Blockchain for the Governance of Common Good

Philémon Poux, Primavera de Filippi, Simona Ramos

Blockchains for the Governance of Common Goods

Philémon Poux
philemon.poux@gmail.com
Universite Paris II, CERSA, CRED,ENPC France

Primavera de Filippi
CNRS, France;
Harvard University, Berkman-Klein Center, USA

Simona Ramos
Universitat Pompeu Fabra, Barcelona, Spain
Nokia Bell Labs France

Abstract

This paper analyses the use of blockchain technology to support the governance of commons-pool resources, as studied by Elinor Ostrom. It argues that the technological guarantees of blockchain technology —in terms of *ex-ante* automation and *ex-post* verification— can replace the traditional requirements of monitoring and sanctioning. Despite its own limitations and challenges, this novel approach to governance could provide new opportunities for experimentation in the context of commons-pool resources.

1 Introduction

Although originally invented as the underlying infrastructure for the Bitcoin cryptocurrency [15], blockchain technology has progressively evolved into a general-purpose technology that can support a large variety of applications other than monetary transactions. As a distributed ledger operating on top of a peer-to-peer network, a blockchain relies on cryptographic primitives and a consensus protocol in order to maintain a database that is logically centralized, yet technically decentralized. With the development of more sophisticated blockchains with smart contracts capabilities, novel opportunities have emerged to coordinate agents in secure and distributed manner. One particularly interesting affordance of blockchain technology is the extent to which it enables communities to govern themselves through a series of predefined code-based rules in order to reach mutual consensus without the interference or the need for a central authority[12].

This paper investigates the use of blockchain technology for the governance of Common-Pool Resources (CPRs). It shows that, while a distributed system cannot easily address the challenges of monitoring and sanctioning (which are often regarded as key pillars for the proper governance of CPRs), blockchain technology could largely bypass these challenges by way of its technological guarantees. As such, the technology could bring new perspectives to the traditional analysis and practices of CPR governance.

The paper is structured as follow: After presenting the core characteristics of blockchain technology

(section 2), we introduce the traditional work of Ostrom on the governance of Common-Pool Resources (section 3) and subsequently analyse the extent to which some of the components of CPR governance could be simplified or even enhanced by means of a blockchain-based infrastructure. The paper will focus in particular on the opportunities to move away from the need of monitoring and sanctioning, with the possibility to rely instead on a system of *ex-ante* automation and *ex-post* verification (section 4). Finally, the paper will conclude by discussing the limitations of a purely blockchain-based approach to CPR governance, in light of the necessity to account for real world events (section 5), as well as the challenges inherent to blockchain technology more generally (section 6).

2 Blockchains in a Nutshell

A blockchain is an append-only distributed ledger that records transactions in a transparent, verifiable and permanent manner by storing them into a sequence (or "chain") of blocks. The content of a blockchain is secured through cryptographic primitives (e.g. public-private key cryptography and hashing functions) so that, once a transaction has been recorded into a block, it cannot be tampered with without such a violation being detected by all the network nodes [26]. The tamper-resistant properties of a blockchain are crucial to guarantee the integrity and authenticity of all data stored into this decentralized database.

While the first generation of blockchains were mostly used for the exchange of cryptocurrencies like Bitcoin, many blockchains today also make it possible to engage into a series of more complex transactions by incorporating pieces of code directly into the blockchain. These programs —which are generally referred to as "smart contracts"[25] or DApps (Decentralized Applications)— are executed in a distributed manner by all network nodes. The benefit of smart contracts over traditional software code is that their execution cannot be affected (e.g. modified or terminated) by any single node. In fact, all nodes involved in the verification of blockchain transactions are also responsible for the proper execution of smart contracts. These applications are thus often described as "trustless systems" because they create the possibility of establishing a trust layer between parties that do not know or trust each other[27].

However, considering that smart contracts operate on top of a blockchain-based network, their execution is dictated by the rules of the underlying blockchain protocol. Hence, the operations of a smart contract could potentially be affected by changes in the blockchain protocol itself. Although theoretically immutable, the rules governing a blockchain can be changed by consensus among all network nodes. This is where the issue of blockchain governance comes in.

Broadly speaking, blockchain governance is the process by which changes to the blockchain protocol are decided upon and implemented. While the process may vary from blockchain to blockchain, the operations of a blockchain generally rely on a special group of network nodes —the miners— that are rewarded by the blockchain protocol for their contribution to the network[28]. These nodes are responsible for creating new blocks of transaction, in accordance with the protocol rule.

Yet, this is not to say that blockchains are governed only and exclusively by code. The majority of blockchain-based networks are governed by a combination of on-chain and off-chain rules. On-chain rules are technical rules embedded directly in the code or the protocol of a blockchain-based network (e.g the economic incentives, consensus algorithm, etc.) and are thus automatically enforced by the underlying infrastructure. As noted by De Filippi&McMullen [5], on-chain rules are a form of "governance by the infrastructure". Off-chain rules are social or institutional rules that a blockchain community has put into place in order to elaborate the rules that will subsequently be codified into the technological infrastructure, as well as the procedures to change these rules. As such, off-chain rules refer to the "governance of the infrastructure", including all the procedures and rules capable of influencing the operations and governance of a blockchain-based system, even if that means infring-

ing the original protocol rules[23].

3 Institutional Analysis and Development Framework and Common-Pool Resources Governance

Ostrom dedicated her life to the study of CPRs. Although she mostly focused on natural common-pool resources, she also extended her work the governance of information commons and in particular open-source software [7].

Drawing from years of research by Ostrom and other members of the Bloomington School on the management of Common-Pool Resources (CPRs), *Rules, Games, and Common-Pool Resources*[20] has become a landmark contribution to the study of commons-based governance. The book shows —theoretically, experimentally and empirically— that, without proper communication and coordination mechanisms, groups often end up with a sub-optimal use of CPRs, mostly due to over-exploitation or under-provision. Conversely, when given the means to better coordinate, many groups demonstrated a near optimal use of the CPRs. Crucial to this outcome is the ability for a community to monitor the behavior of all of its members, along with the capacity to sanction the defectors.

Through this work, Ostrom and her colleagues developed the Institutional Analysis and Development (IAD) Framework [20] "to understand the ways in which institutions operate and change over time"[14]. It focuses on an *action-situation* which is the "black box" where policy choices are made[14]. In other words, the *action-situation* is the system studied by IAD analysts, it comprises the environment, the actors and all relationships (in)between actors and their environment. The purpose of the IAD is to reveal and describe this "black box" mechanisms by identifying all of its components (actors, environment, rules, institutions...).

They identified 8 design principles[16] which could each contribute to a more sustainable management of CPRs (although none of them are not

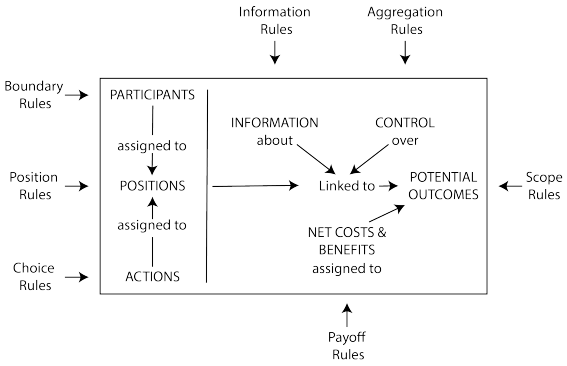

Figure 1: IAD and Rules: depiction of an *action-situation*. Adapted from Figure 7.1 from [18, p.189]

stricto sensu necessary). The following list of principles has been refined by Cox *et al.* [2] (and endorsed by Ostrom [19]): **(DP1)** User and resource boundaries **(DP2)** Congruence with local conditions **(DP3)** Appropriation and provision **(DP4)** Collective choice arrangement **(DP5)** Monitoring users and the resource **(DP6)** Gradual sanctions **(DP7)** Conflict resolution mechanisms **(DP8)** Nested enterprise

Ostrom has often insisted that the IAD framework is an analytic framework that merely provides a "Grammar of Institutions" [3] to help disentangle the complexities of roles and interactions in any given institutional arrangement.The IAD grammar is made of 7 types of rules characterizing the relationships between the different actors involved in a particular *action-situation*. Each of these rules can be implemented in multiple ways depending on the context and contingencies. The rules and the *action-situation* are summarized Figure 1. How blockchains can help implement particular configurations of these rules is discussed below.

Some authors have already been analysing the potential of blockchain technology in light of this specific field of research . In particular, Rozas *et al.* [24] have shown that many blockchains were compatible with the 8 design principles identified by Ostrom for the governance of digital commons. They identified 6 main affordances of blockchain technology that make it particularly suitable for the governance of digital or immaterial commons-based peer-

production resources. Each of the design principles are then checked against the affordances showing how they can be properly reproduced on a blockchain.

In an Ostrom Workshop, Howell&Potgieter[8] used the IAD framework to analyse blockchains as commons-pool resources, using Bitcoin and Ethereum as the two main case studies. They found that the 8 design principles for CPR governance are only partially met within these networks. Yet, their conclusion is that these limitations are not intrinsic to blockchain technology, but rather pertain to the specific implementations thereof.

And most importantly, Cila et al.[1] extensively discuss the dilemmas that could result from a relying on a blockchain governance tool for a energy commons in a fictional community. We here wish to complement their forward planning work while acknowledging the importance of their conclusions and in particular that these dilemmas require political decisions and offer no clear solutions.

This paper aims to move beyond a purely descriptive, prospective or analytical analysis of blockchain technology in the context of CPR governance. It proposes a more normative approach, claiming that some of the components of CPR governance could be delegated to a blockchain, resulting a new set of *action-situations* that rely less on monitoring and sanctioning and more on *ex-ante* automation and *ex-post* verification as a means to reduce the likelihood of opportunistic behaviours.

4 From a “trust-based” to a “proof-based” system

As previously discussed, Ostrom[17] argued that decentralized yet coordinated action may be difficult to achieve without proper monitoring or enforcement. Monitoring is necessary to ensure that all actors remain accountable to each other and continue to act in accordance with the general system of rules they have agreed to. In a centralized setting, this is generally referred to as "surveillance". Enforcement is necessary to ensure that all actors who diverge from these rules will be sanctioned, and potentially even banned or excluded from the system. This is usually referred to as "policing".

Blockchain technology provides a decentralized solution to precisely both of these challenges. While decentralized monitoring would be problematic as it would require an excessive degree of transparency, with an ensuing invasion of privacy for all of the participants, the same benefits can be achieved in a decentralized setting by means of *ex-post* verifiability, using blockchain technology to record (proofs of) information in an encrypted and tamper-resistant manner —so that the information does not have to be disclosed to the public, but the content and integrity thereof can subsequently be verified by the relevant third parties[24]. Enforcement — which is generally done *ex-post* (i.e. after the fact)— can be achieved in a decentralized setting by means of *ex-ante* automation, using a system of smart contracts for the trusted execution of specific agreements, automatically executed by the underlying technology[6].

Accordingly, the benefits of blockchain technology for the governance of CPRs are essentially twofold. Through *ex-post* verifiability, blockchain technology could increase confidence in the institutional arrangements established by the community members managing and operating CPRs, restoring the trust level conferred to these institutional arrangements while simultaneously reducing the need for global scrutiny and oversight. Through *ex-ante* automation, the use of blockchain technology could facilitate new forms of cooperation amongst these community members, providing for a trusted and coordinated mechanism of bottom-up collaboration that does not rely on any centralized superpower or other trusted authority. Hence, we argue that blockchain technology could be a relevant tool for the governance of CPRs, without the need to implement mechanisms of monitoring and sanctioning.

Yet, the creation of a common framework or infrastructure on top of which such decentralized mechanisms of *ex-ante* automation and *ex-post* verification can be built would require all relevant stakeholders to agree upon a common set of rules governing their interactions with one another —a "social contract" of some sort[10]. Such an agreement would have to be voluntarily adopted by all relevant

community members involved in the management of the relevant CPRs.

While it is unlikely that the whole governance structure of a particular CPR can be codified in its entirety into a blockchain-based infrastructure, some of its components could nonetheless be transposed into a series of technological guarantees that would provide a greater degree of confidence in the system. Hence, by analysing the institutional arrangements of a particular community managing CPRs through the IAD framework, it might be possible to identify (a) the specific components or rules that could be (partially) codified into a blockchain-based system, in order to ensure full compliance with these rules through *ex-ante* automation, and (b) the components whose execution could be recorded onto a blockchain, in order to provide for *ex-post* verifiability.

Using the IAD framework to analyse the governance of CPRs would help identify the different types of rules constituting the *action-situations* at play within a particular community. The community governing these CPRs could then decide, to implement some aspects of their governance system into a blockchain-based system. Such a decision could be driven by a desire to enhance the transparency and accountability of the system, or make it more efficient by reducing the costs of monitoring and sanctioning.

Examples of such governance components that could be delegated to a blockchain include:

- "**boundaries**", "**position**" and "**choice**" rules (e.g. the identity of the relevant stakeholders and their respective functions and roles in the management of CPRs)[1]
- "**governance**" rules governing the interactions of community members (e.g. rules governing service provision, monitoring, and management);
- "**scope**" rules that must be respected by community members (e.g. administrative procedures and its timing, maintenance protocols, etc.);
- "**dispute resolution**" rules (e.g. the procedures for the resolution of disputes arising between community members and the procedures for the application of sanctions, if any)

The codification of these components of the IAD framework into a blockchain-based system would enable relevant community members to have a clear insight into the institutional arrangements of the community, as well as their respective roles and responsibilities. Most importantly, to the extent that these rules would be automatically executed by the underlying technology, the need for monitoring and sanctioning would be lessened, given that relevant parties would be unable to infringe these rules in the first place.

With regard to the components that cannot be automated into code, it would still be possible to record the proofs associated with particular operations into a blockchain-based system (e.g. *proof-of-process*) in order to ensure the *ex-post verifiability* of administrative procedures by each responsible party. By recording the fingerprint (or *hash*) of specific documents or data sets onto a blockchain on an on-going basis, one can create an immutable and certified audit trail of relevant events, which can be verified at a later stage. In case of a dispute, these proofs would enable the relevant stakeholders and/or government authorities to verify whether the community rules have been properly observed by the responsible parties by simply comparing the hash of the presented documents or data sets, with those that have been previously recorded onto the blockchain. Such a solution would contribute to creating more transparency and accountability into the system, without unduly jeopardizing the privacy or the confidentiality of sensitive information.

For instance, Provenance is a blockchain-based application that allows for the tracking of the origin and the subsequent chain of custody of materials, from their source to their point of sale[21]. Provenance has already been used in the context of CPRs with a pilot using blockchain technology for tracing yellowfin and skipjack tuna fish in Indonesia from catch to consumer —thus contributing to guaranteeing the source of the fish and the sustainability of the production and commercialisation cycle. A more ad-

[1] Even if they do not add value in and of themselves, the establishment of these basic rules are necessary conditions for the proper implementation of the other rules.

vanced system could rely on a series of automated code-based rules to govern the interactions between the various actors involved in the supply chain, e.g. by specifying the conditions for the delivery of material and automating the rules that govern the corresponding payment to each relevant actor.

In short, the governance of CPRs could be achieved in a more decentralized manner by using a blockchain-based system as a common framework or infrastructure on top of which decentralized mechanisms of *ex-ante* automation and *ex-post* verification can be built. As such, blockchain technology could contribute to the proper implementation of a community's governance rules in a more efficient and cost-effective manner, while ensuring that such CPRs are well-managed and protected against human error and misconduct.

5 The Role of Oracles

While it can be used as a governance tool, a blockchain-based system cannot be the sole driver for the governance CPRs, it can only serve as a complement to an existing governance structure. In particular, in the context natural CPRs, much of the information is external and can only be properly accounted for by a blockchain-based system after it has been recorded onto the blockchain. This is generally achieved through the use of so-called "oracle" systems, specifically designed to provide real-world information to the relevant smart contracts.

As previously noted, a blockchain is a "confidence machine" [4] that does not, however, completely eliminate the need for trust. Using a blockchain-based system for *ex-ante* automation or *ex-post* verifiability only makes sense provided that the data recorded on the blockchain has been properly certified and authenticated by a trustworthy party This is commonly referred to as the problem of *garbage-in/garbage-out*, *i.e.* the reliability of a blockchain-based system only goes as far as the accuracy of the data it has been fed with.

One way to achieve a higher degree of accuracy for external data would be to require multiple oracles to provide the requested information and/or to request trusted third-parties (e.g. certification authorities, or community members with a particular reputation or authority) to validate the information provided via a multiple signatures (*multisig*) system[2]. In this way, the oracles would not be able to lie or provide false information to the blockchain (without the collusion of a majority of the oracles or verifiers).

Let us consider an example to illustrate this point. In order to preserve the atmosphere from excessive carbon emissions, the European Union (EU) has established an Emission Trading Scheme (EU-ETS) for exchanging CO_2 emission rights in the EU. In light of the high costs of monitoring and sanctioning in such an international arena, proposals have been made to implement such a carbon credit market onto a blockchain-based system [11], in order to benefit from more transparency and traceability, while automating the payment and transfer of deeds. However, this can only work if participants are confident that the permits they buy are legitimate and recognized by the EU. Hence, there is a need for a trusted authority (or *oracle*) responsible for issuing and assigning the original permits to the relevant actors. While this would require the approval of all participating countries, once such information has been provably recorded onto a blockchain, the automation and verification capabilities of the technology would allow for a more transparent and seamless carbon credits market.

6 Choice Levels and Implementation Challenges

Blockchains offer innovative solutions for the governance of CPRs. However, it is important to bear in mind that the use of blockchain technology also comes along with a set of technical constraints and risks. First of all, although blockchains are generally regarded as secure and tamper-proof databases, there remain many theoretical challenges to their resilience and integrity [13] Yet, in addi-

[2]A multi-sig system is one where multiple parties must sign off a particular transaction ifor it to be regarded as effective. They can be implemented on a variety of blockchains, with different conditions and restrictions.

tion to these technical challenges, blockchain technology also face a series of important governance challenges.

The IAD framework identifies three embedded levels of rules: *operational level* rules that govern day-to-day operations and decision-making procedures; *collective choice level* rules that determine how rules can be changed at the operational level, and *constitutional level* rules that stipulate how rules are made at the collective choice level[14].

The interplay between these different rules is an essential component of any governance system. In particular, Rahman *et al.*[22] note that most of the failures in the management of natural common-pool resources are often traced back to existing gaps in these inter-levels relationships. If a blockchain-based system were to be used for the governance of CPR at any of these three level, one would need to make sure that the system does not contribute to widening these gaps.

When introducing a blockchain based tool in the *action-situation*, it affects all three levels. Operational level rules could be codified into a smart contract to facilitate the automation of many routine processes and daily tasks. Governance rules to upgrade or modify the operations of a smart contract would instead fall into the category of collective choice level rules. Howell&Potgieter [9] insist that these must include cancellation and dispute resolution mechanisms in case of unforeseen problems.

Collective choice level rules are especially important in the context of a blockchain-based system, given that the codification of agreed-upon community rules into a formal language may not always reflect accurately the original intentions of the parties. Similarly, dispute resolution mechanisms could assume a crucial role in guaranteeing the legitimacy of such a blockchain-based system, in that they allow for community members to express their views on the interpretation of operational level rules, potentially proposing amendments and ideally reaching an agreement on a common interpretation of these rules. In our case, the constitutional level rules are those enshrined directly into the protocol of the blockchain network itself.

In the case of a widely used public blockchain (such as Bitcoin or Ethereum) the rules of the protocol are extremely difficult (although not impossible) to change. The *constitutional choice level* thus becomes much larger than the *action-situation*, leaving community members with little to no leverage on constitutional amendment. This stands in contrast with two of the Ostrom's 8 design principles, namely that "individuals affected by a resource regime shall be authorized to participate in making and modifying its rules" (DP3) and that "governance activities shall be organized in multiple nested layers" (DP8)[2]. Too big a discrepancy between the scales of the layers could cause the costs of relying on a blockchain exceding its benefits.

It is our belief that, rather than relying on a public blockchain, a consortium blockchain — collectively maintained and governed by all relevant stakeholders— could potentially serve as an ideal framework for implementing the community "social contract", while retaining the capacity to make modify the constitutional setting evolve in accordance with the community needs.

7 Conclusion

Drawing from Ostrom's Institutional Analysis and Development Framework, this paper has investigated the theoretical grounds for the use of blockchain-based system for the governance and management of CPRs.When it comes to guaranteeing compliance with community rules, the adoption of blockchain technology could let go of the traditional requirements of "monitoring and sanctioning" to embrace a new paradigm of *ex-ante* automation and *ex-post* verifiability. While this would not entirely eliminate the need for trust in the system, it could contribute to an enhanced governance of CPRs, by increasing the degree of confidence in the management of these resources, while simultaneously reducing the amount of policing efforts involved in the process.

Ostrom has shown that there are several examples of communities who have successfully managed to govern and maintain CPRs over time. Hence, we do not advocate for a systematic adoption of blockchain technology in that field. Yet, we argue that, in cases

where monitoring and sanctioning is either too hard or costly, and in cases where the lack of confidence and trust in governance has led to the poor management of CPRs, the adoption of a blockchain-based solution could prove useful. However, given the lack of empirical data on the matter, more research in needed to delineate the most favorable uses cases for experimentation and the best strategies for the implementations of such a solution.

References

[1] Nazli Cila, Gabriele Ferri, Martijn de Waal, Inte Gloerich, and Tara Karpinski. 2020. The Blockchain and the Commons: Dilemmas in the Design of Local Platforms. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. ACM, Honolulu HI USA, 1–14. https://doi.org/10.1145/3313831.3376660

[2] Michael Cox, Gwen Arnold, and Sergio Villamayor Tomás. 2010. A Review of Design Principles for Community-based Natural Resource Management. *Ecology and Society* 15, 4 (2010). https://doi.org/10.5751/ES-03704-150438

[3] Sue E. S. Crawford and Elinor Ostrom. 1995. A Grammar of Institutions. *American Political Science Review* 89, 3 (Sept. 1995), 582–600. https://doi.org/10.2307/2082975 Publisher: Cambridge University Press.

[4] Primavera De Filippi, Morshed Mannan, and Wessel Reijers. 2020. Blockchain as a confidence machine: The problem of trust & challenges of governance. *Technology in Society* 62 (Aug. 2020), 101284. https://doi.org/10.1016/j.techsoc.2020.101284

[5] Primavera De Filippi and Greg McMullen. 2018. Governance of Blockchain Systems: Governance of and by Distributed Infrastructure. *COALA* (June 2018), 40.

[6] Samer Hassan and Primavera De Filippi. 2017. The Expansion of Algorithmic Governance: From Code is Law to Law is Code. *Field Actions Science Reports. The journal of field actions* Special Issue 17 (Dec. 2017), 88–90. http://journals.openedition.org/factsreports/4518 Number: Special Issue 17 Publisher: Institut Veolia.

[7] Charlotte Hess and Elinor Ostrom. 2011. *Understanding knowledge as a commons: from theory to practice* (1st mit press pbk. ed ed.). MIT Press, Cambridge, Mass. OCLC: 731904330.

[8] Bronwyn E Howell and Petrus H. Potgieter. 2019. Governance of Blockchain and Distributed Ledger Technology Projects: a Common-Pool Resource View. (2019), 25.

[9] Bronwyn E. Howell and Petrus H. Potgieter. 2019. Governance of Smart Contracts in Blockchain Institutions. *SSRN Electronic Journal* (2019). https://doi.org/10.2139/ssrn.3423190

[10] Takashi Inoguchi. 2017. Theoretical Underpinnings of a Global Social Contract. In *Oxford Research Encyclopedia of Politics*.

[11] Khamila Nurul Khaqqi, Janusz J. Sikorski, Kunn Hadinoto, and Markus Kraft. 2018. Incorporating seller/buyer reputation-based system in blockchain-enabled emission trading application. *Applied Energy* 209 (Jan. 2018), 8–19. https://doi.org/10.1016/j.apenergy.2017.10.070

[12] Oleksii Konashevych. 2017. *The Concept of the Blockchain-Based Governing: Current Issues and General Vision*.

[13] Xiaoqi Li, Peng Jiang, Ting Chen, Xiapu Luo, and Qiaoyan Wen. 2020. A survey on the security of blockchain systems. *Future Generation Computer Systems* 107 (2020), 841–853.

[14] Michael D. McGinnis. 2011. An Introduction to IAD and the Language of the Ostrom

Workshop: A Simple Guide to a Complex Framework: McGinnis: IAD Guide. *Policy Studies Journal* 39, 1 (Feb. 2011), 169–183. https://doi.org/10.1111/j.1541-0072.2010.00401.x

[15] Satoshi Nakamoto. 2008. Bitcoin: A peer-to-peer electronic cash system. (2008).

[16] Elinor Ostrom. 1990. *Governing the commons: the evolution of institutions for collective action*. Cambridge University Press, Cambridge ; New York.

[17] Elinor Ostrom. 2000. Collective action and the evolution of social norms. *Journal of economic perspectives* 14, 3 (2000), 137–158.

[18] Elinor Ostrom. 2005. *Understanding institutional diversity*. Princeton Univ. Press, Princeton, NJ. OCLC: 254160820.

[19] Elinor Ostrom. 2010. Beyond Markets and States: Polycentric Governance of Complex Economic Systems. *The American Economic Review* 100, 3 (2010), 641–672. https://www.jstor.org/stable/27871226 tex.ids: noauthor_no_nodate publisher: American Economic Association.

[20] Elinor Ostrom, Roy Gardner, and Jimmy Walker. 1994. *Rules, Games, and Common-Pool Resources*. The University of Michigan Press, Ann Arbor.

[21] Provenance. 2015. Blockchain: The Solution for Transparency in Product Supply Chains.

[22] H. M. Rahman, Arlette Saint Ville, Andrew Song, June Po, Elsa Berthet, Jeremy Brammer, Nicolas Brunet, Lingaraj Jayaprakash, Kristen Lowitt, Archi Rastogi, Graeme Reed, and Gordon Hickey. 2017. A framework for analyzing institutional gaps in natural resource governance. *International Journal of the Commons* 11, 2 (2017), 823–853. https://doi.org/10.18352/ijc.758 Number: 2.

[23] Wessel Reijers, Iris Wuisman, Morshed Mannan, and Primavera De Filippi. 2018. Now the Code Runs Itself: On-Chain and Off-Chain Governance of Blockchain Technologies. *Innovation Finance and Accounting eJournal* (2018).

[24] David Rozas, Antonio Tenorio-Fornés, Silvia Díaz-Molina, and Samer Hassan. 2018. When Ostrom Meets Blockchain: Exploring the Potentials of Blockchain for Commons Governance. *SSRN Electronic Journal* (2018). https://doi.org/10.2139/ssrn.3272329

[25] Nick Szabo. 1997. Formalizing and securing relationships on public networks. *First Monday* (1997).

[26] D. Vujičić, D. Jagodić, and S. Randjić. 2018. Blockchain technology, bitcoin, and Ethereum: A brief overview. In *2018 17th International Symposium INFOTEH-JAHORINA (INFOTEH)*. 1–6.

[27] Kevin Werbach. 2017. *Trust, But Verify: Why the Blockchain Needs the Law*. SSRN Scholarly Paper ID 2844409. Social Science Research Network, Rochester, NY. https://papers.ssrn.com/abstract=2844409

[28] Dylan Yaga, Peter Mell, Nik Roby, and Karen Scarfone. 2018. Blockchain Technology Overview. *arXiv:1906.11078 [cs]* (Oct. 2018), NIST IR 8202. https://doi.org/10.6028/NIST.IR.8202 arXiv:1906.11078 [cs] Comment: 68 pages, National Institute of Standards and Technology Internal Report.