the exclusion of non-owners from the determination of property use (Penner, 1997, quoted in Ishmaev, 2017). In Penner's view, they are *in-rem rights*, creating negative duties for all non-owners even if they have no contractual relations with the property holder (Ishmaev, 2017, p. 678). The universal nature of property requires that the same rules be applied to all rightsholders. In a hypothetical, fully decentralized property system, all individuals should therefore be granted or denied consent to a wealth of intended transactions that might affect their property rights (Arrunada, 2018, p. 25). "A key question is to what extent, in addition to exchanging value, these systems are capable of exchanging property in rem rights, since trading in rem rights requires a minimum of public ordering—in particular, an enforcer who is neutral and independent not only of parties to a given contract but to all holders of property rights on the type of asset being traded in that market "(Arruñada, 2018, p. 2). The situation thickens with smart properties, which raise challenges that cannot be easily addressed within the current legal framework. In fact, "in the case of smart property, however, ownership could be both defined and managed by source code. A person who qualifies as the technological owner (as opposed to the legal owner) of the smart property enjoys absolute sovereignty over that resource, which cannot be seized by anyone unless specifically provided for by the underlying code" (Wright and De Filippi, 2015, p. 35).

Ishmaev (2017, p. 681) claims that transparency, "together with exclusion and separability, in fact, makes blockchain technology a self-sufficient alternative institution of property existing independently of any legal institutions." According to B. Arruñada (2018, p. 1) "contrary to naive conceptions that proclaim the end of intermediaries and state involvement, blockchain applications will rely on a variety of interface, completion, and enforcement specialists, including standard public interventions, especially for property transactions." In fact, while blockchains guarantee transfers of ownership, some enforcement is required to ensure transfers of possession (Abadi and Brunnermeier, 2018). This could be explained by the fact that;

[47] The authors refer to Hodgson, G.M. 2015. 'Much of the 'economics of property rights' devalues property and legal rights', Journal of Institutional Economics, 11: 683-709.

(1) the revolutionary potential of governance-by-network as an absolute, horizontal mode of political and social organization is often overstated and unrealistic (Atzori, 2015, p. 30);

(2) "decentralization is limited in the real world because individuals tend to misbehave with respect to security […] individual freedom has a price in terms of individual responsibility that not all individuals are always willing to pay. […] they often trust more and prefer to rely on centralized solutions based on private and public custodian agents" (Arruñada, 2018, p. 24).

Land Registry

Taking the above-mentioned critical issues into consideration, it is possible to state that "centralization and monopoly in registries are not rooted mainly in economies of scale but in the enhanced neutrality (not only concerning parties to the contract but also concerning strangers to it) required to reach universal legal effects" (Arruñada, 2018, p. 27). According to some scholars, this neutral role can be achieved by placing land registry records and public records of land ownership on the blockchain and thereby allowing the relevant stakeholders and agencies real-time access to ownership records (Kakavand and De Sevres, 2016, p. 18). Recognizing the technical and legal problems to be overtaken to reach a wide adoption, Graglia and Mellon (2018) regard the blockchain as a disruptive technology for land governance thanks to its ability to promote the formalization of property rights, registry modernization, and the collection and analysis of land-related data. This could be true especially for emerging markets, given "the inadequacy of existing record-keeping systems, mistrust of corrupt and ineffective market regulators, and high penetration of information technology such as smartphones" (Yermack, 2018, p. 9). What these authors appear to forget is the fact that "the main problem of property registries is not archiving information but producing reliable information, […] purging them and making sure that transactions are not contradictory with preexisting property rights and do not create new collisions of claims" (Arruñada, 2018, p. 22). "With the exception of systems purely based on possession, contracting property requires at least one intermediary (a registry or court) between the world of mere claims (i.e., in personam rights) and the real world of in rem rights […] what is needed is a third-party enforcer representing the interests of all potential rightsholders and not only the interests of those in the chain of title" (Arruñada, 2018, p. 20). To reach this outcome, very high accuracy in the transposition and insertion of data is required. Blockchain registries do not become significant for land governance until after land rights have been formalized, which means addressing the primary challenge of emerging economies; how to bring citizens and properties into the formal system (Graglia and Mellon, 2018, p. 26). Moreover, the blockchain will not resolve the tedious and time-consuming process of collecting, verifying and bringing *data* into the system in the first instance.

Data accuracy

Data serves as a necessary yet insufficient platform for providing information in economic, political, scientific, social and technical contexts (Allen et al., 2018, p. 2). One of the key promises of blockchain technology is to mitigate information problems, given the way it represents and manages data. The blockchain ensures equal access to transparent and trustworthy information (Savelyev et al., 2017, p. 119). A blockchain database is likely to contain at least two types of data. Firstly, it will store metadata related to transactions, namely both the addresses of the sender and recipient, and a timestamp. Secondly, it will store data on the object of a transaction (Bacon et al., 2017). However, even if the technology works flawlessly, fundamental problems include human fallibility and corruption when creating the underlying records, and enforcing consequences (Sulkowski, forthcoming 2018, p. 2).

Moreover, distributed ledger technologies do not make inaccurate data accurate (Zetzsche et al., 2017, p. 13). The truth of any data appearing on a blockchain ledger is limited by the quality or truth of the data input on the ledger (Walch, 2017); GIGO ('garbage in, garbage out') applies to every blockchain that uses non-native digital assets and/or external data inputs (Hileman and Rauchs, 2017). The "zero state problem" is a major issue for Blockchain-based provenance records for physical objects that predate the blockchain (Lapointe and Fishbane, 2019). Blockchain cannot assess whether a given input from the 'outside world' is accurate/true or not. "If 'off-chain' assets or data sources are digitally represented on the blockchain, a trusted third party is required to verify and guarantee the accuracy of the input when inserting it into a blockchain" (Hileman and Rauchs, 2017, p. 18). For example, smart contracts need external data to run self-executing programs. This role is played by the so-called oracles, which serve as "trusted" third parties that retrieve off-chain information to push it into the blockchain. Oracles can be software, hardware or human intermediaries[48] who verify the trustworthiness of data from the physical world (Waelbroeck, 2018, p. 3). These entities are crucial for the successful integration of smart contracts within the real world, but they also create more complexity and vulnerability, since authentication, security, and trust in oracles must be provided by a third party that may be neither transparent nor trustworthy. In fact, the introduction of oracles may cause the introduction of a single point of failure as well as the possibility for people to interact with each other on a trustless basis. This paradox has been popularly described as the "oracle problem" (Egbert, 2017).

Privacy

The need for third parties could prove particularly risky concerning privacy, which (in information) can be defined as a right to exercise some form of control over information about one's self.[49] "If a user uploads sensitive or private information, policymakers who attempt to enforce or encourage privacy may find no way of ameliorating the damage" (Gabison, 2016, p. 331), e.g., a public blockchain could complicate the implementation of the right-to-be-forgotten[50].

Currently, data protection law raises further complex questions in four interrelated areas: (i) identifying data controllers and processors – e.g., is each node that holds a copy of the distributed ledger a controller in respect of all personal data in the ledger?; (ii) controller and processor relationships – e.g., how can controllers give instructions to processors regarding the processing of personal data when the parties may not even know who they are dealing with?; (iii) international data transfers – e.g., given that a node or user may be anywhere on the planet, must it be assumed that any personal data in a distributed ledger might be transferred worldwide?; (iv) data minimization and data subject rights – e.g., what occurs if a data subject wishes to exercise an individual right, for example

[48] In the case of "human oracles", a three step of complexity exists; the simplest version is a trusted user; the second level is to use a trusted data feed; the most sophisticated form is a consensus oracle; a group of users serve as oracles and the software extracts whatever value they have agreed upon (Grimmelmann, 2019).

[49] "Privacy is a broad concept and its normative content may vary from one country to another." On this point, see: Scassa, T. (2018) "Public draft: Open Data and Privacy" In the State of Open Data edited by Tim Davies, Stephen Walker, Mor Rubinstein, and Fernando Perini (forthcoming in 2019). http://stateofopendata.od4d.net – consulted on April 13, 2019.

[50] Cross-cutting privacy issues in blockchains need to be addressed, e.g., with the recent entry into force of the European General Data Protection Regulation ('GDPR') (Hacker et al., 2019).

the correction or erasure of data, if the relevant data are stored in an 'immutable' blockchain? (Millard, 2018, p. 845).

In tackling the issue underlined by Millard, most of the decentralized platforms promote user privacy by focusing on at least one of the following two paradigms: data confidentiality and data sovereignty (De Filippi, 2016). In a blockchain world, there are two significant possibilities for how data is propagated across the network: global diffusion or multichannel diffusion. Choosing between the two has a profound impact on the topology of the network. "In the global data diffusion model, data is shared among all participants in a single, vast network. In the multichannel data diffusion model, there are generally multiple 'sub-ledgers', '(sub-)channels' or 'segregated ledgers' that together form a network of networks" (Hileman and Rauchs, 2017, p. 53). As recognized above, the nature of the blockchain as censorship-resistant generally complicates the deletion of information in these systems in contrast to a centralized system (Gabison, 2016). Moreover, responsibility for data privacy shifts from the operator to the individual user (De Filippi, 2016). Individual risks could increase in relation to the possibility of extending and enforcing individual property rights in new domains, such as the ownership of private data (Ishmaev, 2017). As suggested by Arruñada (2018, p. 17), the comparative advantage of blockchain applications would be enhanced if it can fulfill its promise to enable individual users to own and keep full control of their historical records of transactional data, which are now in the hands of third-party centralized data silos.

5. Final remarks

A common limitation of previous work on blockchain technology is its limited mono-disciplinary approach or its focus on specific cryptocurrencies that only constitute a single purpose instantiation of a blockchain system (Glaser, 2017, p. 1544). There is great potential for multidisciplinary research since this technology integrates many fields of studies, and also due to the need for clarity. The vocabulary currently used in the space of blockchain technology is notoriously confusing (Walch, 2017). As stressed by Akgiray (2019), the establishment of global standards is needed in three critical areas, such as 1) terminology; 2) architecture; 3) governance. Without these standards the process of adoption may lead to uncertainty that could result in a lasting and clear gap between the potential and actual achievements of this technology.

Gans (2019) affirms that blockchains can be considered trustless technologies because of their potential ability to work independently of social mechanisms for trust; however, according to Hawlitschek et al. (2018, p. 59), "blockchain technology in and by itself is not able to provide an environment that renders trust building outside the closed blockchain ecosystem obsolete". With regards to more complex social relationships involving the sharing of resources and assets, blockchain technology alone does not suffice in enabling people to develop trusted interactions (Pazaitis et al., 2017, p. 17). Blockchain and other institutional and physical technologies supporting impersonal exchange simply replace trust between counterparties with all parties' trust instead pointed towards a third-party intermediary (Arruñada, 2018, p. 32), namely the blockchain and its technological features. As previously shown, the blockchain is neither invulnerable (e.g., 51% attack) nor immutable (e.g., soft or hard fork). Abadi and Brunnermeier (2018) proclaimed a *blockchain trilemma* since no ledger in their analysis can simultaneously satisfy all three ideal qualities (1. correctness, 2. decentralization, and 3. cost-efficiency) of any record-keeping system.

Moreover, Akgiray (2019) identifies several shortcomings and weaknesses of the blockchain that must be addressed: 1. scalability; 2. data and user privacy; 3. governance. Gomez et al. (2019) lengthen the list to: 4. jurisdiction – the nodes responsible for the main functionalities of the system are usually spread around the world; 5. encryption – e.g., anyone with the encryption key is able to read the encrypted data should the key be stolen or made public; if the encryption key is lost, it can never be returned to the user; 6. service level agreements and performance – most blockchain implementations are highly dependent on node and communication availability.

The extent of these shortcomings is such that it will first be necessary to find solutions capable of better outcomes than those provided by the current institutions before imagining a large-scale application that can positively affect the "evolution" of instruments such as the contract or institutions as property.

The universal nature of property rights needs a system that does not coincide with the current state of the art of blockchain technology implementations. "The blockchain users are more like observing spectators than rightsholders […] while in rem rights require all rightsholders to grant their consent, not only those listed in a paper-based chain of title deeds or in the blockchain" (Arruñada, 2018, p. 20). Privacy and data issues persist, especially in the case of public blockchains. Though pseudonymity may not constitute total anonymity, in many practical implementations systems will have to be developed in compliance with the relevant regulations in place, otherwise it will prove challenging to imagine the implementation of such technology for *public* services. However, is there still space for functioning of any public sector and services in an entirely decentralized society? Have they exhausted their role, or will they still persist?

Potts (2019) suggests that many aspects of government function may be integrated into blockchain technology wherever the underlying function is based on recordkeeping. In any case, the technology itself does not solve the problem of how data are uploaded in the ledger; "GIGO" may apply (Zetzsche et al., 2017; Walch, 2017; Hileman and Rauchs, 2017). Concerning industries and business, smart contracts may work for certain operations, yet the "oracle problem" persists. The introduction of a third external party into the blockchain environment that may not be trustworthy raises crucial issues regarding the security, privacy, and reliability of data. This last issue is particularly sensitive considering the integration between blockchain systems and existing institutions [e.g., land registries (Graglia and Mellon, 2018)]. The possibility that this process of "osmosis" will be achieved at no cost is claimed by many which believe that blockchain technology represents the coming of a "decentralized autonomous society" (DAS). However, there has been little investigation as to how the DAS might actually function (Garrod, 2016, p. 62). In a world in which code is the law, social sciences and cyber sciences are at a crossroads where society and technology are integrating to create a mixed socio-technological or techno-social reality (Koletsi, 2019); a new societal configuration could result in the constitution of new forms of social and political elites. "We are in a phase of human development where the power to develop codes and select algorithms has – and it will increasingly have – major implications in contemporary society: this power entails the assertion of authority, and it constitutes politics pursued by other means (Latour 1988, p.229; Musiani, 2013), calling into question the egalitarian nature of technology and networks" (Atzori, 2015, p. 27). This scenario naturally recalls the reasons identified behind the birth and *raison d'être* of the state and central institutions in general; mitigating the particular interest into the general interest in light of the principles and rules that the community gave itself. Politics is about a question of compromise. An opt-in or exit-based political system essentially eliminates the notion of politics because it removes the need for compromise (De Filippi, 2018). Accordingly, blockchain technology represents an alternative vision of the economic system that envisages a shift toward a decentralized international order in which politics may be completely absent (Hacker et al., 2019). People with different values or opinions would no longer need to argue and deliberate in order to reach a consensus because if they are in disagreement, they can leave (De Filippi, 2018).

Blockchain technology can be an instrument, but not an end in itself. "Radical technological innovations should not be considered a panacea to humanity's problems but as social technologies leading to new organizational paradigms that transform the thought and action of societies, providing, at the same time, new structures of distributed and decentralized power, re-shaping social relations and humanity's understanding of social reality" (Koletsi, 2019, p. 30). The rules by which different blockchains will be developed and implemented will have to comply with regulatory provisions for large-scale adoption that take general interest into account; "blockchain technology could create – simultaneously – a utopian society characterized by greater individual freedom and autonomy, and a dystopian society driven by market-based incentives and self-dealing" (De Filippi, 2018).

The history of Internet regulation has taught us that borders, governments, and authority will inexorably advance wherever legal intervention points exist (Rodrigues, 2018). Moreover, it is difficult to imagine the blockchain replacing government when external security or the monopoly on violence are considered (Potts, 2019). Is this a goodbye to the crypto-anarchist dream?

We believe that there is enough space to declare that the majority of centralized institutions will still play a role. After all, as Atzori (2015, p. 22) remarks, "we must not forget that empathy and conscience are irreplaceable components of any social and political interaction, and information efficiency and automation are not the ultimate purposes of human communities."

6. Future research

The present survey highlighted certain theoretical and practical issues that must be addressed to ensure a societal benefit in the case of blockchain implementation on a global scale.

The adoption of the blockchain technology should be tested on several levels (micro and macro) based on its predicted impact and consequences. As stated in the case of regulatory systems, the analysis should be carried out taking the single implementation into consideration that would be adopted in every field of application. No normative implications can be derived from a phenomenon that is not properly understood (Reijers and Coeckelbergh, 2016). On the subject of trust, for example, the shift from individual and central institutions to technology, networks, and platforms may have implications outside the blockchain environment, reshaping the way in which societies work.

Case-studies of single applications are currently being developed (e.g., Davidson et al., 2018), but more needs to be done in light of the concerns over alleged disruption concerning the increased use of blockchain technology. More single and multiple case studies will be needed to frame the landscape of the possible applications and assess the gap between the alleged promises and what actually can be achieved. The analysis must be developed in several layers: on the one hand institutions, their roles, possible developments and evolution, taking the potential integration with the blockchain environment into consideration and the subsidization of those services that could be more efficiently managed in a decentralized manner; on the other hand, an analysis should be carried out on the social and individual consequences of these processes of integration.

Therefore, we suggest testing individual behavior of participants of the network at the micro-level in order to understand the effects of the adoption of this technology on trust, cooperation, and relationality. Another layer of analysis could be added by undertaking research on relational dynamics and cooperation within and between networks when convergent interests arise in a “trustless” environment. In recalling Castells (2009), Koletsi (2019, p. 27) points out that “traditional” networks may have three different layers of power: i) networking power – the access or denial to the flow of information is controlled by authorized gatekeepers; ii) networked power – specific nodes of a network exercise their power upon other nodes; iii) network-making power – the organizational dimensions of a network are based upon the allocation of power to the different subparts of the network. It is certainly plausible to see this picture represented in the case of private or consortium blockchains, while public blockchains should be resilient to this process. This two-level implementation can be a good experimental source to gain a greater insight into the possible functioning of a “stateless society” or “distributed autonomous societies”.

Lastly, we would like to refer to a statement by De Filippi (2018, p.6); “Virtual communities rely on voluntary association; they might remove the need for compromises within a single community. Yet they will not eliminate the need for compromise between multiple communities.” As highlighted by Reijers et al. (2016), blockchain design may lack any conception of common interest and common good that goes beyond facilitating autonomous individuals contracting between themselves. The possibility of creating a distinguished (and conflicting?) network that operates on the basis of different interests calls the issue of power relations directly into question, as investigated by Koletsi (2019). The problem of converging particular interests into the general interest still persists, as do public institutions.

In conclusion, we believe in the possibility that the blockchain could have a significant impact in the future. The quality of this impact will largely depend on our ability to adequately investigate and address the challenges ahead and provide solutions in line with the view and goals established by a sustainable, fair and inclusive society.

Bibliography

Abadi, J., and Brunnermeier, M. (2018) Blockchain Economics, NBER Working Paper No. w25407. Available at SSRN: https://ssrn.com/abstract=3308413

Akgiray, V. (2019) "The Potential for Blockchain Technology in Corporate Governance", OECD Corporate Governance Working Papers, No. 21, OECD Publishing, Paris, https://doi.org/10.1787/ef4eba4c-en.

Allen, D.W.E., (2019) Governing the Entrepreneurial Discovery of Blockchain Applications, Journal of Entrepreneurship and Public Policy. Available at SSRN: https://ssrn.com/abstract=2919170 or http://dx.doi.org/10.2139/ssrn.2919170

Allen, D.W.E., (2017) Discovering and Developing the Blockchain Cryptoeconomy, Available at SSRN: https://ssrn.com/abstract=2815255 or http://dx.doi.org/10.2139/ssrn.2815255

Allen, D.W.E., Berg, C., Markey-Towler, B., Novak, M. and Potts, J. (2019) Blockchain and the Evolution of Institutional Technologies: Implications for Innovation Policy. Available at SSRN: https://ssrn.com/abstract=3160428 or http://dx.doi.org/10.2139/ssrn.3160428

Allen, D.W.E., Lane, A. and Poblet, M. (2019) The Governance of Blockchain Dispute Resolution. Available at SSRN: https://ssrn.com/abstract=3334674 or http://dx.doi.org/10.2139/ssrn.3334674

Allen, D.W.E., Berg C. and Novak M. (2018) Blockchain: An Entangled Political Economy Approach, Journal of Public Finance and Public Choice.

Allen, D.W.E., Berg C., Lane A. and Potts J. (2017) The Economics of Crypto-Democracy. Available at SSRN: https://ssrn.com/abstract=2973050 or http://dx.doi.org/10.2139/ssrn.2973050

Arruñada, B. and Garicano, L. (2018) Blockchain: The Birth of Decentralized Governance, Pompeu Fabra University, Economics and Business Working Paper Series, 1608. Available at SSRN: https://ssrn.com/abstract=3160070 or http://dx.doi.org/10.2139/ssrn.3160070

Arruñada, B. (2018) Blockchain's Struggle to Deliver Impersonal Exchange. Minnesota Journal of Law, Science & Technology, 19, 55-105. Available at SSRN: https://ssrn.com/abstract=2903857 or http://dx.doi.org/10.2139/ssrn.2903857

Atik, J. and Gerro, G. (2018) Hard Forks on the Bitcoin Blockchain: Reversible Exit, Continuing Voice. 1 Stanford J. of Blockchain Law & Policy 1 (2018); Loyola Law School, Los Angeles Legal Studies Research Paper No. 2018-25. Available at SSRN: https://ssrn.com/abstract=3203893

Atzori, M. (2015) Blockchain Technology and Decentralized Governance: Is the State Still Necessary? Available at SSRN: https://ssrn.com/abstract=2709713 or http://dx.doi.org/10.2139/ssrn.2709713

Avital, M., Beck, R., King, J. L., Rossi, M., and Teigland, R. (2016). Jumping on the Blockchain Bandwagon: Lessons of the Past and Outlook to the Future. In ICIS 2016 Proceedings Atlanta, GA: Association for Information Systems. AIS Electronic Library (AISeL). Proceedings of the International Conference on Information Systems, Vol.37

Bacon, J., Michels J.D., Millard C. and Singh J. (2017) Blockchain Demystified. Queen Mary School of Law Legal Studies Research Paper No. 268/2017. Available at SSRN: https://ssrn.com/abstract=3091218

Barrera, C. and Hurder, S. (2018) Blockchain Upgrade as a Coordination Game. Available at SSRN: https://ssrn.com/abstract=3192208 or http://dx.doi.org/10.2139/ssrn.3192208

Beck, R. and Müller-Bloch, C. (2017) Blockchain as Radical Innovation: A Framework for Engaging with Distributed Ledgers. Proceedings of the 50th Hawaii International Conference on System Sciences. Available at: https://www.researchgate.net/publication/312166392_Blockchain_as_Radical_Innovation_A_Framework_for_Engaging_with_Distributed_Ledgers_as_Incumbent_Organization

Beck, R., Stenum Czepluch, J., Lollike, N. and Malone, S. (2016) Blockchain – The Gateway ToTrust free Cryptographic Transactions. *Research Papers* 153. http://aisel.aisnet.org/ecis2016_rp/153

Berg, A., Berg, C. and Novak, M. (2018) Blockchains and Constitutional Catallaxy. Available at SSRN: https://ssrn.com/abstract=3295477 or http://dx.doi.org/10.2139/ssrn.3295477

Berg, A. and Berg, C. (2017) Exit, Voice, and Forking. Available at SSRN: https://ssrn.com/abstract=3081291 or http://dx.doi.org/10.2139/ssrn.3081291

Berg, C., Davidson, S. and Potts, J. (2019) Byzantine Political Economy: Property Rights as a Knowledge Commons. Available at SSRN: https://ssrn.com/abstract=3344110 or http://dx.doi.org/10.2139/ssrn.3344110

Berg, C., Davidson, S. and Potts, J. (2018) Institutional Discovery and Competition in the Evolution of Blockchain Technology. Available at SSRN: https://ssrn.com/abstract=3220072 or http://dx.doi.org/10.2139/ssrn.3220072

Berg, C., Davidson, S. and Potts, J. (2018) Capitalism After Satoshi: Blockchains, Dehierarchicalisation, Innovation Policy and the Regulatory State. Available at SSRN: https://ssrn.com/abstract=3299734 or http://dx.doi.org/10.2139/ssrn.3299734

Berg, C. and Davidson, S. and Potts, J. (2017) Blockchains Industrialise Trust. Available at SSRN: https://ssrn.com/abstract=3074070 or http://dx.doi.org/10.2139/ssrn.3074070

Catalini, C. and Gans, J. S. (2017) Some Simple Economics of the Blockchain. Rotman 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

Conoscenti, M., Vetrò A. and De Martin J.C. (2016) Blockchain for the Internet of Things: A systematic literature review. 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA) (2016): 1-6.

Collomb, A., De Filippi, P. and Sok, K. (2018) From IPOs to ICOs: The Impact of Blockchain Technology on Financial Regulation. Available at SSRN: https://ssrn.com/abstract=3185347 or http://dx.doi.org/10.2139/ssrn.3185347

Davidson, S., De Filippi, P. and Potts, J. (2018) Blockchains and the economic institutions of capitalism. Journal of Institutional Economics, 14(4), 639-658. doi:10.1017/S1744137417000200

Davidson, S., De Filippi, P. and Potts, J. (2016) Disrupting Governance: The New Institutional Economics of Distributed Ledger Technology. Available at SSRN: https://ssrn.com/abstract=2811995 or http://dx.doi.org/10.2139/ssrn.2811995

Davidson, S., De Filippi, P. and Potts, J. (2016) Economics of Blockchain. Public Choice Conference, May 2016, Fort Lauderdale, United States. Proceedings of Public Choice Conference, <10.2139/ssrn.2744751>. <hal-01382002>

Davidson, S., Novak, M. and Potts, J. (2018) The Cost of Trust: A Pilot Study. The Journal of the British Blockchain Association. https://doi.org/10.31585/jbba-1-2-(5)2018

De Filippi, P. (2018) Citizenship in the Era of Blockchain-Based Virtual Nations, in Bauböck R. (Ed.) Debating Transformations of National Citizenship. Springer.

De Filippi, P. (2018) Blockchain: A Global Infrastructure for Distributed Governance and Local Manufacturing, in Diez, T. (Ed.) The Mass Distribution of Almost Everything. Institute for

Advanced Architecture of Catalonia, Spain. Available at SSRN: https://ssrn.com/abstract=3221533

De Filippi, P. and Wright, A. (2018) Blockchain and the Law: The Rule of Code. Cambridge, Massachusetts; London, England: Harvard University Press. doi:10.2307/j.ctv2867sp

De Filippi, P. (2016) The Interplay between Decentralization and Privacy: The Case of Blockchain Technologies. Journal of Peer Production, Issue n.7: Alternative Internets. Available at SSRN: https://ssrn.com/abstract=2852689

De Filippi, P. and Hassan, S. (2016) Blockchain Technology as a Regulatory Technology: From Code is Law to Law is Code. First Monday. 21. 10.5210/fm.v21i12.7113.

Dupont, Q. and Maurer, B. (2015) "Ledgers and Law in the Blockchain." available at: https://www.researchgate.net/publication/319579191_The_Distributed_Liability_of_Distributed_Ledgers_Legal_Risks_of_Blockchain

Egberts, A. (2017) The Oracle Problem - An Analysis of how Blockchain Oracles Undermine the Advantages of Decentralized Ledger Systems. Available at SSRN: https://ssrn.com/abstract=3382343 or http://dx.doi.org/10.2139/ssrn.3382343

Evans, D.S. (2014) Economic Aspects of Bitcoin and Other Decentralized Public-Ledger Currency Platforms. Coase-Sandor Institute for Law & Economics Working Paper No. 685.

Faber, N. and Jonker, J. (2019) At Your Service: How Can Blockchain Be Used to Address Societal Challenges?: In: Treiblmaier H., Beck R. (eds) Business Transformation through Blockchain. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-319-99058-3_8

Fenwick, M., Kaal, W.A. and Vermeulen, E.P.M. (2018) Why 'Blockchain' Will Disrupt Corporate Organizations, Lex Research Topics in Corporate Law & Economics Working Paper No. 2018-3; U of St. Thomas (Minnesota) Legal Studies Research Paper No. 18-17; European Corporate Governance Institute (ECGI) - Law Working Paper No. 419/2018; Journal of the British Blockchain Association. Available at SSRN: https://ssrn.com/abstract=3227933 or http://dx.doi.org/10.2139/ssrn.3227933

Fenwick, M. and Vermeulen, E.P.M. (2019) A Primer on Blockchain, Smart Contracts & Crypto-Assets, Lex Research Topics in Corporate Law & Economics Working Paper No. 2019-3. Available at SSRN: https://ssrn.com/abstract=3379443 or http://dx.doi.org/10.2139/ssrn.3379443

Fenwick, M. and Vermeulen, E.P.M. (2018) Technology and Corporate Governance: Blockchain, Crypto, and Artificial Intelligence, Lex Research Topics in Corporate Law & Economics Working Paper No. 2018-7; European Corporate Governance Institute (ECGI) - Law Working Paper No. 424/2018. Available at SSRN: https://ssrn.com/abstract=3263222 or http://dx.doi.org/10.2139/ssrn.3263222

Finck, M. (2017) Blockchain Regulation, in German Law Journal, 2018; Max Planck Institute for Innovation & Competition Research Paper No. 17-13. Available at SSRN: https://ssrn.com/abstract=3014641 or http://dx.doi.org/10.2139/ssrn.3014641

Flood, J.A. and Robb, L. (2017) Trust, Anarcho-Capitalism, Blockchain and Initial Coin Offerings. Griffith University Law School Research Paper No. 17-23; U. of Westminster School of Law Research Paper. Available at SSRN: https://ssrn.com/abstract=3074263 or http://dx.doi.org/10.2139/ssrn.3074263

Gabison, G. (2016) Policy Considerations for the Blockchain Technology Public and Private Applications, 19 SMU Sci. & Tech. L. Rev. 327. Available at: http://scholar.smu.edu/scitech/vol19/iss3/4

Gans, J.S. (2019) The Fine Print in Smart Contracts. Available at SSRN: https://ssrn.com/abstract=3309709 or http://dx.doi.org/10.2139/ssrn.3309709

Garrod, J.Z. (2016) The Real World of the Decentralized Autonomous Society. Triplec Communication Capitalism & Critique, 14(1), 62–77.

Glaser, F. (2017) Pervasive Decentralisation of Digital Infrastructures: A Framework for Blockchain Enabled System and Use Case Analysis (January 2017). Proceedings of the 50th Hawaii International Conference on System Sciences (HICSS-50), Waikoloa Village, Hawaii, January 4 - 7, 2017. Available at SSRN: https://ssrn.com/abstract=3052165

Gomez, M., Bustamante, P., Weiss, M. B. H., Murtazashvili, I., Madison, M. J., Law, W., Mylovanov, T., Bodon, H. and Krishnamurthy, P. (2019) Is Blockchain the Next Step in the Evolution Chain of [Market] Intermediaries? Available at SSRN: https://ssrn.com/abstract=3427506 or http://dx.doi.org/10.2139/ssrn.3427506

Graglia, J.M. and Mellon, C. (2018) Blockchain and Property in 2018: At the End of the Beginning. Innovations: Technology, Governance, Globalization 2018 12:1-2, 90:116

Grimmelmann, J. (2019) All Smart Contracts Are Ambiguous, Penn Journal of Law and Innovation (Forthcoming); Cornell Legal Studies Research Paper No. 19-20. Available at SSRN: https://ssrn.com/abstract=3315703

Hacker, P., Lianos, I., Dimitropoulos, G. and Eich, S. (2018) Regulating Blockchain: Techno-Social and Legal Challenges - An Introduction. Forthcoming in: Regulating Blockchain. Techno-Social and Legal Challenges, edited by Philipp Hacker, IoannisLianos, Georgios Dimitropoulos, and Stefan Eich, Oxford University Press, 2019. Available at SSRN: https://ssrn.com/abstract=3247150

Hargrave, J., Sahdev, N.K. and Feldmeier, O. (2018) How Value is Created in Tokenized Assets (February 28, 2018). Available at SSRN: https://ssrn.com/abstract=3146191 or http://dx.doi.org/10.2139/ssrn.3146191

Hawlitschek, F., Notheisen, B., and 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.

Hileman, G. and Rauchs, M. (2017) Global Blockchain Benchmarking Study. Available at SSRN: https://ssrn.com/abstract=3040224 or http://dx.doi.org/10.2139/ssrn.3040224

Howell, B. E., Potgieter, P. H. and Sadowski, B. M. (2019) Governance of Blockchain and Distributed Ledger Technology Projects. Available at SSRN: https://ssrn.com/abstract=3365519 or http://dx.doi.org/10.2139/ssrn.3365519

Huckle, S. and White, M. (2016) Socialism and the blockchain. Future Internet, 8 (4). p. 49. ISSN 1999-5903

Immorlica, N., Jackson, M. O. and Weyl, E.G. (2019) Verifying Identity as a Social Intersection Available at SSRN: https://ssrn.com/abstract=3375436 or http://dx.doi.org/10.2139/ssrn.3375436

Ishmaev, G. (2017) Blockchain Technology as an Institution of Property. Metaphilosophy, 48: 666:686. doi:10.1111/meta.12277

Kaal, W.A. (2019) Decentralization - A Primer on the New Economy. Available at SSRN: https://ssrn.com/abstract=3406323 or http://dx.doi.org/10.2139/ssrn.3406323

Kaal, W.A. (2018) Crypto Economics - The Top 100 Token Models Compared. BANKING & FIN. SER. POL. REP. U of St. Thomas (Minnesota) Legal Studies Research Paper No. 18-29. Available at SSRN: https://ssrn.com/abstract=3249860 or http://dx.doi.org/10.2139/ssrn.3249860

Kakavand, H., Kost De Sevres, N. and Chilton, B. (2017) The Blockchain Revolution: An Analysis of Regulation and Technology Related to Distributed Ledger Technologies. Available at SSRN: https://ssrn.com/abstract=2849251 or http://dx.doi.org/10.2139/ssrn.2849251

Keymolen, E. (2013) Trust and technology in collaborative consumption. Why it is not just about you and me. In Leenes, R. E. and Kosta, E. (Eds.). Bridging distances in technology and regulation. Oisterwijk: Wolf Legal Publishers (WLP).

Kolber, A.J. (2018) Not-So-Smart Blockchain Contracts and Artificial Responsibility. Stanford Technology Law Review, vol. 21, p.198, 2018; NYU School of Law, Public Law Research Paper No. 18-44. Available at SSRN: https://ssrn.com/abstract=3186254

Koletsi, M. (2019) Radical technologies: Blockchain as an organizational movement. Homo Virtualis, 2(1), 25-33. doi: http://dx.doi.org/10.12681/homvir.20191

Lapointe, C. and Fishbane, L. (2019) The Blockchain Ethical Design Framework. Innovations: Technology, Governance, Globalization. 12. 50-71. 10.1162/inov_a_00275.

Lo, Y. and Medda, F. (2019) Assets on the Blockchain: An Empirical Study of Tokenomics. Available at SSRN: https://ssrn.com/abstract=3309686 or http://dx.doi.org/10.2139/ssrn.3309686

Markey-Towler, B. (2018) Anarchy, Blockchain and Utopia: A Theory of Political-Socioeconomic Systems Organised using Blockchain. Available at SSRN: https://ssrn.com/abstract=3095343 or http://dx.doi.org/10.2139/ssrn.3095343

Maupin, J. (2017) ‘Mapping the global legal landscape of blockchain technologies’, Working Paper, Centre for International Governance Innovation. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2930077

Mik, E. (2017) Smart contracts: Terminology, technical limitations and real-world complexity. Law, Innovation and Technology. 9, (2), 269-300. Research Collection School of Law. Available at: https://ink.library.smu.edu.sg/sol_research/2341

Millard, C. (forthcoming 2018) Blockchain and Law: Incompatible Codes? (2018). Forthcoming, Computer Law & Security Review. Available at SSRN: https://ssrn.com/abstract=3220406

Nofer, M., Gomber, P., Hinz, O. and Schiereck, D. (2017) "Blockchain," Business & Information Systems Engineering: Vol. 59: Iss. 3, 183:187. Available at: https://aisel.aisnet.org/bise/vol59/iss3/7

Novak, M. (2018) The Implications of Blockchain for Income Inequality. Available at SSRN: https://ssrn.com/abstract=3140440 or http://dx.doi.org/10.2139/ssrn.3140440

Oh, S. and Wallsten, S. (2018) Is Blockchain Hype, Revolutionary, or Both? What We Need to Know. A Research Agenda for New Institutional Economics, Mary Shirley and Claude Menard, eds. 2018 Forthcoming. Available at SSRN: https://ssrn.com/abstract=3244783

Ølnes, S., Ubacht, J. and Janssen, M. (2017) Blockchain in government: Benefits and implications of distributed ledger technology for information sharing, Government Information Quarterly, Volume 34, Issue 3, 355:364, available at: https://doi.org/10.1016/j.giq.2017.09.007

Pazaitis, A., De Filippi, P. and Kostakis, V. (2017) Blockchain and value systems in the sharing economy: The illustrative case of Backfeed. Technological Forecasting and Social Change, Elsevier, 125, 105:115. 10.1016/j.techfore.2017.05.025>. <hal-01676881>

Potts, J. (2019) Blockchain and Government. Data61 'Future of Blockchain' Report, June 2019. Available at SSRN: https://ssrn.com/abstract=3404406 or http://dx.doi.org/10.2139/ssrn.3404406

Rajagopalan, S. (2019) Blockchain and Buchanan: Code as Constitution, in James M. Buchanan: A Theorist of Political Economy and Social Philosophy, Richard E. Wagner (ed). Palgrave Macmillan, 2019. Available at SSRN: https://ssrn.com/abstract=3238472

Raskin, M. (2017) The Law and Legality of Smart Contracts. Georgetown Law Technology Review 304. Available at SSRN: https://ssrn.com/abstract=2959166 or http://dx.doi.org/10.2139/ssrn.2842258

Reijers, W. and Coeckelbergh, M. (2016) The Blockchain as a Narrative Technology: Investigating the Social Ontology and Normative Configurations of Cryptocurrencies. Philosophy & Technology. 31. 10.1007/s13347-016-0239-x.

Reijers, W., O'Brolchain, F. and Haynes, P. (2016) Governance in Blockchain Technologies & Social Contract Theories. Ledger. 1. 134-151. 10.5195/LEDGER.2016.62.

Reyna, A., Martín, C., Chen, J., Soler E. and Díaz, M. (2018) On blockchain and its integration with IoT. Challenges and opportunities, Future Generation Computer Systems, Volume 88, 173:190, https://doi.org/10.1016/j.future.2018.05.046.

Risius, M. &Spohrer, (2017) A Blockchain Research Framework -What We (don't) Know, Where We Go from Here, and How We Will Get There. K. Bus Inf Syst Eng, 59: 385. https://doi.org/10.1007/s12599-017-0506-0

Rodrigues, U. (2018) Law and the Blockchain. Iowa Law Review, Vol. 104, 2018, Forthcoming; University of Georgia School of Law Legal Studies Research Paper No. 2018-07. Available at SSRN: https://ssrn.com/abstract=3127782

Rozas, D., Tenorio-Fornés, A., Díaz-Molina, S. and Hassan, S. (2018) When Ostrom Meets Blockchain: Exploring the Potentials of Blockchain for Commons Governance (July 30, 2018). Available at SSRN: https://ssrn.com/abstract=3272329 or http://dx.doi.org/10.2139/ssrn.3272329

Rousseau D., Sitkin S., Burt R. and Camerer C. (1998) Not So Different After All: A Cross-discipline View of Trust. Academy of Management Review. 23. 10.5465/AMR.1998.926617.

Savelyev, A. (2017) Contract law 2.0: 'Smart' contracts as the beginning of the end of classic contract law, Information & Communications Technology Law, 26:2, 116-134, DOI: 10.1080/13600834.2017.1301036

Shackelford, S.J. and Myers, S. (2016) Block-by-Block: Leveraging the Power of Blockchain Technology to Build Trust and Promote Cyber Peace. Yale Journal of Law and Technology (2017 Forthcoming); Kelley School of Business Research Paper No. 16-85. Available at SSRN: https://ssrn.com/abstract=2874090 or http://dx.doi.org/10.2139/ssrn.2874090

Shakow, D. J. (2018) The Tao of the DAO: Taxing an Entity that Lives on a Blockchain. Tax Notes, Vol. 160, Pg. 929, August 13, 2018; U of Penn, Inst for Law & Econ Research Paper No. 18-23. Available at SSRN: https://ssrn.com/abstract=3247155

Sulkowski, A. J. (2018) Blockchain, Business Supply Chains, Sustainability, And Law: The Future of Governance, Legal Frameworks, And Lawyers? Available at: https://www.researchgate.net/project/Blockchain-Law-and-Sustainability/update/5bba7a0f3843b006753d2385

Swan, M. & De Filippi, P. (2017) Toward a Philosophy of Blockchain in Metaphilosophy. Vol. 48, Issue 5. Wiley. Available at SSRN: https://ssrn.com/abstract=3097477

Tan, L. (2019) Token Economics Framework. Available at SSRN: https://ssrn.com/abstract=3381452 or http://dx.doi.org/10.2139/ssrn.3381452

Tapscott, D. and Tapscott, A. (2016) The Impact of the Blockchain Goes Beyond Financial Services. Harvard Business Review, available at https://hbr.org/2016/05/the-impact-of-the-blockchain-goes-beyond-financial-services

Vatiero, M. (2018) Smart Contracts and Transaction Costs. Available at SSRN: https://ssrn.com/abstract=3259958 or http://dx.doi.org/10.2139/ssrn.3259958

Waelbroeck, P. (2018) An Economic Analysis of Blockchains, CESifo Working Paper Series 6893, CESifo Group Munich.

Walch, A. (2019) Deconstructing 'Decentralization': Exploring the Core Claim of Crypto Systems. Crypto Assets: Legal and Monetary Perspectives (OUP, Forthcoming). Available at SSRN: https://ssrn.com/abstract=3326244

Walch, A. (2017) The Path of the Blockchain Lexicon (and the Law). 36 Review of Banking & Financial Law 713. Available at SSRN: https://ssrn.com/abstract=2940335

Walch, A. (2017) Blockchain's Treacherous Vocabulary: One More Challenge for Regulators. Journal of Internet Law, Vol. 21, No. 2, Aug. Available at SSRN: https://ssrn.com/abstract=3019328

Werbach, K. and Cornell, N. (2017) Contracts Ex Machina. 67 Duke Law Journal 313. Available at SSRN: https://ssrn.com/abstract=2936294

Werbach, K. (2018) Trust, But Verify: Why the Blockchain Needs the Law. Berkeley Technology Law Journal, Forthcoming. Available at SSRN: https://ssrn.com/abstract=2844409 or http://dx.doi.org/10.2139/ssrn.2844409

Wright, A. and De Filippi, P. (2015) Decentralized Blockchain Technology and the Rise of Lex Cryptographia. Available at SSRN: https://ssrn.com/abstract=2580664 or http://dx.doi.org/10.2139/ssrn.2580664

Yeoh, P. (2017) Regulatory issues in blockchain technology , Journal of Financial Regulation and Compliance, Vol. 25 Iss 2 pp. Permanent link to this document: http://dx.doi.org/10.1108/JFRC-08-2016-0068

Yermack, D. (2016) Corporate Governance and Blockchains. Review of Finance, Forthcoming. Available at SSRN: https://ssrn.com/abstract=2700475 or http://dx.doi.org/10.2139/ssrn.2700475

Yli-Huumo J., Ko D., Choi S., Park S. and Smolander K. (2016) Where Is Current Research on Blockchain Technology? A Systematic Review. PLoS ONE 11(10): e0163477. https://doi.org/10.1371/journal.pone.0163477

Zetzsche D., Buckley R.P. and Arner, D. W. (2017) The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain. University of Illinois Law Review, 2017-2018, Forthcoming; University of Luxembourg Law Working Paper No. 007/2017; Center for Business & Corporate Law (CBC) Working Paper 002/2017; University of Hong Kong Faculty of Law Research Paper No. 2017/020; UNSW Law Research Paper No. 17-52; European Banking Institute Working Paper Series 14. Available at SSRN: https://ssrn.com/abstract=3018214 or http://dx.doi.org/10.2139/ssrn.3018214