Blockchain as a confidence machine: The problem of trust & challenges of governance

Primavera de Filippi, Morshed Mannan, Wessel Reijers

Technology in Society 62 (2020) 101284

Contents lists available at ScienceDirect

Technology in Society

journal homepage: http://www.elsevier.com/locate/techsoc

Blockchain as a confidence machine: The problem of trust & challenges of governance

Primavera De Filippi [a,b,*], Morshed Mannan [c], Wessel Reijers [d]

[a] CERSA (Centre d'Études et de Recherches de Sciences Administratives et Politiques), Paris, 75005, France
[b] Berkman-Klein Center for Internet & Society at Harvard University, Cambridge, MA, 02138, USA
[c] Leiden University, Leiden, 2311 EZ, the Netherlands
[d] European University Institute, Fiesole, 50014, Italy

ARTICLE INFO

Keywords:
Trust
Confidence
Blockchain
Governance
Rule of law
Polycentricity

ABSTRACT

Blockchain technology was created as a response to the trust crisis that swept the world in the wake of the 2008 financial crisis. Bitcoin and other blockchain-based systems were presented as a "trustless" alternative to existing financial institutions and even governments. Yet, while the trustless nature of blockchain technology has been heavily questioned, little research has been done as to what blockchain technologies actually bring to the table in place of trust. This article draws from the extensive academic discussion on the concepts of "trust" and "confidence" to argue that blockchain technology is not a 'trustless technology' but rather a 'confidence machine'. First, the article provides a review of the multifaceted conceptualisations of trust and confidence, and the relationship between these two concepts. Second, the claim is made that blockchain technology relies on cryptographic rules, mathematics, and game-theoretical incentives in order to increase confidence in the operations of a computational system. Yet, such an increase in confidence ultimately relies on the proper operation and governance of the underlying blockchain-based network, which requires trusting a variety of actors. Third, the article turns to legal, constitutional and polycentric governance theory to explore the governance challenges of blockchain-based systems, in light of the tension between procedural confidence and trust.

1. Introduction

The past decade has seen a reinvigorated interest in the concept of trust, primarily driven by the onset of the global financial crisis in 2008, which has been commonly attributed to the failure of trusted institutions such as banks and other financial institutions [1]; p. 786–787). More recently, abuses of information and communication technologies for surveillance, dissemination of disinformation, and public coercion have come to light, leading to a growing loss of trust in governmental authorities—even in democracies such as the United States following the Snowden revelations—as well as in large online platforms such as Facebook, Google and Twitter, who have been complicit in such abuses [2,3]; Cadwalladr & Graham-Harrison 2014; [4]).[1] These developments have triggered a new attitude towards sociotechnical systems, whereby the requirement to trust third parties—whether they be corporations or governments—is considered to be more of a hindrance than a help. (see Table 1, Fig. 1)

Blockchain technology, in particular, has emerged as a potential solution to the erosion of trust in traditional institutions and online intermediaries more generally, as it allegedly eliminates the need for trust between parties. The underlying premise of blockchain technology and its various applications is that users subject themselves to the authority of a technological system that they are confident is immutable, rather than to the authority of centralized institutions which are deemed untrustworthy. Regardless of the end to which a public blockchain is used, when properly functioning, it mitigates principal-agent problems (e.g. moral hazard, shirking) that characterizes trusted relationships. This has led to many describing blockchain as a 'trustless' or 'trust-free' technology [5,6]. However, the academic discussion only considers this central property of blockchain technology from a negative perspective: blockchain technology does *not* need trust to operate. There has been relatively little interrogation of the positive perspective that is implied,

* Corresponding author. Room B2.33, Kammerlingh Onnes Gebouw, Steenschuur 25, 2311 ES Leiden, The Netherlands.
E-mail addresses: pdefilippi@gmail.com (P. De Filippi), m.mannan@law.leidenuniv.nl (M. Mannan).

[1] Some have gone so far as to say that the need to trust and rely on "online service providers"—something that they encourage—leads to the creation of a fiduciary relationship between users and said providers, see Balkin [110]; p. 1220).

https://doi.org/10.1016/j.techsoc.2020.101284
Received 3 April 2020; Received in revised form 15 May 2020; Accepted 3 June 2020
Available online 19 June 2020

Table 1
A tentative overview of the aspects that distinguish trust from confidence, considering for each (1) its character as a mental state, (2) its source, (3) its destination, and (3) the relationship between actors and systems.

	Trust	Confidence
Mental state	Decision in the context of uncertainty or complexity	Assurance in the context of personal experience or evidential knowledge
Source	Integrity of interpersonal relations or "leap of faith"	Predictability of regulated processes or reliance on larger systems
Destination	Always need to be addressable	Can be either addressable or non-addressable
Relationship between actors and systems	Agency of the trustee puts the trustor in a situation of vulnerability	No sense of vulnerability because no recognition of agency

namely *what* blockchain technology produces in order to operate. To fill this gap, this article embeds the discussion about trust in blockchain technology in the wider sociological and philosophical discussions on trust and confidence. It engages with the argument that blockchain technology reconfigures trust in society, by contending that the technology does not qualify as a 'trust machine' (e.g. Ref. [7] but rather as a 'confidence machine'. The paper asks the question: to what extent is blockchain technology trustless, and if it is 'without' trust in a certain sense, what replaces trust as a fundamental aspect of its governance?

There are numerous sociological and philosophical discussions on trust (e.g. Ref. [8–10], trust in governments (e.g. Ref. [11,12], levels of trust in and across societies (e.g. Ref. [13,14] and trust in technology (e.g. Ref. [15–19], including trust in algorithmic authority[2] [20]. However, only a small segment of the voluminous trust literature has been dedicated to the analysis of the related, but distinct, concept of confidence. Moreover, only few authors have questioned the impact of blockchain technology on trust, arguing that blockchain technology relies on a new model or a new architecture of trust [21]; p. 50 [22]; p. 3).

This article presents a three-fold argument. First, it argues that trust and confidence are distinct phenomena: trust depends on personal vulnerability and risk-taking, whereas confidence depends on internalised expectations deriving from knowledge or past experiences. Second, the article claims that blockchain technology should be regarded not so much as a "trustless technology" but rather as a "confidence machine", because it creates shared expectations with regard to the manner in which it operates, and the procedural correctness of its operations. The arguments presented here focus on public and permissionless blockchains such as Bitcoin and Ethereum rather than private or permissioned blockchains such as Hyperledger and Amazon's QLDB—as the latter are not considered to be "trustless" due to the dominant role of one or more organizations in maintaining those ledgers [23]. Third, the article argues that even public and permissionless blockchains rely on a particular type of "distributed trust". Indeed, although there is no centralized "trusted authority", a low-level of trust is required in relation to a large number of—often unknown—actors (such as miners) in charge of maintaining and securing the network. Hence, the increased confidence that the technology provides ultimately depends on a variety of factors, including the collective management of the network by a large number of distributed actors (e.g. miners, validators) who—although they do not have the power to unilaterally influence the network—nonetheless need to be trusted not to collude in order to further their own interests, at the expense of the overall network.

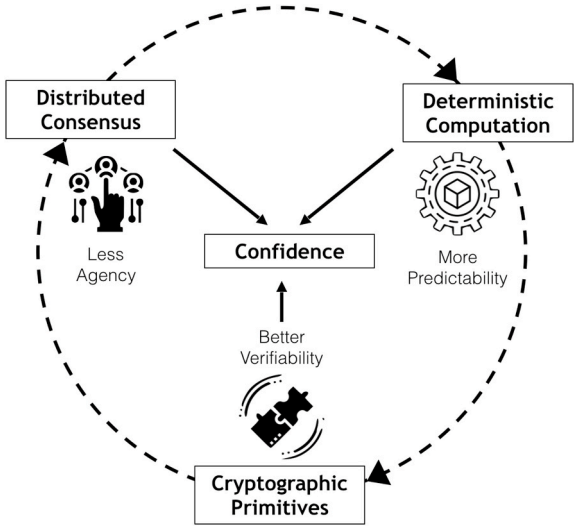

Fig. 1. Schematic representation of the blockchain as a confidence machine.

The article comprises three sections. The first section examines both general sociological and philosophical discussions on the distinction between trust and confidence,[3] including specific discussions on trust in technological systems, in order to provide a conceptual framework for distinguishing trust and confidence. The second section provides a concise overview of the nascent literature on the impact of blockchain technology in reconfiguring trust, before developing the argument that the blockchain is a confidence machine that tries to displace trust in favor of confidence. The third section explores the limitations of such a view, by showing how the underlying governance of blockchain-based systems might impinge its operations, thereby reducing the confidence in these systems, in particular (but not exclusively) during states of exceptions. Finally, the paper draws upon legal, constitutional and polycentric governance theory in order to explore the governance challenges of blockchain-based systems in light of this tension between trust and confidence.

2. Trust and confidence

2.1. *Vertrauen ist gut, sicherheit noch besser*[4]

Trust and confidence are two significant and interrelated concepts that describe and explain the functioning of interpersonal relationships and institutions in society. While the concepts of trust and confidence sometimes overlap, the following sections provide an in-depth analysis of the meanings of "trust" and "confidence" respectively. It will be shown that trust is a multifaceted phenomenon that has different, equally legitimate meanings, but that confidence denotes a more precise and distinct phenomenon. The aim is to construct a framework to

[2] Lustig & Nardi [20] define "algorithmic authority" as "the authority of algorithms to direct human action and to verify information, in place of relying exclusively on human authority".

[3] We note at the outset that this article does not engage with what Oliver Williamson [111] termed as 'calculativeness', to describe how economics (and increasingly, other social sciences) anticipate risk. In his view, in economic transactions the role of trust is negligible as the transactions are determined by the calculative behaviour of actors. Later scholars, such as Earle [1]; have deemed calculativeness to be one of the attributes of a state of confidence (p. 786).

[4] Trust is good, confidence is better. This old German proverb is mentioned by Seligman [46]; p. 17).

distinguish trust and confidence in a way that enables us to explain how blockchain technology is attempting at eliminating trust for the sake of confidence..

2.2. Trust

This section provides a panorama of established conceptualisations of trust, highlighting both their similarities and divergences. Rather than committing to any of these conceptualisations, our claim is that trust is an inherently multifaceted and complex social phenomenon, with no single established definition. Yet, from a preliminary analysis of the various definitions provided to the term, it emerges that—even though they disagree on the source or substance of trust—most scholars nonetheless acknowledge the fact that trust inevitably comes along with a certain degree of risk and vulnerability.

Gambetta [24] defines trust as "*the subjective probability with which one agent assesses that another agent […] will perform a particular action […] independently of his capacity to be able to monitor it, and in a context in which it affects his own action.*" In other words, trust can be regarded as a relationship between two or more parties, whereby one party (the trustor) voluntary decides, under a condition of uncertainty, to rely on another (the trustee) for the achievement of a particular task, based on the belief that the latter will perform the task in line with the expectations of the former—thereby putting the trustor in a vulnerable position with regard to the trustee. Luhmann [10] elaborates on the distinctive properties of *trust*, characterized by a risk and uncertainty, by distinguishing it from the feeling of *confidence,* which does not seemingly present these characteristics. Before engaging in a trust relationship, a person always makes a choice among at least two alternatives: one alternative that involves trusting another (and therefore introduces an element of vulnerability and risk), and one—ostensibly more secure—alternative that entails either a lower degree of trust or no trust at all.[5] All things being equal, the decision will depend both on the amount of trust that can be conferred to a third party and the possible consequences that a breach of trust might entail. If the alternative involving trust is chosen, the trustor implicitly assumes responsibility for her decision, and will therefore assume part of the blame, should that choice turn out to be wrong. Conversely, in a situation of confidence, where people do not perceive the risk that their expectations might remain unfulfilled, people act without considering alternatives to that risk. As no choice has been made explicitly between two alternatives, people acting upon confidence do not blame themselves for any potential disappointment in the outcome of their actions; the fault will naturally be attributed to the actions of third parties or external (and unforeseeable) events [25]; p. 31).

Trust is beneficial because it enables the trustor to economise resources by (a) delegating to a third party the performance of a task, and (b) reducing the level of direct involvement needed to ensure the proper performance of that task. For some, like John Locke, the existence of trust was the most fundamental requirement for humans to leave a state of nature and form societies [26]; p. 359). However, the flipside of trust is that it necessarily comes with some degree of risk and uncertainty, or unpredictability [27]; p. 208) insofar as the trustee has the ability to act against the interests of the trustor[6]—which is especially true in the case of information and power asymmetries [28]. As Giddens [25] points out, trust necessarily puts the trustor in a situation of vulnerability because "trust is only demanded where there is ignorance—either of the knowledge claims of technical experts or of the thoughts and intentions of intimates upon whom a person relies" (1990, p.89).

While most scholars agree about these basic characteristics of trust, opinions diverge as to what constitutes the source and the object of trust. One strand of scholarship considers trust as a *psychological attitude* held by one individual, who "believes in" someone or something [29] [1978]). This means that before entrusting a third party with a specific task, the trustor must believe that the trustee will act in accordance with his or her interests [30]. Trust relates, therefore, less to a "cognitive understanding" and more to an actual "leap of faith" or "commitment" toward a particular state of affairs [25]; p.27). Giddens [25] further elaborates on the idea, by describing interpersonal trust as an on-going project between multiple individuals, which requires the "opening out of the individual to the other". As such, trust "cannot be controlled by fixed normative codes, it has to be won" (p.121). Weckert [31] goes even further by claiming that trust ultimately refers to an agent's aptitude, or a mood, and that trust should therefore be considered as a habitual disposition that agents have to possess in order to engage in relations of familiarity with other agents. In a similar vein, Coeckelbergh [17] regards trust as '*a priori*' to relations themselves, or as a constitutive element of relations. Macneil [32] expands on this approach by equating trust with social solidarity, defined as "a state of mind or, rather, a state of minds. It is a belief not only in future peace among those involved but also in future harmonious affirmative cooperation" (p. 572).

In contrast, another strand of scholarship sees trust as a *rational choice* undertaken by one individual, in order to achieve a particular goal more easily or efficiently. In that regard, Taddeo [33] insists that trust is inherently goal-oriented, *i.e.* it should not be regarded as a general property of an agent, but rather as a property that must be assessed in light of a specific objective or task to be performed by that agent. In particular, Taddeo [33] argues that trust is a 'property' of a relation between communicating agents (*i.e.* a second-order property of a first-order relationship), which requires agents to engage in a probabilistic evaluation of each other's trustworthiness. Such a definition fits with the analyses of Luhmann [34]; Gambetta [24] and Castelfranchi & Falcone [35]; who regard the evaluation of trustworthiness as an exercise that requires some effort from the part of the trustor, who needs to balance the potential benefits derived from the trustee's performance, with the risk that the trustee will not perform as expected. In other words, agents have to calculate whether the self-interest of the trustees or their altruistic intent, will lead to them acting in a manner that is in the interest of the trustor. Trusting a third party therefore involves the trustor assessing whether another actor can be expected to act in her own interest because the trustee's interests—whatever they may be—somehow encompasses the trustor's interest [36]; p. 26). In that regard, Petit [27] further elaborates on the idea that the mere act of trusting someone—through a manifestation of reliance—will induce that person to act in a more trustworthy manner, as a result of a general desire for the good opinion of others (p. 213). This is especially true if the manifestation of reliance is done in public or in front of a witness,

[5] Giddens [25] paraphrases Luhmann as follows: "Where trust is involved, in Luhmann's view, alternatives are consciously borne in mind by the individual in deciding to follow a particular course of action. Someone who buys a used car, instead of a new one, risks purchasing a dud. He or she places trust in the salesperson or the reputation of the firm to try to avoid this occurrence. Thus, an individual who does not consider alternatives is in a situation of confidence, whereas someone who does recognise those alternatives and tries to counter the risks thus acknowledged, engages in trust." (p. 31).

[6] Note that the element of risk or betrayal is important in the context of a trust relationship, because, if the trustee did not have the capacity to act against the interests of the trustor (i.e. if the actions of the trustee were perfectly predictable by the trustor), then the trustor would have confidence about the outcome of the task, and would not even need to trust the trustee.

thereby giving the trustee the opportunity to display to others that she is a trustworthy person (p. 215).[7]

In some cases, however, trust emerges as a tacit acceptance of circumstances, which are incorporated into everyday routine, without any conscious act of commitment or leap of faith from the part of the trustor [25]; p. 90). Luhmann [34] also recognizes this possibility by pointing out that people sometimes engage into a more routinised (and therefore less rational) type of trust, based on familiarity. This is echoed by Mansbridge [37]; who argues that trust may be extended to others for altruistic reasons, such as a respect for another person due to filial relation or status. More generally, investing trust in someone sometimes merely signals a desire to form a relationship with that person, hoping that he or she will respond in a trustworthy manner, thereby establishing the foundation for a stronger and lasting relationship to be established [27]; p. 220).

Depending on whether the trustee is a person or an institution, the trustor will adopt different strategies to assess the trustworthiness of the trustee. Trustworthiness of an individual can be assessed in one of two manners: either as a result of repeated and direct interactions with that individual, whose actions and intentions become known, and therefore more reliable, as a long-term acquaintance (e.g. Ref. [38]; p.59 [39]; p. 247), or as a result of the trust that other people or institutions have conferred to that individual, who provide the necessary credentials for that individual to be trusted by third parties (e.g. in the case of diplomas or reference letters). Trust in an institution takes the form of a sustained belief that the institution will act and operate in line with the interests of the trustor, even though the trustor does not know or fully comprehend the internal workings of the institution. While the trustworthiness of an institution can be established on a more abstract level, without any interaction with the individuals who are responsible for its operations, Giddens [25] reminds us that the contacts or encounters with the representatives or delegates of an institution—what he calls its "access points"[8] (p. 83)—play a consequential role in the process of analysing the trustworthiness thereof. Moreover, in addition to these access points, which merely represent the face of the institution, trusting an institution generally also requires assessing the trustworthiness of the persons involved in the design, the production and the administration of that system, insofar as they have the power to change or influence its operations [25]; p. 34). This assessment of trustworthiness can, of course, lead to disappointment. People or institutions–regardless of their track record–can be mistrusted and they can act in a manner that betrays the trust reposed in them. Mistrust occurs whenever an individual develops a negative attitude towards the integrity of specific persons or institutions, and therefore becomes sceptical about the underlying intentions or motivations that motivates their actions [25]; p.99).

The situation is different in the case of a technological arrangement—where one only has to ensure that the technology has been designed in such a way as to comply with a set of predefined rules, which it cannot depart from Ref. [40]. As a result, people often regard technologically-run institutions to be more 'trustworthy' than human-led institutions [20], which, as the article will argue, is in fact the capacity of technology to build confidence. Indeed, unless a technological arrangement is controlled by a third-party operator—which will thus need to be trusted by the trustor—analysing the trustworthiness of a technology ultimately amounts to assessing the *predictability* and *reliability* thereof [41]. If a person has the ability to correctly analyse the functioning of a technology, predict its operations in a reliable manner and potentially gain experience in seeing it in operation, this person will no longer need to "trust" the technology, because she now has "confidence" in the way it operates.

2.3. Confidence

In all of its definitions, trust presupposes awareness of a certain element of risk [34]. Indeed, as mentioned above, trust is inherently connected with a trustee's ability to breach the trust she has been conferred with [24]: by delegating a task to another, the trustor (voluntarily) assumes the risk of being betrayed by the trustee, if the latter were to abuse its discretionary power. Confidence, in contrast, does not presuppose an acknowledgment of risk, but rather an attitude of assurance. As opposed to trust, confidence does not require an individual to put herself into a vulnerable position because it does not operate under a condition of uncertainty. When used to describe a relationship with other people, institutions or systems, a state of confidence involves a sense of predictability, which significantly contributes to reducing the feeling of risk and uncertainty that would otherwise be felt in entering into such a relationship [42]; p. 230; [34].

Confidence does not entail personal vulnerability, because it emerges from prior experience or statistical evidence of how a system operates [1]; p. 786)—this is what Simmel [29] [1978]) calls "weak inductive knowledge".[9] Accordingly, the state of confidence implicitly exists whenever a person engages with another without the need for reflection about the existence of risk or uncertainty, thereby eliminating the need of choosing among alternatives. In that sense, confidence—unlike trust—emerges when an individual believes that the person or system she interacts with does not have the agency to betray her expectations [43]; p. 397). As such, confidence derives from predictability of future events. It is important to note, however, that confidence does not require a complete mastery and understanding of all the technical components that a particular system is made of—*i.e.* one does not need to understand the workings of a plane in order to feel confident that the plane will fly safely and arrive at destination. In the case of complex systems, confidence can be achieved as a result of previous experiences and general knowledge accumulated over time—*i.e.* common knowledge that very few planes crash or divert their destination—or reliance in the expertise of (trusted) third parties —*i.e.* the engineers who have designed, tested and validated all the pieces that come into the airplane, along with the multitude of regulations on flight safety which ultimately ensure that the journey can be made safely [25]; p. 112).

It should also be noted that confidence does not denote a voluntary disposition, but rather an assured cognitive state of expectation about the future, which emerges progressively over time through the gathering of experience or evidence about the attributes and standard operation of a system. Accordingly, as opposed to trust, which involves individual judgement, confidence reflects a particular state of mind—*i.e.* one does not "decide" to be confident, but rather "is" confident that an event will occur in a particular manner. This is not to say that confidence cannot be disappointed. Yet, as opposed to trust, the undermining of confidence will generally entail blaming other people (or things) rather than oneself. In other words, while a breach of trust will merely lead the trustor to lose faith in a particular individual or organization (without influencing the perceived identity thereof), the undermining of confidence may bring an individual to question the essential attributes and features of a

[7] According to Petit [27]; there are three conditions necessary for the manifestation of reliance to communicate a belief or presumption that the trustee is trustworthy: (1) that there are enough instances of trustworthiness in evidence to make it plausible that a trustor should hold by such a belief or presumption; (2) that the trustor does not have any more salient motives for manifesting reliance; (3) that the trustee is not subject to external pressures to act in a trustworthy way (p. 225).

[8] Giddens [25] defines "access points" as "the points of connection between lay individuals or collectivities and the representatives of abstract systems [or institutions]. They are places of vulnerabilities for abstract systems, but also junctions at which trust can be maintained or built up (p. 88).

[9] Giddens illustrates how confidence can be regarded as a form of weak inductive knowledge involved in many future transactions. For instance, "if a farmer were not confident that a field would bear grain in the following year as in previous years, she or he would not sow" [25]; p.26).

particular person or organization.

Referring to confidence as a cognitive state does not mean that it is a sentiment or a mood. Even scholars who are of the view that confidence (like trust) is a 'social emotion' concur that confidence is not associated with a high level of feeling when compared with faith or trust [44]; p. 229–230). Confidence enables practical conduct, even in uncertain environments, and is therefore considered to be "one of the most important synthetic forces within society" [45]; p. 318). Crucially, it also enables the entering into of contracts, promises and obligations without always relying on the presence of third-party enforcement [46]; p. 4) and as such, the existence of confidence allows for there to be freedom of action without coercion. Seligman, who like us has elaborated on the distinction between trust and confidence, contends that relations in pre-modern societies were governed by confidence, rather than trust, as the actors in such societies had well-defined and ascribed roles (e.g. due to kinship or status by birth) and were sanctioned for not acting in accordance with these roles [46]; pp. 36–37 [47]; pp. 146–148). This contrasts with role expectations that are achieved through contractual obligations, for instance, which are of a more negotiable and variable nature.[10] Using the analytical framework of Robert Merton (role-set theory), Seligman argues that when role expectations can no longer be taken for granted and are negotiable, as the system permits the change of roles (e.g. employee to entrepreneur) and statuses (e.g. availability of separation and divorce for partners, husbands and wives), it becomes more difficult to ensure that a role will be fulfilled through the existence of confidence. Instead, in these cases, the fulfilment of negotiable roles can only be assured by establishing interpersonal trust relationships (1997, p. 40).

Conceptualising confidence as a state of expectation is important for understanding the formation of confidence as well as its dissipation. In comparison to trust, it is arguably easier to build confidence, because it does not require any communication or mutual commitment by at least two actors, but rather emerges through the cognitive process of one single agent [48]; pp. 175, 183–184 [34]; p. 50). This also makes it more difficult to assess whether confidence exists in a given situation, as its psychological quality is harder to identify than the perceptible forms of communication involved in creating trust relationships [48]; p. 184). Conversely, while relationships of trust can be broken by a single act of infringement, the state of confidence is less fragile, as it requires a breach of expectations with regard to a broader context [49]; p. 527). Morgner explains this with the example of the Watergate scandal, in which the revelations of President Nixon's impropriety caused an erosion of trust in the individual but not a loss of confidence in the overall system of democracy. The increase in political interest and higher voter turn-out in the subsequent elections were referred to as evidence of this [49]; p. 525).

Morgner [49] further distinguishes confidence from trust by their *addressability— i.e.* the capacity of someone (or something) to qualify as a recipient of communication. Morgner clarifies this with a literal example: while individuals and collective actors (e.g. organizations) may be addressed in a letter, "[o]ne cannot write a letter to the economy or to society" (or to money, power or other abstract concepts and systems) (p. 519). This is because said concepts and systems, as forms of social reality, do not have fixed motives or intentions nor can they reciprocate, as a trustee does by acknowledging the trust reposed in them or by *a priori* signalling their trustworthiness. It is because of this lack of fixed motivation and mutuality that the interpersonal dimension of trust goes missing and it becomes redundant to speak of *trusting* said concepts or systems (or conversely, being betrayed by them). Instead, such non-addressable concepts and systems can only be handled in terms of the existence or absence of confidence (p. 520). This is particularly relevant today because, as Dunn [50] has noted, the complexity of contemporary societies and the division of labour in these societies necessitates confidence in political, social and economic systems and would not be able to operate simply through interpersonal trust (p. 85).

Most people would agree that confidence and trust are two essential factors for effective interaction, communication and cooperation among individuals, which may subsist both at the interpersonal and institutional level [34,51,52]. Yet, understanding the actual link that connects these two concepts is a more challenging task. Giddens [25] considers that trust is "a particular type of confidence" which entails the expectation of an agent not to be disappointed by the action of another party.[11] Luhmann [10] argues that, while it is true that trust and confidence share a symbolic basis, they should nonetheless be regarded as two distinct concepts, most notably because of their different implications in terms of vulnerability and risk. Indeed, while both trust and confidence refer to a particular set of expectations that could potentially be frustrated, only the former recognizes an element of risk that must be accounted for in the calculation as to whether or not to trust a third party [34].

In light of the different accounts of "confidence" and "trust" provided above, we analyse below the relationship that subsists between these two concepts, with a view to better understanding their mutual influences and dependencies. Indeed, neither trust nor confidence exist in a vacuum, they emerge from a context that comprises both internal (personal) and external (third-party's) contingencies. More precisely, trust and confidence can be regarded as having a concentric relationship with one another, because trust and/or confidence in a given system both depend upon and potentially impact the level of trust and/or confidence in other interrelated systems.

One the one hand, confidence in a system ultimately depends on the level of trust or confidence that one has in the actors or institutions involved in higher-order systems [10]; p. 104 [48]; p. 185). Giddens [25] explains how much of the confidence we experience in our daily activities only subsists because of the trust we have in a variety of expert systems[12] (e.g. the legal system, professional guilds, the scientific community, etc.) which we believe provide the necessary 'guarantees' for us to build expectations on matters which we do not have the ability to exhaustively verify on our own.[13] These expectations are grounded both on previous experience and common knowledge that these systems generally operate as expected, and on the trust assigned to a series of regulatory agencies responsible for overseeing these systems [25]; p.28). As such, confidence also depends on general knowledge about the existence of sanctions from higher-order expert systems [43]. The law has a particularly important function in this context as, in Cotterrell's words, the "[l]aw guarantees systems of confidence, in the main, indirectly by sustaining and encouraging patterns of trust embodied in ideal typical forms of collective involvement or interaction" [53]; p. 75).

On the other hand, confidence in a particular system can also contribute to the establishment of greater and better trust relationships in another system. For instance, people may be more likely to trust their

[10] Seligman goes on to observe that colonialism and impingement on indigenous life eroded confidence as it caused the crumbling of custom and moral obligations (1997, p. 37), creating the need for trust as in modern societies.

[11] According to Giddens [25]; p. 34), "trust may be defined as confidence in the reliability of a person or system, regarding a given set of outcomes or events, where that confidence expresses a faith in the probity or love of another, or in the correctness of abstract principles (technical knowledge)".

[12] "By expert systems I mean systems of technical accomplishment or professional expertise that organise large areas of the material and social environments in which we live today. Most laypersons consult "professionals" - lawyers, architects, doctors and so forth - only in a periodic or irregular fashion. But the systems in which the knowledge of experts is integrated influence many aspects of what we do in a continuous way" [25]; p. 27).

[13] For instance, while we "know very little about the code of knowledge used by the architect and the builder in the design and construction of the home," we nonetheless "trust their competence [and] the authenticity of the expert knowledge they apply" [25]; p.28) because of our confidence in the educational system and qualifications that produce architects.

counterparties in honouring monetary transactions because of the confidence that major fiat currencies will remain a widely-accepted medium of exchange, as well as the confidence in the smooth operation of legal and financial systems.[14] Similarly, one may be more willing to trust a doctor to provide medical advice than a neighbor or a close friend, because the fact that the doctor holds a medical degree and a license is a valid indication of expertise, provided that there is enough confidence in the scientific community and healthcare system. Accordingly, confidence essentially operates as a platform for trust: the more confidence there is in a higher-order system, the easier it becomes for people to establish trust relationships with persons or institutions operating in the lower-order systems.

Armed with this analysis, it is now possible to turn our attention to blockchain technology, in order to analyse the extent to which the adoption of such a technology could successfully boost confidence in the absence of trust (section 3) and, if this is not possible, how to increase the level of trust in a blockchain-based system so as to increase the confidence in its operations (section 4).

3. Blockchain as a confidence machine

It is commonly understood that the raison d'etre of a blockchain-based system is that it does not require trusted third parties. As described by blockchain advocate Andreas Antonopoulos [54]; blockchain technology enables a "shift from trusting people to trusting math". Werbach [55] reiterates this point by defining blockchain technology as an enabler of "trustless trust", where transactional security is achieved via reliance on deterministic computation. Yet, all of these definitions are grounded on a negative argument, framed around the elimination of trust. Such a negative argument is grounded on the idea that a situation characterized by a low level of trust may reduce the willingness for people to transact with each other [56]; p. 111) insofar as they do not wish to take on the risk or the necessary 'leap of faith' that would render them vulnerable to opportunism by others [57]; p. 35). Hence, the negative argument inherent in the notion of a "trustless" technology aims at restoring the willingness for people to transact with one another by completely eliminating the need for trust between parties. This argument does not, however, describes what trust is actually replaced by. In contrast, the positive argument brought forward in this paper is that blockchain-based systems are intended to produce 'confidence' in a particular system—not by eliminating trust altogether, but rather by maximizing the degree of *confidence* in the system as a means to indirectly reduce the need for *trust*. Such a higher degree of confidence allows transactions to take place more easily, by reducing the perceptions of risk associated with these transactions. The next subsection expands on how blockchain technology specifically contributes to building more confidence.

3.1. Replacing trust with confidence

According to Luhman [34]; the higher the complexity of a system, the longer it will take for concrete expectations to develop about the operations of that system. Hence, interacting with a complex system is likely to require more trust than interacting with a single entity, or with a system made of only a few simple parts. Indeed, lack of trust in any of the constitutive parts of a system might bring people to distrust the system as a whole. In that regard, Hume [58] suggests that governments and other complex institutional arrangements should not be trusted at the outset. Rather, as Hardin [59] points out, one should instead focus on setting up the necessary checks and balances and transparency requirements that will enable the emergence of a more trustworthy system. Indeed, if trust is a "device for coping with the freedom of others" [24], the need for trust is less correlated with a situation of power imbalance than from a situation of information asymmetry.[15]

While ensuring a greater degree of transparency might seem like an elusive ambition in the context of social or political institutions, the task can be more readily accomplished in the context of technological arrangements—especially open source software.[16] To the extent that one can understand the code of a particular piece of software, it becomes (theoretically) possible to predict the output of that software, for any given input. Hence, the higher the predictability of the software code is, the higher is the *confidence* in the system and the lower is the need for *trust* in the developers and/or operators of that technological system.

As Szabo [60] observes, blockchains seek to substitute "[t]rust in the secret and arbitrarily mutable activities of a private computation" with "verifiable confidence in the behaviour of a generally immutable public computation". In the case of Bitcoin, for instance, anyone who understands the Bitcoin protocol can be confident that the network will generate a particular quantity of new Bitcoins (12.5 Bitcoins) under specific conditions (whenever a miner finds a new block) and at a particular pace (within an average of 10 min), without the need to rely on any financial institution or other centralized authority, which have the power to print money at their own discretion, within the bounds of institutional mandates. Indeed, one of the core characteristics of Bitcoin is that "no one needs to be trusted" and "no one can pretend to be a trusted party, as there is none" [54]. Moreover, because everyone can hold a copy of the blockchain, users can collectively review and verify all transactions executed on the network, in order to ensure that they are all compliant with the rules of the protocol [61]. This provides network participants with a sense of "being in control" [20], as illustrated by the expression "*Don't Trust, Verify*" which has become the mantra of many blockchain communities.

More generally, confidence in any blockchain-based system is achieved through a combination of multiple elements. First, there is confidence in the mathematical rigour of the hashing algorithm, especially with regard to the cryptographic primitives that constitute the underlying foundation of a blockchain (e.g. public-private key cryptography, hashing functions, etc). Mathematics does not require trust, to the extent that it can be proven to work in a particular manner. This leads to a very high level of predictability, since the rules of the protocol are guaranteed by the technological design of the blockchain protocol. Giddens would attribute the users' confidence to the existence of expert systems: systems in which the knowledge of experts is embedded and taken for granted by laypersons, due to a combination of faith, confidence and trust (1990, pp. 27–29). With regard to Bitcoin, confidence in the system is mostly supported by the fact that Bitcoin's open source code has been scrutinized by millions of people, and that the Bitcoin protocol has never been hacked despite the significant benefits that could derive from it. In the context of open source software, Seligman [46] argues that this relationship with expert systems also includes confidence or trust in the core programmers, as well as the "various forms of social control and sanctioning mechanisms" that ensure their performance (p. 25).

Second, blockchain-based networks generate confidence in the economic incentives and game theoretical schemes that govern the network, grounded on the premise that miners will always act in such a

[14] The relationship between money, trust and confidence has been analysed by Simmel [29]]) cited in Giddens [25]; p.26).

[15] According to Giddens [25]: "There would be no need to trust anyone whose activities were continually visible and whose thought processes were transparent, or to trust any system whose workings were wholly known and understood" (p. 33).

[16] Yet, in addition to the lack of information as one of the main drivers of trust, Luhmann [10] introduces the additional element complexity. Even a perfectly transparent system might require some level of trust, because the system might simply be too complex for an individual to perfectly analyse and understand or such an analysis may require so much effort that it would make more sense for the individual to trust the enablers of the system (and assume the corresponding risk) instead of scrutinizing it in details.

way as to maximize their financial rewards.[17] Yet, because miners are ultimately controlled by people, and might therefore be bribed or corrupted, additional guarantees have been introduced into these systems in order to further reduce the need to trust any individual miner. On the one hand, the consensus algorithm of most blockchain-based networks (e.g. Proof of Work or Proof of Stake) is intended to distribute trust among a large variety of miners, thereby reducing the risk of individual opportunism. On the other hand, because all participating nodes (such as miners and validators) hold a copy of the blockchain, they can always verify that every recorded transaction is valid and legitimate. Hence, anyone interacting with a blockchain may have a high level of confidence that it will operate as planned, even if they do not know (and therefore do not trust) the parties operating or maintaining the network.

Blockchain technologies operate on the basis of deterministic functioning and consequent predictability, which is enabled by their reliance on mathematical properties of hash functions and public-private key cryptography, and the soci-oeconomics of associated game-theoretical mechanisms. The perceived automation and impartiality inherent in the protocol of a blockchain-based network becomes, therefore, a new source of *confidence* that transpires in many fields of endeavor. Because the technological infrastructure is not managed (nor controlled) by any social or political institution, blockchain-based systems are often regarded as a superior alternative to many of our current human-led, and therefore corruptible institutions [20]. For instance, in the context of supply chain management, blockchain-based solutions have been devised to guarantee the source and authenticity of goods [62], and to increase the transparency of the supply chain [63] by certifying the use of specific production processes and the delivery of physical assets [64]. Similarly, in the context of the Internet of Things, blockchain technology provides many new opportunities for more robust and reliable IoT infrastructure [65], by supporting secure peer-to-peer communications and greater interoperability between devices from different manufacturers [66]. When combined with 5G, blockchain technology could play a significant role in facilitating the seamless integration of smart agents or devices, whose interactions can be securely registered, authenticated and validated in a trusted and decentralized manner [67]. More generally, blockchain-based systems can be leveraged to provide more confidence, transparency, and auditability in a variety of business processes [68], as well as greater traceability and predictability in sectors such as clinical trials [69] or the energy sector [70].

Yet, despite the increased confidence that blockchain technology could provide, the existence of uncertainty and risk becomes apparent upon closer inspection. The act of making payments or other currency transactions with a crypto-wallet implicitly involves trusting the organization(s) responsible for providing the crypto-wallet and cryptocurrency exchanges. The need for trust may be mitigated if there is enough confidence in the expert systems that inhabit the blockchain ecosystem, as well as in the legal system that will provide for financial and consumer protection. However, confidence in a blockchain-based system may also be undermined by the actions of core developers who hold significant influence over exceptional (yet fundamental) decisions concerning changes in the blockchain protocol, as well as by the possible collusion of miners or mining-pools. Hence, despite the qualification as a trustless system, enabled by the building of confidence, the need for trust in a blockchain-based system is not eliminated.

3.2. Bringing trust back in

Each blockchain-based network is a complex system composed of many separate components that interact with one another to ensure the operations of the overall system. Hence, even though there is no centralized trusted authority, people need to believe (as a result of either trust or confidence) that the network will operate as expected. At first glance, a blockchain-based network might appear to operate in a deterministic and self-contained manner, independently of the influence of third parties. Yet, the reality is that these networks are hybrid systems made up of both technical and social components [41].

The idea that technology can be designed to be fully impartial, unbiased or apolitical to existing human-led institutions ignores the fact that all "artifacts have politics" [71]. The design of any technology comes with some underlying political choices—including the choice of being apolitical—which are reflected in the manner in which people can or cannot interact with the technology. In the case of a blockchain system, the characteristics of decentralization, censorship-resistance, tamper-resistance and automation—which all contribute to increasing the degree of confidence in the system—require a certain level of trust to be put in a variety of human actors, which operate both within and outside the system. This may not be readily apparent to the average user of a blockchain, such as the user of a crypto-wallet, who may be said to be in a state of confidence.

In short, blockchain-based systems are socio-technological assemblages [72] which are made up not only of code, but also of a large variety of actors, including miners, validators, programmers, cryptocurrency and token holders, end-users, and, to a lesser extent, regulators. Having confidence in the system ultimately means trusting the whole assemblage of actors associated with that network [20]. Blockchain technology will reduce the need to trust any one of these individual actors. However, as demonstrated above, it does not eradicate the need for trust altogether [61]. Rather, the technology displaces trust in the technological artifacts that underpin a blockchain-based system, and shifts it towards the network of actors that contribute to operating and maintaining the system. Accordingly, despite the decentralized nature of a blockchain-based system, some level of oversight is nonetheless necessary in order to ensure the proper functioning of the network [20]. The following sections illustrate how trust is required from at least four different types of actors involved in the operations and maintenance of a blockchain-based network.

First, a few economic players—such as the largest mining pools and mining farms, as well as the most popular online exchanges and blockchain explorers—have become centralized points of failure and control in the governance of many blockchain networks.[18] These actors have significant influence over the operations of the network, and are likely to leverage that power to further their own economic interests, either directly or indirectly—including by furthering the interests of the overall system.[19]

Second, core developers and open source contributors have the power to influence the evolution of the blockchain-based network, by lobbying for or against the introduction of specific features into the technical design of the platform. While most blockchain-based networks are open source (meaning that anyone is free to contribute code to the project), actual production and maintenance of code is generally done in a considerably centralized and hierarchical way, with only a few core developers having the power to decide which contributions will be

[17] Of course, this also requires confidence that the legal system(s) will not operate in a way that would prevent miners from acting in line with these game theoretical incentives (including acting through omission).

[18] For instance, as of September 2019, the three largest mining pool on Bitcoin and two largest mining pools on Ethereum control nearly 50% of the overall hashing power on their corresponding network. For an updated overview of the hashing power distribution, see https://www.blockchain.com/en/pools and https://www.etherchain.org/charts/topMiners.

[19] For instance, in 2013, the Bitcoin experienced a technical crisis as the network split into two separate networks as a result of a discrepancy in the code of two different versions of the Bitcoin client (version 0.7 and 0.8). In order to resolve the issue, the largest mining pools collectively decided to intervene by downgrading their clients, thereby shifting their mining power back to the old branch of Bitcoin. In practice, the mining pools have effectively executed a 51% attack on the Bitcoin network, in order to resolve the fork. For more details, see Narayanan [112].

accepted or rejected into the core repository. These decisions may appear to be purely technical in nature but they are also political choices, given the implications they have on the identity of the system and potential economic repercussions. It is unlikely that the average cryptocurrency holder, for instance, expects core developers to make political decisions that will affect the value of the cryptocurrencies they hold, yet the decision to upgrade the protocol in one way or another will necessarily affect the way the cryptocurrency will be perceived by the public at large, thereby positively or negatively impacting its overall value.[20]

Third, cryptocurrency and token holders, as well as users more generally (albeit to a lesser extent) might also have a voice in dictating the type of changes they would like to see in a blockchain-based network.[21] Yet, insofar as many of these players have conflicting interests, maintaining the operation of the network might give rise to complex governance problems when it comes to deciding upon a particular protocol change—as we have already seen in the context of Bitcoin [73] and Ethereum [74].

Fourth, regulators might also intervene by either approving or disapproving the use of a blockchain-based system. If legitimacy is a prerequisite for mainstream adoption, regulators have the power to significantly affect the adoption of a particular blockchain network by creating regulation that will make it easier or harder for the network to be employed by existing institutions, consequently impacting the trust that people might place in the technology.[22]

With the above in mind, the denomination of a blockchain-based system as "trustless" or "trust-free" technology is largely misleading. To paraphrase Lustig & Nardi [20]; algorithms draw their authority from both the confidence one has in its proper functioning as well as the trust one has in the socio-technical actors that develop and mediate these algorithms. Yet, trust is never absolute [75], and neither is confidence—both depend on external contingencies in which a given system operates. In the context of a blockchain-based system, to the extent that there are people at the extremities of the system, trust can never be completely eliminated, it is partially displaced to the developers and maintainers of the network [41]. Hence, while the blockchain protocol might contribute to increasing the confidence in the manner in which transactions will be processed, such a degree of confidence is only possible to the extent that one can trust the network of miners and validators, cryptocurrency exchanges and holders, as well as the core developers to act in a way that does not undermine the security, reliability and predictability of the blockchain-based system.

It is because of this invariable need for trust at the interstices of any blockchain-based system, and the implications that any breach of trust could have on the overall confidence in the system, that governance questions arise. The following section explains the unique challenges related to the governance of a blockchain-based system, and considers whether solutions derived from constitutional and polycentric governance theory may account for these particularities.

[20] This state of affairs resembles the illustration used by Seligman [43] of a client having confidence in the plumbing skills of a professional plumber, but having to exercise a considerable degree of trust in leaving her child with him–a responsibility that the client has no reason for expecting the plumber to be able to do adequately (p. 399). Similarly, the average wallet-holder faces uncertainty about the developers discharging their political responsibility properly.

[21] This was illustrated, for instance, after TheDAO hack [74], when the Ethereum community had to gauge the public opinion as to whether or not to fork the Ethereum network. Different mechanisms have been explored to collect a maximum of opinions from the largest variety of stakeholders, including systems of token-based voting (Carbon voting), Twitter polls, and open discussions in public forums.

[22] Although this comes with the risk that widespread adoption of a blockchain-based system like Bitcoin might ultimately lead it to becoming like the very institutions that it was originally intended to replace [20].

4. Challenges of governance

In the preceding section, it was shown that while blockchain-based systems replace trust with confidence, this confidence is predicated on trusting a variety of actors that are associated with the system. Governance becomes a crucial issue as good governance practices need to be adopted in order to prevent these actors from operating in an untrustworthy manner, thereby undermining confidence in the system as a whole.

In the context of liberal democratic institutions, good governance generally implies adherence to the Rule of Law, *i.e.*, the clear and impartial application of existing laws and regulations, unaffected by social or political considerations. Assessing whether a particular system complies with the Rule of Law requires accounting for at least the formal and procedural attributes of law [76]: laws must be clear, stable, clearly publicized and applied prospectively [77]; p.39); and must be enforced fairly, equally and evenly [78,79]. Governments themselves should act within the bounds of these laws and not act arbitrarily [26]. A "thicker" interpretation of the Rule of Law [80] also accounts for the substantive aspects of the law, which must guarantee the protection of fundamental rights—such as private property [81] and human rights [82]—as well as the integrity of the adjudication process, through fidelity to theories of fairness and justice which undergird a set of legal rules [83]; p. 338).

In the last few decades, some of the principles and requirements of good governance have been applied to the digital realm, with serious discussions concerning the design of procedural and substantive constraints to improve Internet governance. The management of the domain name system by the Internet Corporation for Assigned Names and Numbers (ICANN) provides an interesting illustration of the issues at stake. While the administration of the domain name system is only one of ICANN's functions, it is a politically sensitive one as it engages concerns ranging from trademark disputes to the appropriation of names that are culturally and ecologically significant (e.g. .amazon) [84]; pp. 337–338). The California-based ICANN was ostensibly subject to multi-stakeholder governance from its inception [85]; p. 115), including national governments, internet service providers, business actors, non-profits and internet users, but primary control was exercised by its Board of Directors and ICANN's public principal, the US government [86]; p. 561). For most of its existence, it was argued that the non-profit Board is effectively unaccountable as it lacked a mechanism for ensuring that its Directors acted within their authority and commitments, given that ICANN lacked corporate members that could enforce the Board's fiduciary duties and the intervention of California's Attorney General was unpredictable and contingent on political circumstances [87]; p. 49). Moreover, due to its direct relationship with the U.S. Department of Commerce since its creation in 1998, ICANN's authority over the assignment of domain names was not exclusively an outcome of multi-stakeholder governance [87]; pp. 8–9), as evidenced by the U.S. government's veto of ICANN's decision to award a Florida-based business the controversial ".xx" top-level domain name [88]; pp. 126–127).

In 2009, due to extensive criticism about the U.S. Government's extensive powers over the governance of ICANN, the U.S. Government signed an agreement aimed at reiterating ICANN's commitment to multi-stakeholder governance without, however, removing it from the oversight and control of the U.S. Department of Commerce. It was clear that the U.S. Government did not favor bringing ICANN under the control of an intergovernmental organization, given its potential consequences for the freedom of the internet, but any private alternative required procedural and substantive safeguards to ensure its accountability. To improve the internal governance of ICANN, recommendations were made that, among other things, drew from constitutional theory. Weber & Gunnarson [87]; for instance, suggested that the organization be bound to a formally ratified written charter (specifying standards and remedies for violations of the charter) and only enjoy narrowly-defined enumerated powers over technical issues, that the rights of stakeholders be clearly declared *ex-ante*, that the directors of its

board be removable and that its decisions be reviewable and reversible by an independent body (pp. 62–71). When ICANN eventually terminated its contract with the Department of Commerce in October 2016, thereby moving further away from the U.S. government, its bylaws were substantially amended. The inspiration drawn from constitutional law principles is apparent. Two major reforms that were introduced were the separation of the policymaking and technical functions of ICANN–between the Board and the newly-created Post-Transition IANA (PTI) public benefit corporation–and the creation of an Empowered Community nonprofit association that is composed of ICANN's constituent organizations and advisory committees. This multi-stakeholder association has meaningful tools to enforce the duties of ICANN's Board, as it has the power to initiate a review of the Board's actions, appoint or remove directors, reject bylaw amendments and approve fundamental bylaw amendments [86]; p. 271).

While research that applies constitutional law principles to Internet governance is illuminating, there are limits to its applicability to blockchain technology. In the context of blockchain-based systems, an important distinction must be made between the Rule of Law (defined and enforced by governmental institutions) and the Rule of Code (defined and enforced by technology). While governments have the monopoly of force over their own territory, they cannot easily exercise that power over a blockchain-based system. Indeed, because of the distinctive characteristics of public blockchain networks—most notably, their distributed and decentralized character, their inherent pseudonymity (or anonymity in the case of e.g. Zcash or Monero), and their (purported) immutability and incorruptibility—the laws of national jurisdictions are difficult (but not impossible) to enforce on these systems. Blockchain-based systems are governed by an alternative set of rules and procedures—sometimes referred to as *Lex Cryptographica* [89]—which are defined by the underlying blockchain protocol, and are enforced by a distributed network of miners and validators maintaining the system.

This raises the question as to the extent to which the blockchain-based systems can operate outside of the purview of the law. Going back to the previous literature of Internet regulation, in his landmark book "*Code and other laws of cyberspace*", Lawrence Lessig [90] investigated the degree of regulability —or "unregulability"— of the Internet network, claiming that, while ordinary laws apply equally in the physical and digital world, the effectiveness of these laws might vary depending on the architecture of the different components of the network. Yet, while governments have the opportunity to regulate the code of Internet platforms, by regulating the institutions that produce, maintain or operate that code, in the case of a blockchain-based system (whose code is executed by a distributed network of peers) there is no identifiable, single entity or group of entities upon which a government can legitimately exert pressure, in order to mandate a particular technological design.[23] In other words, the lack of any single point of failure and control (such as ICANN in the context of Internet governance) contributes to increasing the resilience of blockchain-based systems, while also making it more difficult for national laws to be enforced on them [91].

Accordingly, while an analysis of the extent to which existing regulations can prevail over the rules of a particular blockchain-based system is outside the scope of this article,[24] given the greater degree of autonomy that characterizes these systems, it is nonetheless worth investigating whether some of the basic tenets of the Rule of Law can—to a limited extent—be replicated in the Rule of Code. This requires an analysis of the extent to which some of the procedural rules and substantive constraints that have been adopted in traditional (centralized) governance structures can be transposed in, or adapted to the context of a technological framework [92], and how these rules can be enforced—short of formalizing a sovereign authority with coercive power.

While national laws are defined by the legislative power and are subsequently enforced by judicial and executive authorities, the rules and procedures of a blockchain-based network are defined by the developers and are subsequently "adopted" by a variety of actors, who willingly agree to submit to these rules. While the protocol rules will be enforced by the miners maintaining the network, anyone is free to exit the system or even fork it into a separate system, operated by a different protocol. Although there are many incentives for people to remain in the same system (mostly economic incentives resulting from network effects), no one has the legal authority to coerce anyone into submitting to the rules of a particular protocol. Participation in any given blockchain-based system is purely optional and voluntary. Hence, any technological constraints that would affect the governance of a particular blockchain-based system will have to be agreed upon by all (or a sizable majority) of participants in the network.

Blockchain governance is, therefore, essentially driven by the economic and game-theoretic incentives coded into the protocol, as well as the social norms and community rules that bring all network participants to converge towards a particular "schelling point" (the choice that everyone thinks everyone else will make). This pattern of behaviour is similar to what Unger calls *customary* or *interactional* law, i.e. "any recurring mode of interaction among individuals and groups, together with the more or less explicit acknowledgment by these groups and individuals that such patterns of interaction produce reciprocal expectations of conduct that ought to be satisfied" (1977, p. 49). Interactional law, so defined, can only exist in systems with solidified role expectations that provide a high degree of confidence regarding individuals' behaviours [43]; p. 394). In the case of a blockchain-based network, such a degree of confidence can be found in the activities of miners, which are expected to process transactions in accordance with the blockchain protocol, without arbitrarily discriminating between specific transpactions. In this context, confidence emerges from the fact that it is in the economic interests of all miners to follow the rules, as collusion by a majority of miners could lead to a drastic drop in the value of the associated cryptocurrency.

Yet, this interpretation of blockchain-based systems is a simplistic one, which ignores circumstances in which confidence in the system may be lost, as a result of the actions undertaken by a multiplicity of actors involved in the maintenance and governance of a blockchain. Indeed, this reading fails to address the fact that a blockchain is a socio-technical system in which reciprocal expectations of conduct may be frustrated. Actors involved in the maintenance of a blockchain-based system can sometimes "overpower"[25] other actors in the system,

[23] This is distinct from the economic argument that jurisdictions can exert pressure on a blockchain system through the prohibition of mining activity or the closure of cryptocurrency exchanges as its effect on the design of a network is indirect. The distributed nature of blockchain systems means that it can tolerate the loss of miners without the entirety of the system being compromised.

[24] Several legal scholars have been exploring the interplay between the rules established by a blockchain-based system and the laws enshrined in national jurisdictions, with a view to determine whether one can overcome the other. See e.g. De Filippi & Wright [89]; Werbach [22]; Finck [98]; Reyes [113]; Yeung [114]; Walch [115].

[25] Unger's distinction between public and non-public rests on there being a particular group that can stand apart from other groups in a system (what we most commonly see as centralized government) and to an extent being beyond the purview of the law applicable to other groups. This group can overpower other social groups and limit their interaction, if it so wishes (1977, pp. 50, 58).

thereby limiting the impact of positivist technological governance through Rule by Code (a.k.a "on-chain" governance).[26] Indeed, governance processes that subsist outside of the technological infrastructure (a.k.a "off-chain" governance) are often driven by actors with higher social capital or better technical skills, who can therefore exercise a higher degree of influence on decisions that generally require consensus by distributed actors (e.g. whether or not to implement a hard fork).

In short, interactional or customary law fails when the conditions for confidence no longer subsist. This becomes particularly apparent in moments when (implicit) shared values are called into question, as illustrated by 'states of exception', such as the one triggered on the Ethereum network in the aftermath of TheDAO attack [93]. It is in these situations that blockchain-based systems may experience a coalescence of private interests (with certain actors being more influential than others) exercising powers that are considered to be a sovereign prerogative—*i.e.* to decide on the exception. While TheDAO attack was exceptional–in multiple senses of the word–it is possible to observe similar failures of customary law in standard operations of blockchain-based systems as well. For instance, a participant in a blockchain-based system may expect that a miner will always act in accordance with the consensus algorithm of that system but empirical research has shown that miners can deviate from the standard protocol and engage in 'selfish mining'[27] [94].

In Unger's view, "as soon as there is a well-differentiated set of social ranks with varying degrees of power over one another, group relationships are thrown into a permanent, though often latent, instability" [95]; p. 60), with pervasive relationships of dependence and dominance necessitating the emergence of some form of centralization. This is because only a centralized entity, such as a state, can stand above the other actors in a system to limit their powers and resolve their disputes, while simultaneously being able to claim impartiality so as to retain the allegiance of the other actors in the system (*ibid*, p. 61).

However, pivoting towards centralization would be counterproductive in building confidence in public blockchain-based systems as these systems are intended to operate as a decentralized infrastructure. Blockchain-based systems are arguably, polycentric systems of governance [96–98]; p. 185)— where there are diverse, overlapping clusters of influences (instead of a single dominant centralized authority), which each enjoy some degree of autonomy and decision-making power [97]; p. 831 [99]; p. 932). A polycentric governance system emerges from the fact that, although all clusters remain relatively independent from each other, when it comes to making decisions, they necessarily account for what the others are doing [100]; p. 29). This is particularly true in the context of overlapping jurisdictions (e.g. when their influence and decision-making authority overlaps in scope or subject-matter). That is not to say that every actor in a polycentric governance system is involved in decision-making activities; some may simply have a critical supporting role in technical or policy issues, with no explicit decision-making authority [99]; p. 933). Hence, such a level of interdependence does not have to be demonstrated through conscious efforts at system-wide coordination, but can be evidenced by regular efforts at coordination as a matter of practice (*ibid*, p. 38).

According to Polanyi [96]; the particularity of a polycentric system, is that, as a result of the interdependence between this web of actors, a common set of rules, norms and strategies emerge to guide the behaviour of a large majority of actors within the system [100]; p. 40). This repertoire of rules are created irrespective of whether the actors in a system cooperate with each other or are in competition with one another. These rules may be general and domain-specific. General overarching rules are intended to counteract tendencies towards monocentricity; they include rules that provide institutional mechanisms for separation of powers, monitoring, conflict resolution, appeal, system entry and exit. Domain-specific rules are tailored to the needs of particular domains, such as private production or public service provision, and often supply the mechanisms needed for a particular domain to effectively self-organize [101]; pp. 71–73). For instance, in the context of resource management, a single actor may hold multiple, related positions. An individual can be a representative serving on the board of a multi-stakeholder organization that manages a particular resource, as well as a consumer of such a resource. Such a situation might require an adaptation of general rules to the needs of a particular domain, ranging from customized forms of informal and formal dispute resolution, to the introduction of redundant decision-making processes [99]; p. 945). Redundant decision-making generally occurs in the context of overlapping jurisdictions, i.e. when multiple actors have decision-making authority over the same domain. For instance, fishermen often have informal rules about not catching certain fish during their breeding season and the State also imposes a law sanctioning the catching of the same fish during that same period.

Together, the combination of general and domain-specific rules are broadly understood as the 'constitution' of a polycentric system [102]; p. 219) Indeed, independent actors within a particular system are confronted with a 'Faustian bargain': needing to forgo a degree of local autonomy to benefit from being part of a functioning and properly coordinated larger-scale ecosystem (*ibid*, p. 220). A well-documented example of such a 'constitution' is the New York City Watersheds Memorandum of Agreement, which emerged from voluntary and bottom-up negotiation among a variety of actors involved in a large-scale polycentric water-management system. The Memorandum was negotiated between the City of New York, the State of New York, the federal United States Environmental Protection Agency, various municipal parties, an inter-municipal body comprising municipalities within the New York City Watershed and a multi-stakeholder non-profit corporation (The Catskill Watershed Corporation)—each with their own jurisdiction and decision-making power over the same water-management system. The Memorandum of Agreement establishes the rules for multi-stakeholder governance over this common resource; it sets out the terms on which New York City can acquire land from willing sellers, as well as a series of infrastructural and economic development commitments by the Catskill Watershed Corporation to keep the surface water supply clean. Compliance with these rules is monitored by an independent multi-stakeholder body, The Watershed Protection and Partnership Council, which also has the authority to resolve disputes between jurisdictions [102]; p. 232).

At first glance, a blockchain-based network can be regarded as a polycentric governance system composed of a variety of actors (i.e. miners and validators) who are collectively in charge of securing and maintaining the network, and who collectively agreed to follow the same set of rules or 'constitution' (i.e. the blockchain protocol). Even though some miners and validators have more power than others (e.g. large mining-pools, crypto-currency exchanges, blockchain explorers, etc.), no one has the ability to unilaterally change the protocol, or to tamper with the data recorded on the blockchain. Yet, if we consider a blockchain-based network from a broader perspective, looking at both on-chain and off-chain governance, the polycentric character of the network might be significantly diminished, as a few influential actors ultimately have the power to affect the operations of the overall network—often in order to further their own interests. Accordingly, in order to increase confidence in these systems, and reduce the risk of opportunism, the content of the general and domain-specific rules of public blockchain systems have to be carefully crafted not only with regard to on-chain, but also with regard to off-chain governance.

In the accounts discussing existing polycentric governance systems,

[26] Unger defines positivist law as being law that is articulated and codified, rather than implicit and evinced through conduct.

[27] This is when a miner withholds the fact that it has mined a block by not broadcasting this information to the other participants in the blockchain network. The miner can continue to mine the next block and opportunistically reveal this information later when it has demonstrated relatively more proof-of-work compared to other miners, so as to realize a higher financial reward.

the general and domain-specific rules that have been typically proposed for effective governance closely resemble those recommended to strengthen the Rule of Law, particularly within a federalist constitutional framework. Some have gone so far as to suggest that only explicitly polycentric arrangements (e.g. separating disputing parties from the arbiter of a dispute) can come close to realizing the Rule of Law [103]; pp. 305, 308). Overall, the link between polycentric governance and the Rule of Law is not coincidental, as both Michael Polanyi and Vincent Ostrom, two early theorists of polycentricity, were deeply interested in how polycentricity may contribute to preserving the Rule of Law [104]; p. 237 [105]; p. 14).

With this in view, it may be useful to investigate how the procedural and substantive constraints that characterize a thick conception of the Rule of Law in an ideal-type polycentric governance system could be adapted to the context of blockchain governance. Public blockchain systems have relatively low costs of exit, which is desirable from the perspective of polycentric governance [102]; p. 229). Yet, as discussed above, when it comes to entry, requirements have become relatively high for the standard operations of on-chain governance (e.g. mining requires a lot of hashing power, token-based voting require extensive token holdings) and is even higher for positions of significant political influence in the context of off-chain governance (e.g. core-dev or majors crypto-currency exchanges). As a result, the governance of most blockchain-based systems is highly centralized: on-chain governance is inherently plutocratic, dominated by a few large operators or individuals who control most of the mining resources and/or token holdings, whereas off-chain governance most often operates as a technocracy, with a few influential players dominating both the front-stage and the backstage [106].

As it has been argued in this article, to enhance confidence in the system, governance cannot be limited to the introduction of codified functions and technological guarantees at the on-chain level but also requires institutional mechanisms and constitutional guarantees at the off-chain level. However, most of the procedural safeguards (such as transparency, representativeness, direct accountability, separation of powers and avoidance of conflicts of interest), as well as substantive safeguards (such as the protection of vulnerable actors, defining the rights, duties and attributes for politically influential roles) have been defined for traditional institutions with a centralized governing body. In the context of a blockchain-based system, where there is no centralized coordinating authority nor coercive force that can *impose* a particular constitution onto the various network participants from above, it may be necessary to adapt these constitutional safeguards so that they can be more easily applicable—and, ideally, enforceable—in a governance system that is decentralized and polycentric. Exploring how this may be achieved requires further research.

5. Concluding remarks

Blockchain technology is often described as a 'trustless' technology [55,107] because it eliminates the need for a trusted authority and replaces it with a system of publicly verifiable proofs. However, this characterisation is problematic because it does not account for the multiple layers of trust inherent in blockchain governance [106], and the complex power dynamics that subsist underneath the technological infrastructure of many blockchain-based systems [108].

This article tries to move away from the definition of blockchain technology as a "trustless" system or "trust machine" (e.g. Ref. [7], to focus instead of what blockchain technology actually brings to the table. It argues that blockchain technology should instead be regarded as a "confidence machine" in the sense that it increases the confidence in the operation of a particular system, and *only indirectly* (*i.e.* as a corollary to that) reduces the need for trust in that system.

To substantiate that argument, the article provided an in-depth literature review of the various conceptions of "trust" and "confidence" as described by different authors and from a variety of disciplines, with a view to identify both the commonalities and key characteristics that distinguish these two concepts, as well as the mutual relationships that subsist between them. Without adhering to any particular definition, we found that most accounts of trust regard it as a decision or predisposition to make oneself vulnerable by delegating a task or a choice to a trusted third-party, under the expectation that he or she will act in line with one's personal interests, while nonetheless acknowledging the risk that the trust one has conferred might be—willingly or unwillingly—violated by such party. Conversely, confidence is generally used to describe a particular state of mind that creates expectations as regards the behaviour of a person or the operations of a system, but that does not entail any sentiment of risk or vulnerability, because it is grounded on prior experience or general knowledge about a particular state of affairs. As such, while trust is often associated with a feeling of uncertainty, confidence is generally associated with a feeling of predictability [34].

Blockchain technology produces confidence (and not trust) in blockchain-based systems based on an understanding of their procedural and rule-based functioning, which is derived from mathematical knowledge and cryptographic rules, as well as a long-standing account of its past performance. By creating strong expectations about the proper operations of blockchain-based systems, the technology ultimately increases confidence in these systems, thereby eliminating the need for any centralized "trusted" authority, as well as the requirement to trust any of the actors who interact over a blockchain network.

However, the absence of a trusted authority in charge of managing and coordinating interactions over a blockchain-based network does not, in and of itself, make it a "trustless technology". In fact, while trust is less relevant when it comes to the standard operations of a blockchain-based system, it is nonetheless necessary to trust the actors securing and maintaining the underlying blockchain network, in order to guarantee a sufficient level of confidence in any of the blockchain-based applications operating on top of that network. Confidence in a procedural system such as a blockchain ultimately depends on the proper governance of that system. This means that the increased confidence derived from the use of blockchain technology is inherently correlated with the degree to which the various actors involved in the governance of the underlying blockchain infrastructure can be trusted to act as expected. These includes miners and mining-pools, responsible for processing and validating transactions, but also large commercial operators, such as cryptocurrency exchanges or custodian wallet providers, who can leverage their market power to unilaterally impose their decisions onto their user-base, as well as core developers and social media influencers, whose voice can contribute to shifting the schelling point. Regulators and policy makers also have a role to play in the governance of blockchain-based systems, to the extent that they can introduce legal restrictions and constraints in order—albeit indirectly—influence the decisions taken by any of these actors.

The governance of most blockchain-based systems has been constructed in such a way as to distribute trust over a large number of actors, with different interests and preferences, so that no single actor has the capacity to unilaterally affect or influence the operations of the overall network. Problems emerge, however, when standard governance practices are threatened in the case of an emergency that calls for decision-making beyond the scope of ordinary procedures—as in the case of TheDAO attack on the Ethereum network [93].

Accordingly, the article concludes that blockchain technology is a confidence protocol that builds upon an external layer of trust, grounded into the governance of the underlying blockchain protocol. Although it is possible to enhance confidence in the proper operations of blockchain-based systems through the introduction of a series of technological guarantees related to *on-chain* governance, the robustness of the underlying governance system requires a whole different set of constraints that extend beyond the scope of a purely codified protocol and code-driven rules. Hence, in order to ensure a proper level of confidence in such blockchain-based systems, it may be necessary to introduce a series of procedural and substantive constraints related to *off-chain* governance, addressing both situations of normalcy and states of exception.

While the principles of legal and constitutional theory, such as those enshrined in the Rule of Law, might be a useful starting point for this exercise, the challenge is that these principles were designed with traditional centralized institutions in mind, and do not easily map to a decentralized setting. Similarly, in the context of Internet governance, the challenges related to the governance of a decentralized global network like the Internet were tackled through the progressive introduction of new points of centralization—such as ICANN, or large online operators more generally—responsible for managing and policing the network. The inherently decentralized architecture of blockchain-based systems introduces a whole new set of governance challenges, which are similar to those found in the context of global governance and international law. These disciplines might provide valuable insights on how to tackle the governance of polycentric systems [96,109], characterized by the imbalanced power dynamics between multiple clusters of power. Yet, additional research is needed to identify ways in which the Rule of Code enshrined in a blockchain-based system could reflect some of the prerogatives of the Rule of Law, without compromising on the decentralized nature of the overall system.

CRediT authorship contribution statement

Primavera De Filippi: Conceptualization, Writing - original draft. **Morshed Mannan:** Conceptualization, Writing - original draft. **Wessel Reijers:** Conceptualization, Writing - review & editing.

Acknowledgments

This research is funded by the European Research Council (ERC) under the European Union's Horizon 2020 Research and Innovation Programme (Grant Agreements No. 716350 and No. 865856).

We would like to acknowledge the thoughtful comments of Christopher Wray, Judith Donath and Balazs Bodo.

Appendix A. Supplementary data

Supplementary data to this article can be found online at https://doi.org/10.1016/j.techsoc.2020.101284.

References

[1] T.C. Earle, Trust, confidence, and the 2008 financial crisis, Risk Anal. 29 (6) (2009) 785–792.
[2] R. Gallagher, Twitter helped Chinese government promote disinformation on repression of uighurs, The Intercept (2019). https://theintercept.com/2019/08/19/twitter-ads-china-uighurs/.
[3] V. Ryan, Google is deepening its involvement with Egypt's repressive government, The Intercept (2019). https://theintercept.com/2019/08/18/google-egypt-office-sisi/.
[4] R. Gallagher, G. Greenwald, How the NSA Plans to Infect 'Millions' of Computers with Malware, The Intercept, 2014, 12 March 2014.
[5] G. Vidan, V. Lehdonvirta, Mine the gap: bitcoin and the maintenance of trustlessness, New Media Soc. 21 (1) (2019) 42–59.
[6] F. Hawlitschek, B. Notheisen, T. Teubner, The limits of trust-free systems: a literature review on blockchain technology and trust in the sharing economy, Electron. Commer. Res. Appl. 29 (May-June) (2018) 50–63.
[7] The Economist, The Promise of the Blockchain: the Trust Machine', The Economist, 2015 available at: https://www.economist.com/leaders/2015/10/31/the-trust-machine.
[8] B.A. Misztal, Trust in Modern Societies: the Search for the Bases of Social Order, Blackwell, Oxford, 1996.
[9] F.L. Flores, R.C. Solomon, Rethinking trust, Bus. Prof. Ethics J. 16 (1) (1997) 47–76.
[10] N. Luhmann, Familiarity, confidence, trust: problems and alternatives, in: D. Gambetta (Ed.), Trust: Making and Breaking Cooperative Relations, Oxford University Press, Oxford, 2000.
[11] C. Foster, J. Frieden, Crisis of trust: socio-economic determinants of Europeans' confidence in government, Eur. Union Polit. 18 (4) (2017) 511–535.
[12] C.J. Tolbert, K. Mossberger, The effects of E-government on trust and confidence in government, Publ. Adm. Rev. 66 (3) (2006) 354–369.
[13] F. Fukuyama, Trust: the Social Virtues and the Creation of Prosperity, The Free Press, New York, 1995.
[14] R.D. Putnam, Bowling Alone: the Collapse and Revival of American Community, Simon & Schuster, New York City, 2000.
[15] P. Sumpf, System Trust: Researching the Architecture of Trust in Systems, Springer, Berlin, Heidelberg, 2019.
[16] E. Keymolen, Trust on the Line: A Philosophical Exploration of Trust in the Networked Era, Wolf Legal Publishers, Nijmegen, 2016.
[17] M. Coeckelbergh, Can we trust robots? Ethics Inf. Technol. 14 (1) (2012) 53–60, https://doi.org/10.1007/s10676-011-9279-1.
[18] M. Taddeo, Trust in technology: a distinctive and a problematic relation, Knowl. Technol. Pol. 23 (3–4) (2010) 283–286, https://doi.org/10.1007/s12130-010-9113-9.
[19] H. Nissenbaum, Will security enhance trust online, or supplant it? in: R. M. Kramer, K.S. Cook (Eds.), Trust and Distrust in Organizations: Dilemmas and Approaches Russell Sage Foundation, New York City, 2004, pp. 155–188.
[20] C. Lustig, B. Nardi, Algorithmic authority: the case of bitcoin, in: S. Misra, et al. (Eds.), 2015 48th Hawaii International Conference on System Sciences, IEEE, 2015, January, pp. 743–752.
[21] R. Botsman, Who Can You Trust? Penguin Business, Milton Keynes, 2018.
[22] K. Werbach, The Blockchain and the New Architecture of Trust, MIT Press, Cambridge MA, 2018.
[23] M. Hildebrandt, Law for Computer Scientists and Other Folk, Oxford University Press, Oxford, 2020.
[24] D. Gambetta, Can we trust trust? in: D. Gambetta (Ed.), Trust: Making and Breaking Cooperative Relations Blackwell, Oxford, 1998, pp. 213–238.
[25] A. Giddens, The Consequences of Modernity, Polity Press, Cambridge, 1990.
[26] J. Locke, Two Treatises of Government, Cambridge University Press, Cambridge, 1988.
[27] P. Pettit, The cunning of trust, Philos. Publ. Aff. 24 (3) (1995) 202–225.
[28] A. Baier, Trust and Antitrust, *Ethics* 96 (2) (1986) 231–260.
[29] G. Simmel, in: [1978]). The Philosophy of Money, third ed., Routledge, Abingdon, 2004.
[30] D.H. McKnight, N.L. Chervany, Trust and distrust definitions: one bite at a time, in: M.P. Singh (Ed.), Trust in Cyber-Societies: Integrating the Human and Artificial Perspectives, Springer, Berlin, Heidelberg, 2001, pp. 27–54.
[31] J. Weckert, Trust in cyberspace, in: R.J. Cavalier (Ed.), The Impact of the Internet on Our Moral Lives, University of New York Press, Albany, 2005, pp. 95–120.
[32] I.R. MacNeil, Exchange revisited: individual utility and social solidarity, Ethics 96 (3) (1986) 567–593.
[33] M. Taddeo, Modelling trust in artificial agents, A first step toward the analysis of e-trust, Minds Mach. 20 (2010) 243–257, https://doi.org/10.1007/s11023-010-9201-3.
[34] N. Luhmann, Trust and Power: Two Works, UMI Books, Ann Arbor, 1979.
[35] C. Castelfranchi, R. Falcone, Principles of trust for MAS: cognition anatomy, social importance, and quantification, in: Third International Conference on Multi-Agent Systems (ICMAS'98), IEEE Computer Society, Paris, 1998, pp. 72–79.
[36] R. Hardin, Do we want to trust in government? in: M. Warren (Ed.), Democracy and Trust Cambridge University Press, Cambridge, 1999, pp. 290–309.
[37] J. Mansbridge, Altruistic trust, in: M. Warren (Ed.), Democracy and Trust, Cambridge University Press, Cambridge, 1999, pp. 290–309.
[38] P. Dasgupta, Trust as a commodity, in: D. Gambetta (Ed.), Trust: Making and Breaking Cooperative Relations, Blackwell, Oxford, 1990, pp. 49–72.
[39] R.C. Ellickson, Order without Law, Harvard University Press, Cambridge MA, 1994.
[40] C. Mitchell (Ed.), *Trusted Computing*. Volume 6 of IEE Professional Applications of Computing, The Institution of Electrical Engineers, 2005.
[41] P.J. Nickel, Design for the value of trust, in: J. van den Hoeven, J. Vermaas, I. van de Poel (Eds.), Handbook of Ethics, Values, and Technological Design: Sources, Theory, Values and Application Domains, Springer, Berlin, Heidelberg, 2015, pp. 551–567.
[42] T. Pavlíčková, L. Nyre, J. Jurišić, What does it mean to trust the media? in: N. Carpentier, K.C. Schrøder, L. Hallet (Eds.), Audience Transformations: Shifting Audience Positions in Late Modernity Routledge, Abingdon, 2013, pp. 228–244.
[43] A.B. Seligman, Trust and scalability: on the limits of confidence and role expectations, Am. J. Econ. Sociol. 57 (4) (1998) 391–404.
[44] J.M. Barbalet, Confidence: time and emotion in the sociology of action, J. Theor. Soc. Behav. 23 (3) (1993) 229–247.
[45] K.H. Wolff (Ed.), 1906]). The Sociology of Georg Simmel, The Free Press, New York, 1950.
[46] A.B. Seligman, The Problem of Trust, Princeton University Press, Princeton NJ, 1997.

[47] C. Alès, Anger as a marker of love: the ethic of conviviality among the Yanomami, in: J. Overing, A. Passess (Eds.), The Anthropology of Love and Anger: the Aesthetics of Conviviality in Native Amazonia, Routledge, London and New York, 2000, pp. 133–151.
[48] J. Jalava, From norms to trust: the luhmannian connections between trust and system, Eur. J. Soc. Theor 6 (2) (2003) 173–190.
[49] C. Morgner, Trust and confidence: history, theory and socio-political implications, Hum. Stud. 36 (4) (2013) 509–532.
[50] J. Dunn, Trust and political agency, in: D. Gambetta (Ed.), Trust: Making and Breaking Cooperative Relations, Blackwell, Oxford, 1990, pp. 73–93.
[51] O. Lagenspetz, Legitimacy and trust, Phil. Invest. 15 (1) (1992) 1–21.
[52] T. Govier, Social Trust and Human Communities, McGill-Queen's Press, Montreal, 1997.
[53] R. Cotterrell, Law, Culture, and Society, Routledge, Abingdon, 2006.
[54] A. Antonopoulos, Bitcoin Security Model: Trust by Computation. O'Reilly Radar, 2014. February 20, available at: http://radar.oreilly.com/2014/02/bitcoin-security-model-trust-by-computation.html.
[55] K.D. Werbach, Trustless trust, in: Paper Presented at the TPRC Conference on Telecommunications, Information, and Communications Policy, Arlington, VA. September, 2016.
[56] T.K. Das, B.-S. Teng, The risk-based view of trust: a conceptual framework, J. Bus. Psychol. 19 (1) (2004) 85–116.
[57] H. Miller, C. Griffy-Brown, Developing a framework and methodology for assessing cyber risk for business leaders, Journal of Applied Business and Economics 20 (3) (2018) 34–50.
[58] D. Hume, Essays: Moral, Political, and Literary, vol. 1, Longmans, Green, and Company, London, 1907.
[59] R. Hardin, Trust and Trustworthiness, Russell Sage Foundation, New York, 2002.
[60] N. Szabo, Money, Blockchains, and Social Scalability, Unenumerated (Feb. 9), 2017 available at: http://unenumerated.blogspot.com/2017/02/money-blockchains-and-social-scalability.html.
[61] B. Maurer, T.C. Nelms, L. Swartz, "When perhaps the real problem is money itself!": the practical materiality of Bitcoin, Soc. Semiotic. 23 (2) (2013) 261–277.
[62] S. Saberi, M. Kouhizadeh, J. Sarkis, L. Shen, Blockchain technology and its relationships to sustainable supply chain management, Int. J. Prod. Res. 57 (7) (2019) 2117–2135.
[63] K. Korpela, J. Hallikas, T. Dahlberg, January). Digital supply chain transformation toward blockchain integration, in: Proceedings of the 50th Hawaii International Conference on System Sciences, 2017.
[64] H.R. Hasan, K. Salah, June). Blockchain-based solution for proof of delivery of physical assets, in: International Conference on Blockchain, Springer, Cham, 2018, pp. 139–152.
[65] A. Banafa, IoT and Blockchain Convergence: Benefits and Challenges, IEEE Internet of Things, 2017.
[66] A. Reyna, C. Martín, J. Chen, E. Soler, M. Díaz, On blockchain and its integration with IoT. Challenges and opportunities, Future Generat. Comput. Syst. 88 (2018) 173–190.
[67] A. Chaer, K. Salah, C. Lima, P.P. Ray, T. Sheltami, Blockchain for 5G: opportunities and challenges, in: 2019 IEEE Globecom Workshops (GC Wkshps, IEEE, 2019, December, pp. 1–6.
[68] Paul Snow, Brian Deery, Jack Lu, David Johnston, Peter Kirby, Andrew Yashchuk Sprague, Dustin Byington, Business Processes Secured by Immutable Audit Trails on the Blockchain, 2014.
[69] M. Benchoufi, R. Porcher, P. Ravaud, Blockchain protocols in clinical trials: transparency and traceability of consent, 2017, p. 6. F1000Research.
[70] M. Andoni, V. Robu, D. Flynn, S. Abram, D. Geach, D. Jenkins, A. Peacock, Blockchain technology in the energy sector: a systematic review of challenges and opportunities, Renew. Sustain. Energy Rev. 100 (2019) 143–174.
[71] L. Winner, Do artifacts have politics? Daedalus 109 (1) (1980) 121–136.
[72] A. Mallard, C. Méadel, F. Musiani, The paradoxes of distributed trust: peer-to-peer architecture and user confidence in Bitcoin, Journal of Peer Production (2014) 1–10, available at: https://hal-mines-paristech.archives-ouvertes.fr/hal-00985707.
[73] P. De Filippi, B. Loveluck, The invisible politics of bitcoin: governance crisis of a decentralized infrastructure, Internet Policy Review 5 (4) (2016).
[74] Q. DuPont, Experiments in algorithmic governance: a history and ethnography of "The DAO," a failed decentralized autonomous organization, in: Bitcoin and beyond (Open Access), Routledge, 2017, pp. 157–177.
[75] A. Jøsang, Trust and reputation systems, in: A. Aldini, R. Gorrieri (Eds.), Foundations of Security Analysis and Design IV, Springer, Berlin, Heidelberg, 2007, pp. 209–245.
[76] P. Craig, Formal and substantive conceptions of the rule of law: an analytical framework, in: R. Bellamy (Ed.), The Rule of Law and the Separation of Powers, Routledge, Abingdon, 2017, pp. 95–115.
[77] L. Fuller, The Morality of Law, Yale University Press, New Haven, Connecticut, 1964.
[78] J. Raz, The Authority of Law: Essays on Law and Morality, Oxford University Press, Oxford, 1977.
[79] J. Waldron, The rule of law and the importance of procedure, Nomos 50 (2011) 3–31.
[80] B.Z. Tamanaha, On the Rule of Law: History, Politics, Theory, Cambridge University Press, Cambridge, 2004.
[81] R. Cass, Property rights systems and the rule of law, in: E. Colombatto (Ed.), The Elgar Companion to the Economics of Property Rights, Edward Elgar, Oxford, 2014, pp. 131–163.
[82] T. Bingham, The Rule of Law, Allen Lane, London, 2010.
[83] R. Dworkin, Law's Empire, Harvard, Cambridge MA, 1986.
[84] S. Bradshaw, L. DeNardis, The politicization of the internet's domain name system: implications for internet security, universality, and freedom, New Media Soc. 20 (1) (2018) 332–350.
[85] D.L. Cogburn, Transnational Advocacy Networks in the Information Society: Partners or Pawns, Palgrave Macmillan, New York, 2017.
[86] M. Becker, When public principals give up control over private agents: the new independence of ICANN in internet governance, Regulation & Governance 13 (2019) 561–576.
[87] R.H. Weber, R.S. Gunnarson, A Constitutional Solution for Internet Governance, vol. 14, Columbia Science & Technology Law Review, 2012, pp. 1–72. Fall.
[88] V. Pickard, Neoliberal visions and revisions in global communications policy from NWICO to WSIS, J. Commun. Inq. 32 (2) (2007) 118–139.
[89] P. De Filippi, A. Wright, Blockchain and the Law: the Rule of Code, Harvard University Press, Cambridge MA, 2018.
[90] L. Lessig, Code: and Other Laws of Cyberspace, Basic Books, New York City, 1999.
[91] A. Wright, P. De Filippi, Decentralized Blockchain Technology and the Rise of Lex Cryptographia, March 10, 2015 available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664.
[92] P. De Filippi, S. Hassan, Blockchain technology as a regulatory technology: from code is law to law is code, Clin. Hemorheol. and Microcirc. 21 (12) (2018).
[93] Wessel Reijers, Iris Wuisman, Mannan Morshed, Filippi Primavera De, Now the code runs itself: On-chain and off-chain governance of blockchain technologies, Topoi (2018) 1–11.
[94] M. Kędziora, P. Kozłowski, M. Szczepanik, P. Jóźwiak, Analysis of blockchain selfish mining attacks, in: L. Borzemski, J. Świątek, Z. Wilimowska (Eds.), Information Systems Architecture and Technology: Proceedings of 40th Anniversary International Conference on Information Systems Architecture and Technology – ISAT 2019, vol. 1050, Springer, Cham, 2019, pp. 231–240. ISAT 2019. Advances in Intelligent Systems and Computing,.
[95] R. Unger, Law in Modern Society: toward a Criticism of Social Theory, The Free Press, New York City, 1977.
[96] M. Polanyi, The Logic of Liberty: Reflections and Rejoinders, Routledge, Abingdon, 1951.
[97] V. Ostrom, C.M. Tiebout, R. Warren, The organization of government in metropolitan areas: a theoretical inquiry, Am. Polit. Sci. Rev. 55 (4) (1961) 831–842.
[98] M. Finck, Blockchain Regulation and Governance in Europe, Cambridge University Press, Cambridge, 2018.
[99] K. Carlisle, R.L. Gruby, Polycentric systems of governance: a theoretical model for the commons, Pol. Stud. J. 47 (4) (2019) 927–952.
[100] M. Stephan, G. Marshall, M. McGinnis, An introduction to polycentricity and governance, in: A. Tiel, W.B. Blomquist, D.E. Garrick (Eds.), Governing Complexity: Analyzing and Applying Polycentricity, Cambridge University Press, Cambridge, 2019, pp. 21–44.
[101] A. Thiel, C. Moser, Foundational aspects of polycentric governance, in: A. Tiel, W. B. Blomquist, D.E. Garrick (Eds.), Governing Complexity: Analyzing and Applying Polycentricity, Cambridge University Press, Cambridge, 2019, pp. 65–90.
[102] V. Tarko, E. Schlager, M. Lutter, The faustian bargain: power sharing constitutions and the practice of polycentricity in governance, in: A. Tiel, W. B. Blomquist, D.E. Garrick (Eds.), Governing Complexity: Analyzing and Applying Polycentricity, Cambridge University Press, Cambridge, 2019, pp. 219–236.
[103] S. Rajagopalan, R.E. Wagner, Constitutional craftsmanship and the rule of law, Constitutional Political Economy 24 (2013) 295–309, https://doi.org/10.1007/s10602-013-9144-9.
[104] P.D. Aligicia, V. Tarko, Polycentricity: from Polanyi to Ostrom, and beyond. *Governance*, An International Journal of Policy, Administration, and Institutions 25 (2) (2012) 237–262.
[105] V. Ostrom, in: Polycentricity. Annual Meeting of the American Political Science Association, Washington D.C., September 5-9, 1972, pp. 1–44, available at: https://dlc.dlib.indiana.edu/dlc/bitstream/handle/10535/3763/vostr004.pdf.
[106] P. De Filippi, Blockchain technology and decentralized governance : the pitfalls of a trustless dream, in: F. Duarte (Ed.), Decentralized Thriving : Governance and Community on the Web 3.0, 2019 available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3524352.
[107] D. Tapscott, A. Tapscott, Blockchain Revolution: How the Technology behind Bitcoin Is Changing Money, Business, and the World, Penguin, London, 2016.
[108] P. De Filippi, G. McMullen, Governance of Blockchain Systems: Governance of and by the Infrastructure, COALA & Blockchain Research Institute Big Idea Whitepaper, 2019 available at: https://hal.archives-ouvertes.fr/hal-02046787/document.
[109] V. Ostrom, Polycentricity, in: M.D. McGinnis (Ed.), Polycentricity and Local Public Economies: Readings from the Workshop in Political Theory and Policy Analysis, University of Michigan Press, Ann Arbor, 1999, pp. 52–74.
[110] J.M. Balkin, Information fiduciaries and the first amendment, UC Davis Law Rev. 49 (4) (2016) 1183–1234.
[111] O. Williamson, Calculativeness, trust, and economic organization, J. Law Econ. 36 (1) (1993) 453–486.
[112] A. Narayanan, Analyzing the 2013 Bitcoin Fork: Centralized Decision-Making Saved the Day, Freedom to Tinker, 2015. July 28th, 2015.
[113] C.L. Reyes, Conceptualizing cryptolaw, Nebr. Law Rev. 96 (2) (2017) 384–445.
[114] K. Yeung, Regulation by blockchain: the emerging battle for supremacy between the code of law and code as law, Mod. Law Rev. 82 (2) (2019) 207–239.
[115] A. Walch, In code (rs) we trust: software developers as fiduciaries in public blockchains, in: I. Lianos, P. Hacker, S. Eich, G. Dimitropoulos (Eds.), Regulating

Blockchain: Techo-Social and Legal Challenges, Oxford University Press, Oxford, 2019, pp. 58–81.

Primavera De Filippi is a Researcher at the National Center of Scientific Research in Paris, and Faculty Associate at the Berkman-Klein Center for Internet & Society at Harvard. She is the founder and coordinator of the Internet Governance Forum's dynamic coalitions on Blockchain Technology (COALA). Her book, "Blockchain and the Law," was published in 2018 by Harvard University Press (co-authored with Aaron Wright).

Morshed Mannan is a PhD candidate at the Company Law Department of Leiden University. His research concerns cooperatives and digital technologies. He also lectures on comparative corporate law at a Bachelors and Masters level. Previously, Morshed worked as a Barrister in Bangladesh.

Wessel Reijers is a Max Weber Fellow, European University Institute, and a Visiting Researcher, WZB Berlin Social Science Center. He is an expert in ethics and philosophy of technology. His research focuses on investigating the impacts of emerging technologies on citizenship. His upcoming work discusses the Chinese Social Credit System, as well as a new, hermeneutic theory of technology."