How to govern the confidence machine?

Citation for published version:
de Filippi, P, Mannan, M & Reijers, W 2025, 'How to govern the confidence machine?', *Regulation and Governance*, pp. 1-16. https://doi.org/10.1111/rego.70017

Digital Object Identifier (DOI):
10.1111/rego.70017

Link:
Link to publication record in Edinburgh Research Explorer

Document Version:
Publisher's PDF, also known as Version of record

Published In:
Regulation and Governance

Regulation & Governance

Regulation & Governance

Check for updates

ORIGINAL ARTICLE OPEN ACCESS

How to Govern the Confidence Machine?

Primavera de Filippi[1] | Morshed Mannan[2] | Wessel Reijers[3]

[1]CNRS, Paris, France | [2]Edinburgh Law School, University of Edinburgh, Edinburgh, UK | [3]Institute for Media Sciences, Paderborn University, Germany

Correspondence: Wessel Reijers (wessel.reijers@uni-paderborn.de)

Received: 18 October 2022 | **Revised:** 24 February 2025 | **Accepted:** 7 March 2025

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

ABSTRACT

Emerging technologies pose many new challenges for regulation and governance on a global scale. With the advent of distributed communication networks like the Internet and decentralized ledger technologies like blockchain, new platforms emerged, disrupting existing power dynamics and bringing about new claims of sovereignty from the private sector. This special issue addresses a gap in the literature by focusing the discourse on the issue of *trust* and *confidence* in the digital realm. In particular, looking at the evolution of the web (from Web 1.0, to Web 2.0, and then Web 3), this article analyses how every iteration reflects a different way of dealing with the problem of *trust* online, resulting in a different regulation and governance landscape. Technology is often regarded as a new lever of regulation, attempting to resolve the problem of "trust" online, either through the introduction of a new trusted authority (Web 2.0) or through the introduction of technological guarantees that provide more assurance—or "confidence"—in the way interactions can be operationalized (Web 3). Yet, each of these technologies also introduce new risks and governance costs, ultimately shifting the problem of trust in a new direction rather than resolving it or removing the need for trust altogether. The main contribution of the articles in this special issue is providing a better understanding of the trust challenges faced and posed by emerging technologies and demonstrating how they affect institutional governance—in both theory and practice—with a view to help policymakers find appropriate answers to these challenges.

1 | Introduction

Governance and regulation in the 21st century are increasingly entangled with digital technologies. National governments and international organizations are grappling with the regulation of centralized online platforms and, more recently, with that of distributed digital technologies like blockchains. This distinction between centralized, decentralized, and distributed technologies—which Baran (1964) referred to as different "network models"—has a strong bearing on governance and regulation. *Centralized* digital networks have a single hub through which transactions flow from various network nodes, and *decentralized* digital networks have multiple such hubs, but *distributed* networks transact directly across many nodes in a peer-to-peer manner, avoiding any single hub that can act as a single point of failure. At least in theory, distributed networks can continue to function even if some nodes fail, while the compromise of network hubs in centralized and decentralized networks can adversely affect their functioning. The network model affects how these technologies are governed or regulated by outside forces (i.e., governance *of* the technology) as well as their own internal governance and regulatory dynamics (i.e., governance *by* the technology). Accordingly, online platforms controlled by centralized platform operators introduce different governance dynamics than decentralized networks, and in particular blockchain networks, that are governed in a more distributed manner.

The operators of centralized platforms are registered in at least one jurisdiction, which has an important function in regulating the operations of these online platforms (De Gregorio 2022). Yet, large online operators increasingly operate like private governments, implementing their own constitution, rules, and arbitration processes on their online platforms. Facebook's Oversight Board is one prominent example of a private company implementing its own private dispute resolution process for resolving content moderation disputes. Public and permissionless blockchain protocols, in contrast, are operated through a globally dispersed network of nodes which are not managed by a centralized operator but rather by "distributed consensus." Unlike private, permissioned blockchains, anyone can read, submit, or validate transactions in a public, permissionless blockchain, so long as they follow the rules of the protocol. While these blockchains are open to anyone participating, they cannot be controlled by any single person or entity. A public, permissionless blockchain protocol cannot be unilaterally modified or coerced by one network actor—even updates and forks of the protocol require the active consent and participation of all network nodes (De Filippi et al. 2022). This means that—at least in theory—everyone must abide by the rules enshrined in the blockchain protocol: any attempt to violate these rules will be immediately detected, and therefore rejected, by the other network participants (Zwitter and Hazenberg 2021). These properties significantly constrain the discretionary and coercive capacity of individual network actors, leading to many—largely unsubstantiated—claims that blockchains are "trustless" systems, as compared to corporate platforms that rely on "trusted" intermediaries (De Filippi et al. 2020). The trustlessness of these systems is, however, questionable, as certain network actors (e.g., protocol founders, developers, large mining or validator pools, crypto-currency exchanges, and other dominant players in the blockchain ecosystem) can leverage their influence (or soft power) to influence the behavior of the other actors in a blockchain network, thereby potentially affecting the operations of the network itself.

Perhaps due to the crypto-libertarian roots of blockchain technology (Golumbia 2016; DuPont 2018; Swartz 2018), the early literature on blockchain governance was focused mainly on core economic and game-theoretical aspects (Kroll et al. 2013; Böhme et al. 2015) of the technology. Most of the early literature also had a strong technologically deterministic flavor (Heilbroner 1967), focusing on the potential implications of blockchain technology on the law (Szabo 1997, Buterin 2014), economy (Swan 2015, Vigna and Casey 2016), politics (Atzori 2017), and society more generally (Tapscott and Tapscott 2016), with little attention paid to the broader societal context in which the technology was introduced and the governance implications that the technology could have, both at the micro and macro levels.

As the editors of this special issue, we have been exploring in our research the implications of blockchain technology, looking at both their benefits and drawbacks, with a view to analyzing the potential opportunities and challenges of these new technologies, and how they can inform our understanding of regulation and governance. In the past few years, our work has been focusing mostly on the regulatory issues raised and faced by blockchain technology (De Filippi 2014; De Filippi and Wright 2018; De Filippi et al. 2024a), with particular regard to the limitations of governance systems for the most part grounded on code-based rules (De Filippi et al. 2024a; Reijers et al. 2021). We have also investigated the role of blockchain technology as a regulatory technology (De Filippi and Hassan 2018) and the ways in which it can also be used to, at least partially, escape from existing regulatory frameworks (De Filippi et al. 2022). In this context, we drew analogies to the "*rule of law*" and the authoritarian "*rule by law*," claiming that centralized platforms are usually "*ruled by code*," while blockchain protocols are subject to the "*rule of code*" (De Filippi et al. 2022). In this research, we find instances in which the *rule of code* conflicts with the *rule of law*, with increasing attempts by states to rein in the rule of code using various legislative and regulatory strategies. Finally, we have looked into the various ways in which blockchain technologies can be leveraged for the creation of new organizational structures with a more community-based governance system (De Filippi 2017), with specific focus on the use of blockchain technology in the context of platform cooperatives (Mannan and Pek 2024; Mannan 2018).

The aim of this special issue is to provide an interdisciplinary forum to discuss the latest developments in the realm of regulation and governance that have been brought about by blockchain technologies, as well as their implications for trust and confidence. We invited both theoretical and practical contributions, with a view to helping regulators and policy-makers address the challenges and opportunities raised by these emerging technologies.

This framework article illustrates how the multi-faceted concepts of trust and confidence are crucial for analyzing the regulatory and governance challenges created by these different network models. Drawing upon an extensive, transdisciplinary body of literature on trust, this article articulates the contributions to this special issue to enrich our understanding of the challenges related to the governance *of* and *by* digital technologies and how building trust or confidence can aid in mitigating these challenges. This is a novel theoretical contribution for two main reasons.

First, scholars have long been exploring what is the right lens to investigate the quickly changing landscape of digital governance, but have paid relatively limited attention to the interplay between governance *of* digital technologies and governance *by* digital technologies. Some have argued that emerging technologies urge us to consider a new form of jurisprudence, or "*digisprudence*" (Diver 2021), or a new form of "*digital constitutionalism*" (Suzor 2018; Celeste 2019) that would draw on constitutional principles and norms to place checks and balances on the governance of digital platforms. Others believe that the fundamental principles of liberal democracies, such as the rule of law, should govern and constrain digital platforms (Hildebrandt 2018; Bradford 2023). Scholars have also questioned the emerging power dynamics stemming from the emergence of "*digital sovereigns*" (Pasquale 2018) or "*cloud empires*" (Lehdonvirta 2022) that confront us with a new form of "*digital feudalism*" (Mazzucato 2019) or "*techno feudalism*" (Varoufakis 2023). Similar concerns have been expressed with regard to blockchain systems and the emergence of private powers acting as *functional sovereigns* during certain states of exception (Reijers et al. 2021). These bodies of literature often tackle either the question of governance *by* technology (i.e., institutional design questions, such as how can we design sociotechnical systems to support the rule of law?) or governance *of* the technology (i.e., the question of agency in these systems, such as how to check the decision-making powers of new ostensible "feudal lords" like Elon Musk and their digital platforms?). The interplay between governance *of* and *by* digital technologies has yet to be adequately investigated in the literature. Considering these topics jointly is helpful in understanding the extent to which these two modes of governance each constrain and potentially enhance the other. In other words, how does the governance *by* digital technologies influence the governance *of* these technologies, and—vice versa—how does the governance *of* digital technologies influence the governance *by* these technologies?

Second, this special issue seeks to fill this gap by focusing on the analytic lens of *trust* and *confidence*. The concept of trust has already been heavily discussed in the fields of sociology (Luhmann 2000), political philosophy (Pettit 1995), and rational choice theory (Hardin 2002). Some scholars have defined trust as a mental state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behavior of another (Giddens 1999). Others have looked at trust as a sociological concept and have argued that trust is essential for the functioning of any society because it allows humans to interact with each other and to cooperate with one another without having to constantly monitor and police each other (Gambetta 2000; Costa 2007). Still others have looked at trust from a more economic perspective, showing that trust is an essential component of any market economy because it allows people to trade with one another on a recurrent basis even if they do not know each other (Lorenz 1999).

Trust is an important phenomenon that impacts the way people behave and coordinate themselves in society. While on a personal level, trust essentially relates to a person's individual disposition towards vulnerability and risk, trust is also a structural or systemic concept related to shared expectations about broader societal systems or institutions. It is in this latter sense that we "trust" our government. Sometimes, expectations are so enshrined in our understanding of the world that we no longer perceive the risk associated with a particular course of action. This is what led the sociologist Niklas Luhmann to draw a distinction between the phenomena of *trust* (*vertrauen*) and *confidence* (*sicherheit*).

In this framework article, we claim that the interplay between trust and confidence offers a fruitful lens through which to analyze the regulation and governance *of* and *by* digital technologies. Drawing from the historical reasons that motivated the development of Web 1.0 and 2.0 technologies, we focus in particular on blockchain technologies—regarded as the catalysts of Web 3—because these technologies raise novel issues with regard to trust and confidence, while also providing new ways for governance and regulation to respond to those issues. In the first section of this article, we demonstrate the benefit of using trust and confidence as an analytic lens to look at the various iterations of the Web and their respective implications for regulation and governance. In the second section, we turn to what we call the "confidence machine"—that is, blockchain technology—and the new challenges it raises with regard to regulation and governance. In the third section, we describe these challenges in more detail and we delineate potential regulatory and governance responses. We conclude, in the fourth section, with an overview of the articles in this special issue, according to three broad themes: (1) the impact of emerging technologies on trust and confidence, (2) trust and governance in the context of blockchain systems, and (3) emerging technologies for trust and global governance.

2 | Trust, Confidence and Internet Governance

In this section, we rely on trust and confidence as an analytic lens to investigate the operations of the multiple iterations of the Web throughout the years and their influence on regulation and governance. While there is no single established definition of "governance" (Kjaer 2023) or "regulation" (Levi-Faur 2011) in the academic literature, for the purposes of this article, we refer to governance as the overall processes and structures by which organizations or communities are directed, controlled, and managed—both *endogenously* and *exogenously*. This comprises the various mechanisms, processes, and relationships through which deliberation is made, power is assigned, decisions are taken, and ultimately put into practice. While we take regulation to refer specifically to the creation and enforcement of formal rules, laws, or directives by an external authority (such as a government or regulatory body) to control specific behaviors or activities (Mitnick 1975; Laffont 2005; Bernstein 2016), we regard governance as a broader concept that also encompasses the informal practices, cultural norms, and ethical considerations adopted within organizations or communities to facilitate the processes of decision-making, management, and accountability (Kaler 2002; Christiansen and Piattoni 2003; Fukuyama 2013).

2.1 | Understanding Trust and Confidence

Trust and *confidence* represent distinct yet complementary mechanisms through which humans navigate social and institutional relationships. Depending on the contingencies, they may constitute the input (i.e., a precondition) and the output (i.e., a consequence of) regulation and governance. Before delving into the implications of trust and confidence on Internet governance and regulation, we provide a preliminary definition of these two important terms. In particular, although there is still some degree of discussion and disagreement among scholars about the precise meaning of these terms (see e.g., Gambetta 2000; Hardin 2002), we rely in this section on Luhmann's conceptualization to elucidate the distinction between *trust* and *confidence* (Luhmann 2000).

Trust, according to Luhmann (2000), has to do with the conscious act of putting oneself in a situation of vulnerability with respect to the behavior of another. As such, trust is fundamentally interpersonal and relational: it is a relationship between two parties—the trustor and the trustee—whereby the former voluntarily decides to rely on the behavior of the latter, under the belief that the latter will behave in line with the expectations of the former (Gambetta 2000). By trusting another agent, however, the trustor makes him or herself vulnerable for betrayal. For instance, when we entrust our children to a babysitter, we make a conscious choice to accept vulnerability based on our assessment of that person's character and capabilities. Similarly, when we share sensitive information with a friend, we trust them not to misuse it, knowing they could potentially betray that trust. Hence, central to the notion of trust is the feeling of risk or uncertainty. Risk refers to situations where the probabilities of different outcomes are known or can be reasonably estimated (i.e., known unknowns). Uncertainty, on the other hand, refers to situations where the probabilities of outcomes are unknown or cannot be accurately estimated. It is characterized by a lack of information, unpredictability, and the presence of unknown factors (i.e., unknown unknowns). As described by Giddens (1990) "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" (p. 89). Thus, all things being equal, the decision to rely on a third party in a situation of risk or uncertainty will depend both on the amount of trust that can be conferred to the third party, and the possible consequences that a breach of trust might entail. One may choose to trust a third party even if fully aware that betrayal is possible, because trust makes it possible to offload some of the cognitive load that would have to be incurred otherwise on all kinds of "what if" questions. John Locke (1988) regarded the development of trust as a fundamental requirement for humans to leave a state of nature and form more advanced societies, where crucial tasks can be delegated to (trusted) third-parties. Naturally, because trust is a conscious choice by the trustor, should the trustee breach the trust, the trustor will assume responsibility and ultimately take the blame for choosing to confer trust to a non-trustworthy party. In sum, the key characteristics of trust can be synthesized as follows:

1. Trust is interpersonal or relationship-based.
2. It involves a conscious choice to accept vulnerability.
3. It operates in the presence of risk or uncertainty.
4. It can be betrayed, leading to personal disappointment and revised expectations.

Confidence, in contrast, operates through our assessment of systems, processes, and patterns, rather than through interpersonal relationships (Luhmann 2000). Different from trust, confidence is not associated with a feeling of risk or uncertainty, but rather with a feeling of certainty and assurance resulting from individual experience and shared expectations. Certainty refers to a state of conviction that something is true beyond any reasonable doubt, leaving no room for ambiguity. Assurance recognizes the potential for some degree of uncertainty but with a sufficiently low probability as to be considered reasonable and acceptable. When we have confidence in a system or process, we rely on it based on observed patterns of behavior or institutional guarantees, rather than personal relationships. For example, when we use an ATM, we have confidence in the banking system to accurately process our transactions—not because we trust any individual banker, but because we rely on the systematic processes, technological infrastructure, and institutional guarantees in place. Generally, in a situation of confidence, people do not even perceive the risk that their expectations might remain unfulfilled. As a result, when acting upon confidence, people will 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, largely unforeseeable events (Giddens 1990). In sum, the key characteristics of confidence can be synthesized as follows:

1. Confidence operates through assessment of processes rather than relationships.
2. It is based on systematic patterns and institutional arrangements.
3. It is generally associated with a strong sense of assurance and low uncertainty.
4. Its failure leads to system critique rather than a feeling of personal betrayal.

This demonstrates how trust and confidence are not simply points on a certainty –uncertainty continuum, but rather distinct mechanisms that can operate independently or in concert. While both contribute to reducing the cognitive load of decision-making, they do so through different channels: trust through interpersonal relationships and voluntary vulnerability, and confidence through systematic processes and institutional arrangements.

Most social interactions typically require a combination of both confidence and trust. For instance, when engaging a lawyer, clients rely on both confidence in the legal system's professional standards and oversight mechanisms, and trust in their specific lawyer's commitment to representing their interests. These mechanisms complement each other but serve distinct functions. Likewise, in the context of e-commerce, when purchasing from an established online marketplace, consumers typically exhibit both trust and confidence. They have confidence in the platform's systems (payment processing, delivery tracking, return policies) while also trusting specific sellers based on reviews and past performance. A failure in the platform's systems would undermine confidence, while a dishonest seller would breach trust.

Albeit semantically distinct, the two concepts are inherently related to one another. On the one hand, trust and confidence can feed into each other, leading to a direct correlation among the two: trust can contribute to achieving more confidence, and confidence, in turn, can be an important driving factor for trust. For example, in the context of healthcare, patients typically have confidence in the medical system's processes (standardized procedures, licensing requirements, quality controls) while simultaneously developing trust relationships with individual healthcare providers. The system's confidence-building mechanisms actually facilitate the development of interpersonal trust. Conversely, it is often the case that confidence in a system may result from there being trust in a higher-level actor in the system. For instance, I am confident that I will not get robbed when walking down the street because I trust my government to provide a functioning police force to dissuade criminals from attacking me. The existence of this confidence, in turn, enables me to trust strangers—an important and necessary activity in modern society.

On the other hand, trust and confidence can be regarded as two distinct forces that have the ability to complement and sometimes even supplement each other. This means that trust and confidence may have an inverse relation, whereby the insufficiency of one will be mitigated by increasing the other: in a low-trust environment, more confidence is required, and vice versa, in a low-confidence environment, higher levels of trust are required to engage in social interactions. For example, in places where confidence in governments is low, specific mechanisms need to be put into play to support social and economic activities. These include both confidence-enhancing solutions, such as third-party organizations responsible for ensuring the safety of citizens (e.g., private police forces) and trust-enhancing mechanisms, including stronger social bonds and peer-to-peer pressures designed to bring higher levels of trust amongst individuals. The reason why some societies might favor confidence over trust, or vice versa, ultimately depends on multiple factors, whose delineation is beyond the scope of this article.

While both trust and confidence are valuable tools to support human interaction, one challenge with trust is that it does not scale well: it is viable in a small communal setting, but not amongst strangers who might be tempted to betray each other. Regulation can enhance both trust and confidence (in the way people or institutions behave) through different mechanisms. It can increase confidence by standardizing processes and creating predictable outcomes, while simultaneously fostering trust by providing frameworks for accountability and recourse in cases of betrayal. In particular, the standardization of education, evaluation, and accreditation makes it easier to predict the skills and capacities of individuals, allowing citizens to be more confident in certain systems and processes, while also making it easier for people to engage in trusting relationships. Understanding these distinct but complementary roles of trust and confidence is crucial for analyzing how different regulatory and governance mechanisms operate in various contexts, from traditional institutions to emerging technological systems.

2.2 | The Role of Technology for Confidence and Trust

The relationship between technology, confidence, and trust remains largely ambiguous. On the one hand, technology plays a crucial role in the production of confidence to the extent that it is used to create standardized processes with a higher degree of automation, and thus predictability. This has been the case with the invention of the printing press (enabling more standardized administrative processes), the development of factories and assembly lines (enabling predictable labor patterns and more standardized outputs), and, more recently, with the rise of big data and machine learning to guide and inform policy-making, as with data-driven climate models (enabling more clarity and predictability in terms of policy outcomes). On the other hand, even though technology can produce confidence through standardization and predictability, it also has the capacity to challenge traditional accountability processes, creating greater risk and uncertainty. For instance, while big data and machine learning can promote predictability in governance, when improperly managed or understood, these technologies can equally contribute to undermining trust and confidence, raising questions about privacy and security, along with a new plethora of ethical concerns related to, for example, algorithmic biases and lack of interpretability.

While we acknowledge the importance of investigating the dual role of digital technologies—recognizing both their constructive and potentially detrimental impact on trust and confidence—we focus here on the use of technology as a "regulatory technology" that is specifically geared towards increasing confidence in a technologically mediated system, with a view to making it easier for the users interacting on that system to establish trusted (or trustless) relationships.

The role of technology as a regulatory tool has become particularly apparent with the advent of digital technologies. Indeed, back in the early Internet days, Lawrence Lessig came up with the (often misunderstood) expression "code is law" (Lessig 1999)—underscoring a fundamental shift in how regulations are implemented and enforced in the digital realm. Lessig claimed that digital technologies, through their code-based rules, have the capacity to shape and govern behaviors in ways similar to legal frameworks. Yet, whether or not this creates more confidence, ultimately depends on the trust that users place in the operators of these digital systems. Users must have confidence that the code, which essentially acts as the rulebook, is not manipulated to serve the interests of specific third parties, at the detriment of the users. Hence, once again, we observe that confidence in a technological platform is the result of trust in the entities operating that platform. Once confidence is established, users of the platform will have the opportunity to interact with one another without necessarily having to trust each other—provided that they trust the platform operator to act as a trusted intermediary. The conceptualization of trust and confidence across this special issue's contributions reveals a series of commonalities and tensions in how these concepts operate in technological contexts, and in particular the blockchain context. Bodo and De Filippi (2024), for instance, illustrate how Decentralized Finance (DeFi) systems attempt to establish confidence through technological mechanisms while still requiring traditional trust-based structures for widespread adoption. They suggest that purely confidence-based systems—even with strong technological guarantees—may not fully substitute for trust-based relationships in financial services. This tension is further elaborated in Bayern (2024), which identifies specific costs associated with over-reliance on algorithmic confidence (what he calls "formalism costs"), claiming that pure confidence-based systems may be both expensive and potentially unreliable, requiring complementary trust mechanisms through organizational law. Alston (2024) adds another dimension by distinguishing between institutions (building confidence through ex-ante rules) and norms (facilitating trust via community-driven adaptability), to explain why blockchain systems, despite their strong institutional confidence guarantees, still require trust-based social norms to handle unforeseen circumstances. Davidson and Potts (2024) reinforce this view by arguing that blockchain governance should draw from corporate rather than political models precisely because it operates in a context of voluntary cooperation where trust relationships remain crucial. Backer (2024) concept of "trust platforms" offers a bridge between these perspectives, showing how digital technologies transform trust from purely interpersonal relationships into quantifiable metrics mediated by platforms. This transformation suggests that modern systems often blend trust and confidence mechanisms, with platforms serving as intermediaries that translate trust relationships into confidence metrics while simultaneously requiring trust in their own operations.

These varied perspectives from the special issue's contributors reinforce our argument that trust and confidence operate as distinct but complementary mechanisms rather than points on a certainty –uncertainty continuum. They demonstrate how technological systems often attempt to maximize confidence through algorithmic guarantees while still requiring various forms of trust relationships to function effectively. This interplay becomes particularly evident in blockchain systems, where attempts to create "trustless" confidence-based systems ultimately reveal the persistent necessity of trust relationships at various levels of system operation and governance.

We present below an overview of how, since the advent of the Internet and digital technologies, we have witnessed a significant shift in power dynamics, fueled by a process of disintermediation and reintermediation, which significantly affected the role of trust and confidence in the governance and operation of online platforms. This process culminated in the advent of blockchain technology, touted as a disintermediation technology that would entirely eliminate the need for trusted authorities and enable peer-to-peer interactions in a fully trustless system. Yet, as we will demonstrate, the promises do not always match reality, and blockchain technology—just like any other technology—can be both supportive and detrimental to confidence and trust, depending on the uses that are made of it.

2.3 | The Role of Trust and Confidence in Internet Governance

While the core technologies underpinning the Internet (i.e., the TCP/IP protocol) were developed in a military context (ARPANET), the early ideological promises of digital technologies can be traced back to the 60s counterculture that thrived in Silicon Valley. Figures like Steward Brand and other early Internet visionaries considered that open computer networks could foster new opportunities for long-distance communication and collaboration (Turner 2006). According to them, the Internet—as a new space enabling people to connect and interact without the constraints of geographical boundaries—would support the emergence of a collective intelligence that would mimic the underpinning of a digital commune—in line with Marshall McLuhan's vision of a "global village" (McLuhan 1957). Yet, this digital commune cannot rely merely on trust because it consists of strangers scattered around the world who have no reason to trust each other.

This digital village first became mainstream with the emergence and popularization of the Web in the early 1990s. Yet, the early Web was a space where strangers all over the world could publish content online without any checks and balances. As a result, frauds, scams, illicit content, misinformation, and hate speech started to permeate this new digital realm. This showed that the internet was not a digital commune populated with like-minded individuals who could trust each other, but rather a place full of people with different intentions, some of which were malicious. The uncertainty created by misinformation and dubious and malicious practices eroded confidence and trust in online interactions, hindering the internet's potential to be a reliable space for communication, collaboration, and commerce.

This dilemma was addressed with the enactment of new laws aimed at regulating many aspects of this new digital realm. Yet, because of the decentralized and transnational nature of many Internet services at the time, it was often challenging for regulators to effectively enforce these laws. As proclaimed by early Internet advocates, the internet was regarded as a new digital space that governments simply did not have the right, nor the capacity to regulate—as John Perry Barlow famously proclaimed in his "Declaration of Independence of Cyberspace" (Barlow 1996).

The trust problem that plagued the first iteration of the web was resolved, albeit partially, with the advent of a new generation of the web. This new web was born out of the ashes of the dot-com bubble, which saw the collapse of many companies that had been built on the back of the first generation of internet platforms (Rushkoff 2022). It was designed to build a more trustworthy internet, where users could be *confident* (i.e., assured) that the information they were sharing was accurate and reliable because they *trusted* the online operators to verify and moderate the content uploaded onto their platforms. Social media platforms such as Facebook and Twitter (now X) allowed users to connect with each other and share information in real time, while trusting that any abuse of the platform would be sanctioned by the platform operators. Over the years, the large platforms started to evolve into a set of "walled gardens" (Mazzucato 2019) making things secure and predictable within their own online space. This is achieved, amongst other things, through instruments like ratings and reputation mechanisms (e.g., on Uber or Airbnb) (Bodo 2021).

While not necessarily intended as such, these walled gardens can be said to have, at least to an extent, resolved the trust problem that permeated the early Internet. This was achieved through the introduction of trusted intermediaries that would be in charge of policing their own (centralized) online platform. However, this new version of the Web eventually started to show its limitations, as it became apparent that the solution it provided to the lack of trust among strangers actually introduced a new problem regarding the extent to which these new trusted intermediaries could, indeed, be trusted.

Part of the problem relates to the emergence of "surveillance capitalism" (Zuboff 2019): a new logic of data extraction that turns user data into a resource for profiling, targeted advertising, and behavioral manipulation. Another part of the problem relates to colonialist hubris, following, for instance, from the use of Facebook in the unfolding of genocidal events in Myanmar due to the lack of content moderators understanding the local language (Whitten-Woodring et al. 2020). Problems also arose from third parties infecting these online walled gardens from within, as happened with the Cambridge Analytica scandal (Wylie 2019). More importantly, the erosion of confidence in the everyday operations of the dominant platforms came about as soon as it became clear that the actors operating these platforms cannot be trusted, since they are mostly interested in the maximization of profits rather than in serving the interests of their user base (Mannan and Schneider 2021). Indeed, ultimately, the operations of platforms are decided by powerful individuals, like Mark Zuckerberg, who often exercise discretionary power over the platforms they operate.

With major platforms like Google and Facebook accumulating vast amounts of user data, concerns about privacy and data security came to the forefront. In response to this erosion of trust and confidence, jurisdictions around the world introduced stringent data protection laws, the most notable being the General Data Protection Regulation (GDPR) in the European Union. These regulations empowered national data protection agencies with significant authority over online operators, enabling them to impose substantial fines on non-compliant corporations. This forced major platforms to reassess their data handling practices, leading to greater transparency, enhanced user consent mechanisms, and improved cybersecurity measures. Yet, despite the increased confidence that these regulations brought, once the genie was out of the bottle, it became difficult to put it back in. Once it became clear that centralized online platforms are governed by the whims of their online operators, whose commercial interests are often misaligned with the interests of end users, it became difficult for users to fully trust these intermediary operators.

It is in this context that Web 3 makes its appearance, attempting to overcome the shortcomings of its predecessors in a variety of areas. The Web 3 has to be distinguished from "Web 3.0" originally coined by Sir Tim Berners-Lee (the inventor of the World Wide Web) to describe the concept of the *semantic web*, an evolution of the internet where bits of information are semantically linked to each other in a way that is also comprehensible to machines, facilitating more advanced and contextually relevant user experiences. However, as the semantic web failed to take on, the blockchain community subsequently used the term Web 3 to describe a new generation of web applications that leverage blockchain technology as their backend infrastructure. These applications embody the decentralized and tamper-proof nature of blockchain technology, paving the way for a more secure, transparent, and user-centric internet experience.

Web 3—the primary focus of this special issue—distinguishes itself from the previous iterations of the web in that it presents itself as a "confidence machine" (De Filippi et al. 2020). While the earlier implementations of the web were subjected to the "*rule by men*"—be it a bunch of all-powerful admins or feudal lords (Schneider 2022)—Web 3 relies on blockchain-based technology that, at least in theory, is not subject to the whims of any single entity. Just like in the early days of the Internet, many of the Web 3 visionaries, such as Satoshi Nakamoto and Vitalik Buterin, saw the emergence of blockchain technology as an opportunity to succeed where the Internet had failed, creating a new decentralized infrastructure that does not depend on any centralized authority to operate. As such, Web 3 is regarded by some as a confidence-building machine to the extent that it relies on a peer-to-peer network technology that no human participant can unilaterally manipulate or control. Yet, even if blockchain technology might indeed qualify as a confidence machine, as we will show in the following section, the confidence in the operations of a Web 3 platform ultimately depends on the power dynamics at play in the underlying blockchain network (Rennie et al. 2022), which essentially reintroduces the issue of trust (De Filippi et al. 2020). Moreover, even if the underlying blockchain network is appropriately governed, the Web 3 applications that interface with it constitute the weakest link insofar as they might be flawed and attacked by malicious users, or simply intentionally built to deceive. Trust, therefore, still has an important role to play also in these allegedly "trustless" systems.

This exposition of the dynamic between trust and confidence in different iterations of the web is relevant for regulation and governance for at least two reasons. First, *exogenously*, the failure to establish trust and confidence online has led to important regulatory interventions. For the early Internet, the newfound possibility of freely sharing information online has led to draconian regulations against copyright infringement and online piracy. Later, the potential misuse of power from large platform operators has led to stringent privacy regulation (notably the General Data Protection Regulation in the EU) and far-reaching debates concerning antitrust legislation targeting these platforms. For Web 3, problems of criminality, fraud, and hacks have harmed confidence in blockchain-based systems and have led governments around the world to initiate proposals to regulate this nascent industry. Second, *endogenously*, emerging digital technologies have unlocked new governance dynamics that have led to innovative responses to the erosion of online confidence and trust. For the early Internet, the need to ensure the development and maintenance of many Internet protocols led to the creation of institutional bodies like the IETF, the W3C, or the ICANN, whose legitimacy ultimately depends on the public trust they manage to elicit (Jongen and Scholte 2021). In the platform era, failures of online operators to protect their platforms against abuses, as illustrated by the rampant spread of fake news and misinformation, led to the creation of new governance bodies endogenous to these platforms, like the Facebook Content Oversight Board (Klonick 2020). Finally, for Web 3, the legal and regulatory challenges it has raised have instigated significant experimentation with governance and self-regulatory practices, which are featured prominently in this special issue.

3 | Blockchain Technology and the Confidence Machine

In this third section, we present the role of blockchain technology as a "confidence machine" explaining its relevance for discussing contemporary challenges to trust and governance.

Blockchain technology emerged in the late 2000's with the advent of Bitcoin, a decentralized cryptocurrency that can be traded without the need for any financial intermediary. Since then, the potential of blockchain technology has been leveraged by a variety of different actors and in multiple domains, including decentralized financial applications (DeFi) (e.g., Uniswap, Compound, MakerDAO), insurance (NexusMutual), remittances (e.g., BitPesa, Wyre, Wirex), recordkeeping (e.g., Delaware's blockchain-based recordkeeping of corporate stocks), digital identity (e.g., Worldcoin), and organizational structures (e.g., dOrg). These new blockchain-based organizational structures are being used for a wide range of purposes, including governing and supporting political movements (e.g., AssangeDAO funding legal support for Julian Assange), humanitarian efforts (e.g., UkraineDAO collecting funds to support Ukrainian resistance in the war against Russia), and climate change initiatives (e.g., KlimaDAO seeking to make global carbon offset markets more transparent and efficient). All these applications and services rely on a blockchain in order to facilitate the execution of financial or non-financial transactions in a peer-to-peer and distributed manner. While the concept and operations of a blockchain are fairly complex, in practical terms, it can be described as a distributed ledger, which records transactions in a shared and commonly managed database that is highly resilient (i.e., difficult to shut down) and tamper resistant (i.e., difficult to corrupt).

Drawing from the "code is law" body of literature, blockchain technology is described by many of its proponents as the ultimate solution to the problem of trust, using code-based protocols and technologically-enforced rules to mediate interactions amongst people who do not know, and therefore do not trust each other (De Filippi et al. 2024a). This is what led early blockchain advocates to define this technology as a "trustless" technology—that is, one that no longer requires trust.

There are a number of reasons why blockchain technology is often described as a trustless technology. First, the code-based protocols that are used to mediate interactions among people who do not know each other can be seen as a way of eliminating the need for a trusted intermediary. Second, the fact that these protocols are enforced by technology, rather than by humans, means that they are less likely to be corrupted or manipulated with malicious intent. And third, the transparency requirements in many blockchain systems mean that users must verify and validate all the transactions that are taking place on the network, which makes it difficult for anyone to cheat or act in bad faith.

Yet, we argue that the qualification of blockchain technology as a trustless system is not only misleading—because no system can be perfectly trustless—but also problematic to the extent that it is shifting the focus away from the real contribution of blockchain technology. The point is not to eliminate trust, but rather to increase the level of confidence in the way the system works. Blockchain technology is, therefore, more appropriately described as a "confidence machine"—that is, a system that is designed to instill confidence in its users.

The concept of a "confidence machine" was first introduced in a previous article by the same authors (De Filippi et al. 2020) describing the impact of blockchain technology on confidence and trust. In this article, we argued that blockchain technology can be used to create systems that are more transparent and predictable through the combination of technological elements, namely: *cryptographic primitives, distributed consensus, and deterministic computation*. With regard to the former, blockchain technology relies on public-private key cryptography in order to ensure that transactions are valid, and that only those who hold the private key can execute transactions on behalf of the wallets associated with the corresponding public key address. A blockchain also relies on one-way (hashing) functions in order to guarantee the integrity of all data recorded on the blockchain, as well as to maintain the chronology of each block within the larger chain of blocks. Distributed consensus also contributes to greater confidence in the system. Indeed, a blockchain is a distributed database that is maintained by a network of computers, each of which has a copy of the entire database. When a new transaction is added to the database, all computers in the network must reach consensus on the validity of the transaction before it can be added to the blockchain. This consensus-based approach to transaction validation makes it very difficult for anyone to insert invalid transactions on a blockchain. Finally, because all software code deployed on a blockchain is executed in a distributed manner by all network participants, it comes with a guarantee of execution which is such as to ensure that no one has the ability to influence or terminate the execution of such code. One can therefore be confident that the code will always execute precisely as planned, with no possibility of third-party intervention or interference (Figure 1).

These elements work together to create a seemingly "trustless" environment that can facilitate interactions amongst people that do not know, and therefore do not trust each other. Yet, this allegedly trustless system only works insofar as we can *trust* the underlying governance structure of these systems. Indeed, if some actors were to collude to take control over more than 51% of the network, the confidence-building properties of blockchain technology would no longer be guaranteed. Confidence in a blockchain-based system is, therefore, dependent on at least some degree of trust in another system—namely the underlying network of actors (i.e., miners and validators) operating the network. As one of the articles of this special issue argues, "the human components of these systems, and the vulnerabilities they introduce, cannot be easily engineered away" (Bodo and De Filippi 2024).

The qualification of blockchain technology as a confidence machine has significant implications for regulation and governance. With regard to governance, the characteristics of a blockchain network—in terms of transparency, disintermediation, and automation—make it possible to deploy so-called decentralized applications (DApps) that are executed in a distributed manner by

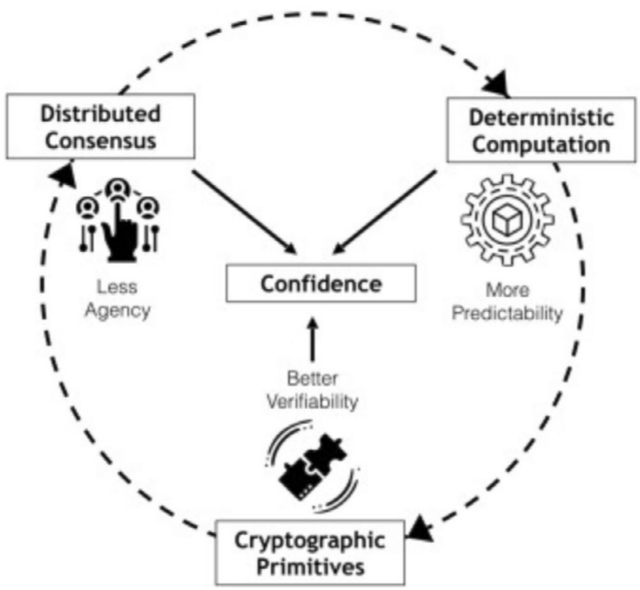

FIGURE 1 | Schematic representation of the blockchain as a confidence machine—reproduced from De Filippi et al. (2020).

all the network's participants. To the extent that they cannot be controlled, manipulated or even terminated by any single actor, these decentralized applications are often regarded as autonomous systems, that is, systems that operate independently of any third party or trusted authority. This eventually spurred the development of so-called Distributed Autonomous Organizations (DAOs), that is, blockchain-based applications that enable the coordination of multiple people towards a common purpose, whose interactions are mediated via technologically-defined rules that do not require any enforcement authority because they are automatically enforced by the underlying blockchain network. The advent of DAOs brought significant developments in the blockchain space, as this novel structure has been used to govern protocols and a host of other collective initiatives. While DAOs are still far from having acquired mainstream adoption, they have gained substantial popularity in recent years, as they have been used in the field of Decentralized Finance (DeFi) to govern significant blockchain protocols such as Uniswap (for the decentralized exchange of cryptocurrency and blockchain tokens), MakerDAO (for the creation and management of "stablecoins" that are pegged to the US Dollar) or Synthetix Protocol DAO (for earning passive income from existing cryptocurrencies). DAOs are increasingly being adopted in fields other than finance as well. The aforementioned KlimaDAO, designed to build a sustainable global carbon offset market, can already benefit from having more than 100,000 members and participants, whereas Uniswap has a treasury worth US$ 2.6 billion as of September 2024. These DAOs have a significant real-world impact, with the litigation funding support of AssangeDAO raising over 50 million USD worth of ETH in February 2022 and being lauded for helping ensure Wikileaks founder, Julian Assange's release from custody (Craig 2024).

In terms of regulation, the decentralized nature of blockchain technology, as well as the pseudonymity of the parties involved in transactions, is perceived by many as a source of legal uncertainty. Indeed, while the regulatory environment is still in its infancy, in many jurisdictions the regulatory approach to blockchain technology is of a reactive nature, with the relevant authorities constantly trying to catch up with the technology's pace of development. Yet, as one of the articles will delineate below, due to the aforementioned properties of blockchain technology, it can be very challenging to retrofit existing regulations drafted for the traditional financial sector to the decentralized financial sector enabled by Web 3 (Bodo and De Filippi 2024).

The combination of disintermediation and autonomy has even led some people to describe blockchain-based systems as being "*alegal*" (Wood 2014), in the sense that they cannot be brought under the aegis of the law. Indeed, many of these systems challenge the boundaries of the current legal system, and any attempt at bringing them within the scope of existing regulation would require a significant legal reform (De Filippi et al. 2022). That idea is not entirely without precedent. Already in 1996, with the *Declaration of Independence of Cyberspace*, John Perry Barlow advocated for the establishment of a global digital environment free from government control (Barlow 1996). A few years later, Lessig (1999) made the observation that cyberspace was "unregulatable," meaning that governments could not exercise coercive power over it. In fact, the decentralized and disintermediated nature of many Internet applications at the turn of the century made it difficult for a centralized authority to regulate their operations.

However, the progressive concentration of power in the hands of a few large online platform operators (like Alphabet/Google, Meta/Facebook, Twitter/X, etc.) who are responsible for a large majority of the Internet traffic eventually made it possible to regulate the Internet by simply regulating the operators in charge of these online platforms, requiring them to implement specific policies or code-based regulations onto their platforms (De Filippi et al. 2024b). As the Internet eventually failed to escape from regulatory oversight, blockchain technology came to the rescue, offering a new decentralized and disintermediated technological infrastructure that comes along with its own technologically mediated regulatory framework, referred to as the *lex cryptographica* (De Filippi and Wright 2018). The *lex cryptographica* would—allegedly—be immune from external regulatory control. Yet, just like with the Internet, while the regulation of blockchain-based systems remains a challenging task, the regulatory framework has begun to catch up with these technological advances—mostly focusing on the operators of newly intermediated Web 3 services (e.g., cryptocurrency exchanges, security brokers, token issuers, or other commercial operators) as the subject of these regulations. This can be seen, for example, in the European Market in Crypto Assets (MiCA) Regulation, which establishes a comprehensive regulatory framework for centralized crypto-asset service providers across the European Union.

Yet, even though it is possible to regulate centralized operators in order to influence the operations of many Web 3 applications, in the context of fully decentralized blockchain-based networks where there is no one single operator in charge of operating the system, enforcing regulations without the collaboration of a large majority of network participants can be very challenging. This is perhaps why EU legislators have chosen to exclude crypto-asset services that are "provided in a fully decentralized manner without any intermediary" (Recital 22, MiCA Regulation) from the scope of the MiCA Regulation. Courts are also struggling to regulate decentralized blockchain networks more generally. The *Tulip Trading*[1] litigation in England provides an illustrative example. Craig Wright—the founder-CEO of Tulip Trading Ltd. and self-proclaimed inventor of Bitcoin—claimed that crypto-assets worth 3 billion GBP (at the time) were stolen from two of his Bitcoin addresses. He alleged that the core developers of the Bitcoin network had both fiduciary duties and a duty of care under tort law to protect the assets of Bitcoin users, including Tulip Trading. Thus, he contended that Bitcoin core developers were under an obligation to implement a technical solution (e.g., a software patch) to help him regain control over the allegedly stolen crypto-assets. The existence of such duties has proven to be contentious, as illustrated by the divergent conclusions provided by the England & Wales' High Court and Court of Appeal when this case appeared before them.

While the High Court found that a fiduciary relationship could not exist as "bitcoin owners can[not] realistically be described as entrusting their property to a fluctuating, and unidentified, body of developers of the software" (paragraph 73, EWHC), the Court of Appeal held that a fiduciary duty could potentially be construed as a result of "entrustment" (paragraphs 77–78, EWCA), to the extent that core developers are the only ones in position to patch bugs in the software. The case shows the difficulty in attributing liability and obtaining remedies in fully decentralized blockchain networks where there is no centralized operator. In particular, it reveals the difficulty in establishing trust relationships (particularly those that are fiduciary in nature) amongst a large, fluctuating, and pseudonymous group of developers, as found in the largest public blockchain networks. Besides, although matters such as restitution and compensation are usually within the purview of the legal system, it is unclear if the legal system can offer an effective remedy in a context where coercion is specifically precluded. Finally, this example shows how the governance *of* the technology is inherently entangled with the governance *by* the technology, to the extent that the latter can impose constraints on how a technological structure may be modified or updated.

4 | Regulatory and Governance Challenges and Responses to Those Challenges

As discussed above, the distinct properties of blockchain protocols present regulatory and governance challenges that can both support and undermine trust and confidence. This is because confidence in the operation of blockchain protocols is linked—to a certain extent—to trust in a particular set of third parties, such as the network validators, or even smart contracts auditors (Bodo and De Filippi 2024).

There are numerous activities in the context of blockchain-based networks and Web 3 applications that warrant regulation and law enforcement. These include, amongst other things, criminal operations (e.g., theft, operation of ponzi schemes, money laundering, child pornography distribution), civil torts (e.g., professional negligence), and violations of human rights (e.g., privacy breaches). These also include financial mismanagement and oversight failures, which—even where they fall short of the liability standards imposed by financial or corporate law—are detrimental to the public. Peer-to-peer networks and global financial networks have long encountered these regulatory challenges, but as explained in the previous section, enforcement is particularly challenging in the context of blockchain-based networks. Even with a court order against the perpetrator of an offense, the pseudonymity of participants in blockchain networks makes regulatory enforcement a very challenging (although not impossible) task (Bodo and De Filippi 2024).

In circumstances where the operations of a Web 3 application are managed by clearly identifiable entities, as Bodo and De Filippi (2024) argue in this issue, there is no need to treat them differently from traditional centralized intermediaries. Indeed, centralized crypto-exchanges can be, and in fact often are, subject to similar Know Your Customer (KYC), Anti-Money Laundering (AML), and Counter-Terrorist Financing (CTF) laws as centralized fiat currency exchanges. Yet, many blockchain-based applications do not have any single operator in charge. Their operations are dictated by a set of code-based rules enshrined into the code of associated smart contracts, often with only limited governance power assigned to the holders of a particular cryptocurrency or token. Hence, it is possible that, in some circumstances, the operations of these blockchain-based systems be—at least partially—incompatible with existing regulations, leading to a potential conflict between the *rule of law* and the *rule of code* (De Filippi et al. 2024b). Among the numerous *constraints* in designing distributed governance systems discussed in this special issue, Bodo and De Filippi's article notes the constraints in *switching* between traditional finance and decentralized finance.

This is the case, for instance, of Tornado Cash, a decentralized blockchain-based system enabling Ethereum users to preserve the privacy of their financial transactions. In light of recent allegations that Tornado Cash was being used to support criminal activities by a North Korean terrorist group, the U.S. government decided to impose sanctions on the service. Yet, faced with the impossibility of identifying any particular legal person responsible for the operations of this blockchain-based system, the U.S. government ultimately went on to sanction Tornado Cash's smart contract addresses on Ethereum—creating controversy about whether a technological system as opposed to a person or legal entity can at all be subject to U.S. sanctions (Brito and van Valkenburgh 2022).

Most blockchain-based applications are not illegal per se, but may nonetheless fail to replicate—whether intentionally or not—specific legal provisions into their own technological ruleset. This might deprive users of some of the legal guarantees that state regulations impose upon more traditional centralized entities. For instance, directors of a company are expected to act with a duty of loyalty toward the company and demonstrate a duty of care in their decision-making processes. Because the bylaws of a company cannot articulate all the contingencies under which these duties may be breached, existing bodies of law—such as corporate law, fiduciary law, and tort law (amongst others)—establish the basic norms for a judge to determine, after the fact, whether a breach has occurred, by evaluating the factual circumstances (Hart 1961). The same does not apply in the context of DAOs. Indeed, to the extent that blockchain-based systems only abide by the rules enshrined in their code-based protocols, if certain issues are not addressed in the smart contract code of a DAO there are no default rules, norms, or mechanisms that can fill in the gaps or resolve any unexpected issue that might arise over time.

Backer's contribution to this special issue reveals the implications of this regulatory and normative void on the sources and nature of trust. He shows how the use of digital technologies was intended to address earlier crises in trust—for example, trust in corporations and corporate directors—but has in the process created new quantified, data-driven regimes of accountability that has transformed trust from being qualitative and interpersonal into a "product" (Backer 2024). Consequently, trust is no longer reposed in individuals leading corporations, but in trust accountability systems (i.e., "trust platforms"), thereby making corporate governance regimes more complex. Backer's contribution thereby highlights the constraints and limits of quantification.

Alston's contribution to this special issue also addresses this specific point on norms. He argues that although "governance by protocol" holds certain benefits (e.g., precision and finality in executing transactions), it remains inevitably *incomplete* and incapable to cope with a “complex set of exogenous shocks and human actions”, such as hacks, defects in the protocol, and the evolving needs of network participants (Alston 2024). These are constraints arising from the incompleteness of contracts—and protocols. His central argument distinguishes between two types of “social rules”: *institutions* and *norms*. The former are articulated by an organization with a view to bind the organization's members to a particular set of rules, thereby increasing confidence in the way the organization operates. The latter emerge from the aggregation of individual preferences on how others should behave. They thus become more and more costly to violate as preferences reach a critical mass. Besides, while institutions precisely define acceptable and unacceptable behavior ex ante, norms are also capable of addressing unforeseen behavior ex post. Hence, while they both contribute to promoting confidence by bringing more predictability in the system, the confidence generated by institutions is limited to a more narrow set of behaviors, whereas norms are broader in scope but weaker in terms of predictability, because they require people to trust that others will in fact intervene in order to enforce these norms. Alston sees blockchain protocols as an “aggregate set of digital institutions” which codify most of their operational rules with little room left for the emergence of social norms (Alston 2024). As such, they can provide high degrees of confidence in their everyday operations, but may sometimes face “significant governance challenges” as individuals start using the system in ways that differ from what the code was originally intended for.

Similarly, Bayern's contribution highlights the constraints of *formalism* emerging as a consequence of relying exclusively on code-based algorithms for governance. He warns that the greater the reliance of an organization on purely algorithmic governance, thereby increasing confidence by and eliminating the scope of human judgment, the greater the risk that the organizations will not be able to respond to events that were unanticipated at the time the algorithmic rules were designed and implemented, thus reducing the reliability of the system. He argues that any attempt of achieving confidence at all costs generates constraints in terms of drafting, handling errors, while removing the benefit of “centuries of legal experience” that is essentially grounded on trust (Bayern 2024).

So what kind of governance mechanism is appropriate when human discretion is desirable? Davidson and Potts (2024) argue that mechanisms inspired by corporate governance—rather than political governance—should be used to address the governance of blockchain systems. These two forms of governance serve very different functions: corporate governance seeks to prevent “insiders” (e.g., managers) exploiting “outsiders” (e.g., shareholders), while political governance seeks to “legitimize and normalize coercion”. In short, a constraint of using political governance concepts and methods to address the governance of blockchain systems is their *maladaptation* to the functions of governance in these systems. They argue that corporate governance is a more apt frame of analysis for blockchain technologies as public, permissionless blockchain protocols operate on the basis of *voluntary cooperation*, where no single actor can unilaterally coerce others. The two authors see corporate governance as a source for trust, to the extent that it can help mitigate the risk that contracts—including smart contracts—do not execute as expected. In making this argument, they depart from the more political conception of governance articulated by Ethereum founder Vitalik Buterin. Indeed, while Buterin sees (political) *legitimacy* as the key justification for people consenting to certain types of behavior and participating in the enactment of said behavior because they expect others to do the same, Davidson and Potts (2024) adopt a more economic lens, justifying these type of behaviors on the ground of property rights.

Allen et al. (2024) further expand on this perspective by investigating the governance of blockchain “treasuries,” that is, pools of cryptocurrencies that are reserved for funding local public goods such as protocol development and research grants. The authors acknowledge that the funding of public goods goes beyond the conventional role of private actors, leaning more towards the role of “nation state” and other public governance bodies. However, they argue that since public permissionless blockchain protocols are not subject to any governmental authority, corporate governance is a better fit to analyze their governance structures. As a result, they propose a hybrid approach for the governance of blockchain treasury governance, straddling both public and private governance. They identify *opportunism* as a distinct constraint of blockchain treasury governance, and designing governance systems to diminish such a constraint necessarily entails trade-offs between insider costs (i.e., opportunism by the small number of insiders who control a treasury) and outsider costs (i.e., opportunism by the outsiders who can legitimately or illegitimately gain control of a treasury).

The importance of trust in blockchain governance becomes even more apparent when blockchain products are implemented by a joint public-private project. Meyers and Keymolen (2023) illustrate this point through the case study of the “Red Button” project implemented in two municipalities in the Netherlands, allowing for indebted citizens to receive a temporary suspension in debt repayments. The project leveraged blockchain technology to allow citizens to credibly signal their indebtedness to relevant public authorities without storing any personal data on-chain, while also benefiting from an immediate stay on payments without having to directly interact with public authorities. In other words, it addressed the issue of shame that often makes indebted persons hesitant to seek help (Meyers and Keymolen 2023). As the authors note, at the time of writing, the Red Button was more of a theoretical blockchain use case than an actual product; the project still required heavy involvement from social workers and debt suspensions were not automated. However, the reference to blockchain technology was useful in revealing the *web of trust relations* that undergird the various stakeholders in this project, including citizens, public authorities, private companies developing blockchain products, and so on. For instance, the reluctance of citizens to seek debt relief is indicative of the distrust that citizens feel towards public authorities, particularly when it comes to sharing personal financial data. The success of such projects—whether or not they eventually come to use blockchain technology—requires trust, as project participants have to be certain that their “openness” or “critique” will not be used against them. In sum, *hesitation* is an overarching theme constraining the use of blockchain technology for certain public administration functions.

In light of the numerous regulatory and governance challenges discussed thus far—and the implications they have on trust and confidence in blockchain systems—what can be done to address these challenges? The authors in this special issue present a range of *solutions* to mitigate these issues by either building trust or cultivating confidence, or both.

Backer (2024) stresses the need for building trust in trust accountability systems (e.g., reputation systems), as trust in organizations, including DAOs, is contingent on trust in these overarching systems. According to Bodo and De Filippi (2024), oftentimes regulators can only indirectly influence blockchain systems, by pressuring developers and maintainers or demanding the use of specific user interfaces. Where coercion is not possible, governance becomes all the more important. In the context of Decentralized Finance (DeFi), confidence in the operations of a blockchain-based application can be increased by means of technical measures, like making smart contracts pausable, undertaking code audits, and incentivizing bug hunting. Yet, as argued by Alston (2024), a blend of both institutions and norms is needed to address the uncertainties confronting the governance of blockchain-based systems, with the former contributing to building confidence and the latter enhancing trust. To handle governance challenges arising from unintended uses of the technology, unexpected errors, or other edge cases, the set of institutional rules that makes up a blockchain-based application needs to incorporate or approximate social norms. In other words, building trust is essential for the resilience of blockchain-based systems, even in nominally trustless systems. Alston (2024) argues that, for instance, an ex post dispute resolution mechanism, like an appeal process, can help cope with unexpected events. Yet, in designing such a resolution mechanism, the selection process and incentive system for the individuals chosen to arbitrate the issue are crucial. Bodo and De Filippi (2024) also make a similar argument, advocating for a "conflict resolution" system and "insurance scheme" to diminish risk and help the DeFi ecosystem grow. Indeed, in certain contexts where ex post enforcement is impracticable, reliance on social norms can provide the "action space" through which relationships and reputations can be cultivated online, thereby making defection costly.

This is broadly in line with the approach of Davidson and Potts (2024) that encourages lessons from corporate governance and private ordering to address governance problems in the blockchain space. In particular in the context of blockchain treasuries, which requires a hybrid approach between public and private governance, trust can be generated by practices like electing foundations or committees, stakeholder voting, self-executing spending decisions, "as well as innovative voting mechanisms with asymmetric voting weights (such as quadratic voting)" (Allen et al. 2024). In the more explicitly public context of municipal debt recovery, Meyers and Keymolen (2023) argue that trust can be built by reducing legal and technical complexity and involving citizens more deeply in the design of blockchain-based applications. This reflects a diversity of approaches towards generating trust in the blockchain space, but as Allen et al. (2024) persuasively argue, each institutional environment is different and this diversity should be embraced.

Bayern (2024), in contrast, tackles the voluntary compliance of state regulation over the cultivation of social norms. He contends that even those blockchain networks which purport to operate beyond the purview of the law should *voluntarily submit* to state regulation (specifically, corporate laws) so as to reduce formalism costs. Indeed, provided that the judicial system will respect the intention and autonomy of parties to set up their governance and business affairs as long as they comply with the law, regulatory compliance will contribute to protecting blockchain systems from outside intervention. In other words, the predictability of a blockchain network can be buttressed with the support of a robust and advanced legal system, bringing greater confidence in a regulatory compliant system than in a system that operates in isolation. Yet, Bodo and De Filippi warn that the application of regulation or the adoption of new supervisory authorities for the blockchain ecosystem comes along with certain trade-offs: the technological and financial risks of an unsupervised environment need to be counterbalanced with the risk of a greater centralization of power in the hands of regulatory authorities, who may potentially interfere with the operations of an allegedly autonomous blockchain-based system.

5 | Articles in This Special Issue

In this section, we provide an overview of the articles that are part of this special issue and how they relate to the use of trust and confidence in the context of regulation and governance. We organized the articles according to three broad themes: (1) theorizing trust and emerging technologies, (2) trust and governance in blockchain systems, and (3) emerging technologies, trust, and global governance.

Theme 1: Theorizing Trust and Emerging Technologies.

Eric C. Alston. *Norms, Institutions, and Digital Veils of Ignorance—Do Network Protocols Even Need Trust?*

This article explores the dynamics of governance in digital spaces, particularly focusing on the role of institutions and norms within blockchain protocols and smart contracts. It distinguishes between institutions, which define and enforce rules ex ante to manage predictable behaviors, and norms, which guide behavior in both known and unpredictable situations. While blockchain systems aim for institutional completeness, they face limitations when dealing with unforeseen events. Thus, Alston highlights the importance of balancing formal institutional rules with community-driven norms, arguing that blockchain protocols need to account for flexibility, as institutions alone may not fully address the complexities and uncertainties that may arise in these systems. Social norms that exist within the user community can complement these protocols to better address uncertainty, making it easier for blockchain systems to adapt to unexpected challenges, thereby maintaining trust among users. The article's practical examples, such as the Facebook oversight board and the Lightning Network, demonstrate how these concepts apply in real-world settings, offering valuable insights for protocol designers and policymakers navigating the challenges of digital governance.

Bodo Balazs and Primavera De Filippi. *Trust in Context: The Impact of Regulation on Blockchain and DeFi*.

This article explores the contrasting foundations of trust and confidence in traditional financial systems and decentralized financial services (DeFi). Traditional finance relies on regulation, trusted intermediaries, and established norms to build trust. In contrast, DeFi seeks to establish confidence through blockchain technology, which enforces rules via protocols and smart contracts, reducing reliance on intermediaries. However, Balazs and De Filippi argue that despite the technological safeguards of DeFi, traditional trust mechanisms, such as governance and anti-fraud regulation, remain essential to address issues like bugs, scams, and overall system integrity.

The article delves into the complex relationship between trust and confidence, suggesting that while DeFi aims to shift reliance from institutions to code, it cannot entirely eliminate the need for traditional trust mechanisms. Regulation and trusted intermediaries may still be necessary for DeFi to gain widespread adoption, particularly in mitigating risks and uncertainties that purely software-based solutions cannot address. In other words, the article suggests that DeFi's confidence-based model, while innovative, must integrate with traditional trust-enhancing structures to ensure reliability and user confidence. This blending of trust architectures is seen as crucial for DeFi's long-term viability and regulatory acceptance.

Yet, the article also acknowledges that if regulation in the DeFi space can help bridge the gap between code-based confidence and the broader trust that users require to engage with financial systems, it may also contribute to reducing the confidence that users have in the operation of DeFi systems that are no longer purely algorithmically regulated and can therefore be influenced and potentially interfered with by regulatory authorities.

Theme 2: Trust and Governance in Blockchain Systems.

Darcy Allen, Chris Berg, and Aaron Lane. *The Blockchain Treasury Governance Dilemma*.

Allen, Berg and Lane's article calls for the governance of blockchain treasuries using both public and private governance. The authors concentrate on the various opportunism costs—both endogenous (e.g., misappropriation of funds by internal actors) and exogenous (e.g., malicious diversion of funds by external actors)—can be mitigated so as to establish trust. Drawing from the Institutional Possibility Frontier (IPF) framework—distinguishing between dictatorship costs (related to public expropriation) and disorder costs (related to private expropriation)—they seek to understand how these trade-offs take place in the context of blockchain treasury governance. Instead of the trade-off between dictatorship costs and disorder costs, they see a trade-off between insider costs and outsider costs. Insider costs are attributable to how *authority* is allocated, while outsider costs arise due to the "open nature of blockchain ecosystems", allowing for private expropriation through economic (e.g., collusion) or technical (e.g., hacking) means.

The authors argue that both typologies of costs (insider and outsiders costs) change over time and generally compensate one another. Through various cases, they show how attempts to reduce one set of costs generally increase the other set of costs. For instance, the use of a multisignature wallet (i.e., a wallet that requires a particular number of authorized signatures to execute a transaction) to govern the treasury of the popular decentralized exchange Uniswap mitigates the outsider costs linked to a potential takeover by the holders of Uniswap's native token, but also generates higher insider costs, as the treasury is controlled by a small number of actors, who necessarily have to be trusted not to collude to divert the funds. The authors also show how institutional design evolves in response to governance crises, with, for example, the Sushiswap decentralized exchange reposing control over their treasury to a small group of early Sushi Swap investors after a scandal concerning an abuse of power by the anonymous founder of the exchange, Chef Nomi, who was then the sole holder of the keys to the Sushi Swap treasury. In the Sushi Swap case, a small increase in outsider costs was seen as worthwhile, in the face of insider opportunism. In the authors' view, the right balance must be found between insider and outsider costs in an effort to bolster trust in the governance of blockchain treasuries.

Sinclair Davidson. *Corporate Governance in a Crypto-World*.

In this article, the author contends that the means and processes used to govern blockchain systems should draw inspiration from corporate governance instead of political governance. He explains that while both forms of governance are influential in discussions on blockchain governance, they do not serve the same function. Political governance is primarily concerned with creating a legitimate basis for coercion in a context of involuntary cooperation. Corporate governance is more concerned with preventing governance insiders like managers from exploiting governance outsiders like shareholders in a context of voluntary cooperation. The latter is more akin to the situation in blockchain-based systems as they also rely on voluntary cooperation in which unilateral coercion by a centralized entity is not possible. As with corporations, the author notes that foundations, trusts, and other corporate entities are often used by blockchain protocols to perform certain coordinating functions and engage with off-chain actors. Thus, just as corporate governance is used to build trust in corporations, principles and mechanisms drawn from corporate governance can also be a source of trust in blockchain-based systems when on-chain governance fails or is incomplete.

Gert Meyers and Esther Keymolen. *A Blockchain Solution Looking for a Problem: Blockchain, Solutionism, and Trust*.

This article critically examines the promises and limitations of blockchain technology, particularly its claim to create "trustless" systems. While blockchain technology is often presented as a solution to trust-related issues, the article argues that it does not eliminate the need for trust. Instead, new forms of trust must be established at different levels to make blockchain applications functional in real-world scenarios. The case study of the Dutch Red Button pilot illustrates this, showing how, even when the promises of blockchain technology are not fully realized, it can still act as a productive force in shaping new technological solutions and governance models.

Overall, the article emphasizes that trust remains crucial even in systems designed to minimize it. The narratives and promises surrounding blockchain technology influence the development of novel applications, regardless of whether these promises are ultimately implemented. By highlighting the gap between the theoretical benefits of blockchain and its practical challenges, the article contributes to the broader discussion on how emerging technologies intersect with trust and governance, underscoring the importance of considering both the technological and social dimensions of blockchain in regulatory contexts.

Theme 3: Emerging Technologies, Trust, and the Law.

Larry Catá Backer. Trust Platforms: *The Digitalization of Corporate Governance and the Transformation of Trust in Polycentric Space*.

In this article, the author traces the evolution of trust prompted by the use of data-driven digital technologies and its implications on corporate accountability. From initially arising through interpersonal relationships, these technologies transform the sources of trust by making seemingly objective and quantifiable metrics and measures the basis of trust. These metrics and measures of trust are mediated by trust accountability systems, which Backer calls "trust platforms." One example of a trust platform provided by Backer is the state itself, but a trust platform does not have to be a public actor.

These trust platforms aggregate and analyze data from multiple groups of producers and consumers. They also enable multiple regulatory frameworks and standards to be applied to the governance of organizations that seek to be trusted (e.g., the UN Guiding Principles of Business and Human Rights applied to corporations). Through their mediation of a patchwork of trust relationships (e.g., boards and user communities) using digital technologies, the nature of trust is transformed by these trust platforms into a "product" and "commodity." Consequently, the author argues that legal compliance requires less normative judgment and increasingly involves purportedly objective assessments of these metrics and measures against relevant regulations and standards. This assessment is often carried out by third parties separate from actors being asked to trust (e.g., consumers) and actors seeking to be trusted (e.g., corporations). Trust is thereby "produced" by these platforms, but ultimately raises questions about the trustworthiness of these trust platforms themselves.

Shawn Bayern. *Trusting Organizational Law*.

This article explores the interplay between trust and confidence within blockchain systems. It argues that while blockchain aims to create trustless systems, eliminating human judgment and relying solely on algorithms introduces significant challenges. Two of these challenges include "implementation costs" referring to the resource-intensive aspects of purely algorithmic governance, and "formalism costs" referring to how purely algorithmic systems are prone to drift from intended outcomes and are vulnerable to unexpected scenarios.

To mitigate these issues, Bayern advocates for integrating principles of organizational law within blockchain systems, using the legal framework as a complement to algorithmic governance as a means to achieve more flexibility for addressing errors or unforeseen circumstances. By doing so, it is possible to enhance trust and confidence in these decentralized platforms, balancing the rigidity of technology with the adaptability of law.

Ultimately, the article emphasizes that reliance on organizational law can reduce the costs and risks associated with relying exclusively on technology, reinforcing the idea that effective governance requires a combination of legal and technological mechanisms, rather than an overreliance on either. By positioning organizational law as a mediator between algorithms and legal enforcement, Bayern contributes to broader discussions on trust and confidence in the governance of emerging technologies.

Acknowledgments

This research is funded by the European Research Council under the European Union's Horizon 2020 Research and Innovation Programme (Grant Agreement No. 865856). Open Access funding enabled and organized by Projekt DEAL.

Conflicts of Interest

The authors declare no conflicts of interest.

Data Availability Statement

Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

Endnotes

[1] *Tulip Trading Ltd. v. Bitcoin Association* [2022] EWHC 667 (Ch) [EWHC judgment]; *Tulip Trading Limited v. van der Laan and others* [2023] EWCA Civ 83 [EWCA judgment].

References

Allen, D., C. Berg, and A. Lane. 2024. "The Blockchain Treasury Governance Dilemma." *Regulation & Governance*.

Alston, E. 2024. "Norms, Institutions, and Digital Veils of Uncertainty—Do Network Protocols Need Trust Anyway?" *Regulation & Governance*. https://doi.org/10.1111/rego.12628.

Atzori, M. 2017. "Blockchain Technology and Decentralized Governance: Is the State Still Necessary?" *Journal of Governance and Regulation* 6, no. 1: 45–62. https://doi.org/10.22495/jgr_v6_i1_p5.

Backer, L. 2024. "Trust Platforms: The Digitalization of Corporate Governance and the Transformation of Trust in Polycentric Space." *Regulation & Governance*. https://doi.org/10.1111/rego.12614.

Baran, P. 1964. "On Distributed Communications Networks." *IEEE Transactions on Communications Systems* 12, no. 1: 1–9. https://doi.org/10.1109/TCOM.1964.1088883.

Barlow, J. P. 1996. "A Declaration of the Independence of Cyberspace." http://editions-hache.com/.

Bayern, S. 2024. "Trusting Organizational Law." *Regulation & Governance*. https://doi.org/10.1111/rego.12616.

Bernstein, M. H. 2016. *Regulating Business by Independent Commission*. Princeton University Press.

Bodo, B. 2021. "Mediated Trust: A Theoretical Framework to Address the Trustworthiness of Technological Trust Mediators." *New Media & Society* 23, no. 9: 2668–2690.

Bodo, B., and P. De Filippi. 2024. "Trust in Context: The Impact of Regulation on Blockchain and DeFi." *Regulation & Governance. Advance Online Publication*. https://doi.org/10.1111/rego.12637.

Böhme, R., N. Christin, B. Edelman, and T. Moore. 2015. "Bitcoin: Economics, Technology, and Governance." *Journal of Economic Perspectives* 29, no. 2: 213–238. https://doi.org/10.1257/jep.29.2.213.

Bradford, A. 2023. *Digital Empires: The Global Battle to Regulate Technology*. Oxford University Press.

Brito, J., and P. van Valkenburgh. 2022. "What Is and What Is Not a Sanctionable Entity in the Tornado Cash Case. *CoinCenter* (15 August)." https://www.coincenter.org/analysis-what-is-and-what-is-not-a-sanctionable-entity-in-the-tornado-cash-case/.

Buterin, V. 2014. "A Next-Generation Smart Contract and Decentralized Application Platform." https://ethereum.org/en/whitepaper.

Celeste, E. 2019. "Digital Constitutionalism: A New Systematic Theorisation." *International Review of Law, Computers & Technology* 33, no. 1: 76–99. https://doi.org/10.1080/13600869.2019.1562604.

Christiansen, T., and S. Piattoni, eds. 2003. *Informal Governance in the European Union*. Edward Elgar Publishing.

Craig, T. 2024. "Early AssangeDAO Member on Freeing of WikiLeaks founder: 'A Huge Victory for Crypto' *DL News* (25 June)." https://www.dlnews.com/articles/defi/assangedao-on-wikileaks-founder-julian-assange/.

Davidson, S., and J. Potts. 2024. "Corporate Governance in a Crypto-World." *Regulation & Governance*.

De Gregorio, G. 2022. "Digital Constitutionalism Across the Atlantic." *Global Constitutionalism* 11: 297–324. https://doi.org/10.1017/S2045381722000016.

De Filippi, P. 2014. "Bitcoin: A Regulatory Nightmare to a Libertarian Dream." *Internet Policy Review* 3, no. 2: 1–11. https://doi.org/10.14763/2014.2.286.

De Filippi, P. 2017. "What Blockchain Means for the Sharing Economy." *Harvard Business Review* 15, no. 03.

De Filippi, P., and S. Hassan. 2018. "Blockchain Technology as a Regulatory Technology: From Code is Law to Law is Code." *arXiv preprint. arXiv:1801.02507.*

De Filippi, P., and A. Wright. 2018. *Blockchain and the Law: The Rule of Code*. Harvard University Press. https://doi.org/10.2307/j.ctv2867sp.

De Filippi, P., M. Mannan, and W. Reijers. 2020. "Blockchain as a Confidence Machine: The Problem of Trust & Challenges of Governance." *Technology in Society* 62: 101284.

De Filippi, P., M. Mannan, and W. Reijers. 2022. "The Alegality of Blockchain Technology." *Policy and Society* 41, no. 3: 358–372. https://doi.org/10.1093/polsoc/puac006.

De Filippi, P., M. Mannan, and W. Reijers. 2024b. "Blockchain Technology and the Rule of Code: Regulation via Governance." *George Washington Law Review* 92: 1229–1280.

De Filippi, P., W. Reijers, and M. Mannan. 2024a. *Blockchain Governance*. MIT Press.

Diver, L. 2021. "Digisprudence: The Design of Legitimate Code." *Law, Innovation and Technology* 13, no. 2: 325–354. https://doi.org/10.31228/osf.io/nechu.

DuPont, Q. 2018. "Experiments in Algorithmic Governance: An Ethnography of "The DAO," a Failed Decentralized Autonomous Organization." In *Bitcoin and Beyond: The Challenges and Opportunities of Blockchains for Global Governance*, edited by M. Campbell-Verduyn, 157–177. Routledge.

Fukuyama, F. 2013. "What Is Governance?" *Governance* 26, no. 3: 347–368. https://doi.org/10.1111/gove.12035.

Gambetta, D. 2000. "Can We Trust Trust?" In *Trust: Making and Breaking Cooperative Relations*, edited by D. Gambetta. University of Oxford Press.

Giddens, A. 1990. *The Consequences of Modernity*. Polity Press.

Giddens, A. 1999. "Risk and Responsibility." *Modern Law Review* 62, no. 1: 1–10. http://www.jstor.org/stable/1097071.

Golumbia, D. 2016. *The Politics of Bitcoin: Software as Right-Wing Extremism*. University of Minnesota Press.

Hardin, R. 2002. *Trust and Trustworthiness*. Russell Sage Foundation.

Hart, H. L. A. 1961. *The Concept of Law*. Clarendon Press.

Heilbroner, R. L. 1967. "Do Machines Make History?" *Technology and Culture* 8, no. 3: 335–345.

Hildebrandt, M. 2018. "Algorithmic Regulation and the Rule of Law." *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 376, no. 2128: 1–11. https://doi.org/10.1098/rsta.2017.0355.

Jongen, H., and J. A. Scholte. 2021. "Legitimacy in Multistakeholder Global Governance at ICANN." *Global Governance* 27, no. 2: 298–324. https://doi.org/10.1163/19426720-02702004.

Kaler, J. 2002. "Responsibility, Accountability and Governance." *Business Ethics: A European Review* 11, no. 4: 327–334. https://doi.org/10.1111/1467-8608.00292.

Kjaer, A. M. 2023. *Governance*. John Wiley & Sons.

Klonick, K. 2020. "The Facebook Oversight Board: Creating an Independent Institution to Adjudicate Online Free Expression." *Yale Law Journal* 129, no. 8: 2418–2499.

Kroll, J. A., I. C. Davey, and E. W. Felten. 2013. The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries; The Twelfth Workshop on the Economics of Information Security (WEIS 2013), Washington, DC, June 11–12, 1–21. https://www.econinfosec.org/archive/weis2013/papers/KrollDaveyFeltenWEIS2013.pdf.

Laffont, J. J. 2005. *Regulation and Development*. Cambridge University Press.

Lehdonvirta, V. 2022. *Cloud Empires: How Digital Platforms are Overtaking the State and How we can Regain Control*. MIT Press. https://doi.org/10.7551/mitpress/14219.001.0001.

Lessig, L. 1999. *Code and Other Laws of Cyberspace*. Basic Books.

Levi-Faur, D. 2011. "Regulation and Regulatory Governance." In *Handbook on the Politics of Regulation*, edited by D. Levi-Faur. Edward Elgar.

Locke, J. 1988. *Two Treatises of Government*. Cambridge University Press.

Lorenz, E. 1999. "Trust, Contract and Economic Cooperation." *Cambridge Journal of Economics* 23, no. 3: 301–315.

Luhmann, N. 2000. "Familiarity, Confidence, Trust: Problems and Alternatives." In *Trust: Making and Breaking Cooperative Relations*, edited by D. Gambetta. Oxford University Press.

Mannan, M. 2018. "Fostering Worker Cooperatives With Blockchain Technology: Lessons From the Colony Project." *Erasmus Law Review* 11, no. 3: 190–203.

Mannan, M., and S. Pek. 2024. "Platform Cooperatives and the Dilemmas of Platform Worker-Member Participation." *New Technology, Work and Employment* 39, no. 2: 219–237. https://doi.org/10.1111/ntwe.12273.

Mannan, M., and N. Schneider. 2021. "Exit to Community: Strategies for Multi-Stakeholder Ownership in the Platform Economy." *Georgetown Law Technology Review* 5, no. 1: 1–71.

Mazzucato, M. 2019. "Preventing Digital Feudalism. Project Syndicate, 1–3." https://www.neweurope.eu/article/preventing-digital-feudalism/.

McLuhan, M. 1957. *Understanding Media*. MIT Press.

Meyers, G., and E. Keymolen. 2023. "Realizing a Blockchain Solution Without Blockchain? Blockchain, Solutionism, and Trust." *Regulation & Governance*. https://doi.org/10.1111/rego.12553.

Mitnick, B. M. 1975. "The Theory of Agency: The Policing "Paradox" and Regulatory Behavior." *Public Choice* 24, no. 1: 27–42. https://www.jstor.org/stable/30022842.

Pasquale, F. 2018. *Digital Capitalism: How to Tame the Platform Juggernauts*, 1–4. Friedrich-Ebert-Stiftung-Division for Economic and Social Policy. http://library.fes.de/pdf-files/wiso/14444.pdf.

Pettit, P. 1995. "The Cunning of Trust." *Philosophy & Public Affairs* 24, no. 3: 202–225.

Reijers, W., I. Wuisman, M. Mannan, et al. 2021. "Now the Code Runs Itself: On-Chain and off-Chain Governance of Blockchain Technologies." *Topoi* 40, no. 4: 821–831. https://doi.org/10.1007/s11245-018-9626-5.

Rennie, E., M. Zargham, J. Tan, et al. 2022. "Toward a Participatory Digital Ethnography of Blockchain Governance." *Qualitative Inquiry* 28, no. 7: 837–847.

Rushkoff, D. 2022. *Survival of the Richest: Escape Fantasies of the Tech Billionaires*. W.W. Norton.

Schneider, N. 2022. "Admins, Mods, and Benevolent Dictators for Life: The Implicit Feudalism of Online Communities." *New Media & Society* 24, no. 9: 1965–1985.

Swan, M. 2015. *Blockchain: Blueprint for a New Economy*. O'Reilly Media.

Swartz, L. 2018. "What was Bitcoin, What Will It Be? The Techno-Economic Imaginaries of a New Money Technology." *Cultural Studies* 32, no. 4: 623–650. https://doi.org/10.1080/09502386.2017.1416420.

Suzor, N. 2018. "Digital Constitutionalism: Using the Rule of Law to Evaluate the Legitimacy of Governance by Platforms." *Social Media + Society* 4, no. 3: 1–11.

Szabo, N. 1997. "Formalizing and Securing Relationships on Public Networks." *First Monday* 2, no. 9. https://doi.org/10.5210/fm.v2i9.548.

Tapscott, D., and A. Tapscott. 2016. *Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World*. Penguin.

Turner, F. 2006. *From Counterculture to Cyberculture: Steward Brand, the Whole Earth Network, and the Rise of Digital Utopianism*. University of Chicago Press.

Varoufakis, Y. 2023. *Technofeudalism: What Killed Capitalism*. Penguin.

Vigna, P., and M. J. Casey. 2016. *The Age of Cryptocurrency: How Bitcoin and the Blockchain are Challenging the Global Economic Order*. St. Martin's Press.

Whitten-Woodring, J., M. S. Kleinberg, A. Thawnghmung, and M. T. Thitsar. 2020. "Poison if You Don't Know How to Use It: Facebook, Democracy, and Human Rights in Myanmar." *International Journal of Press/Politics* 25, no. 3: 407–425.

Wood, G. 2014. Alegality: Systems that Can't Care. Coin Scrum and Proof of Work Media: Tools for the future. https://www.youtube.com/watch?v=Zh9BxYTSrGU.

Wylie, C. 2019. *Mindf*Ck: Cambridge Analytica and the Plot to Break America*. Random House.

Zuboff, S. 2019. *The Age of Surveillance Capitalism*. Public Affairs.

Zwitter, A., and J. Hazenberg. 2021. "Cyberspace, Blockchain, Governance: How Technology Implies Normative Power and Regulation." In *Blockchain, Law and Governance*, edited by B. Cappiello and G. Carullo. Springer.