Université Panthéon - Assas

École doctorale d'Économie, Gestion, Information et Communication (ED455)

Thèse de doctorat en Économie

Soutenue le 18 Octobre 2022

Blockchain and Collective Choice

Blockchains, Governance and the Commons

Philémon Poux

Sous la direction de Bruno Deffains & Primavera de Filippi

Membres du jury :
Pr. Grazia Cecere, Rapporteur
Pr. Yassine Lefouili, Rapporteur
Pr. Balázs Bodó
Pr. Jason Potts
Pr. David Rozas

Avertissement

Remerciements

Ma thèse fut, assurément, une épreuve psychologique autant qu'académique. Comme de nombreux · ses doctorant · es, j'ai dû faire face à des doutes, qui ont pu paraître parfois insurmontables, à la crainte de ne pas être en mesure de compléter ce travail dans le temps imparti, et à des questionnements sur l'intérêt du projet. Si je peux aujourd'hui apporter les dernières touches à mon manuscrit c'est que j'ai eu la chance d'être merveilleusement entouré dans les bons et les moins bons moments qui ont constitué ces trois dernières années.

Tout d'abord par Primavera et Bruno, directeur · ices attentioné · es et complémentaires. Primavera, dès notre première rencontre pour discuter d'une potentielle collaboration, m'a fait bénéficier de sa formidable capacité d'analyse et d'organisation conceptuelle. Il m'est régulièrement arrivé d'aller la voir avec des idées un peu brouillonnes et de ressortir de son bureau avec une approche structurée et cohérente. Primavera a aussi constamment cherché à me faire rencontrer et collaborer avec d'autres chercheur · et, compte tenu du risque de solitude en thèse, je lui en suis profondément reconnaissant. Bruno, de son côté, a tout de suite eu la gentillesse de me consacrer du temps de et l'attention alors que notre collaboration aurait pu n'être qu'administrative. Mon approche de l'économie institutionnelle doit beaucoup à nos échanges, toujours enrichissants, qui ont rapidement donné lieu à une amitié. Son soutien et ses encouragements dans les moments de doutes ont rendu ceux-ci moins longs et m'ont permis à plusieurs reprises de surmonter blocages et stagnations. Je souhaite leur témoigner ma profonde reconnaissance d'avoir accepté de m'accompagner et de m'avoir guidé dans ce travail avec exigence et bienveillance. Thomas Perroud m'aura également été d'une grande aide lors de mon inscription et je l'en remercie.

Le CERSA, tout d'abord, m'a ouvert ses portes et je m'y suis immédiatement senti chez moi grâce à l'ambiance joviale qui y règne. J'ai notamment une pensée pour Natacha Gally et Julie Bailleux qui m'ont prodigué nombre de conseils avec beaucoup d'attention et de gentillesse ainsi que pour Yves Surel pour son accueil dans le laboratoire. La facilité avec laquelle j'ai pu commencer ma thèse doit énormément à la "Team Surel" (et affilié · es)—Anne-Laure, Agathe, Anthony, Jonas, Maximilien, Julie, Thomas, Marie, Pauline et Fanny—qui a eu la gentillesse de m'accueillir en son sein. Au CRED, je me suis immédiatement intégré au petit groupe constitué de Marie-Noëlle, Noé et Eddy. Nous avons partagé d'innombrables cafés et repas, à discuter de nos recherches (parfois), de nos vies personnelles (plus souvent) et surtout à nous soutenir mutuellement et à partager l'expérience unique de la thèse. Notre quatuor s'est ensuite étoffé, notamment avec Yann et Illan, qui m'ont fait profiter de leur intelligence et de leur gentillesse lors de ma dernière année de thèse. Le CRED, ensuite, fut également l'occasion pour moi de rencontrer Étienne Lehmann et Quentin Lippmann qui dont l'expérience et l'amitié me furent précieuses. Je souhaite aussi remercier Claudine Desrieux et Marie Obidzinski pour la confiance qu'elles m'ont accordé, Naima Baba-Aissa pour son aide toujours efficace et bienveillante et tous les autres membres du laboratoire, doctorant · es, chercheur · euses et personnel administratif pour nos échanges réguliers qui contribuent à faire du CRED un lieu de travail si agréable.

Le séjour de Tara Merk a Paris m'a permis de me faire une formidable amie, que je remercie vivement pour sa relecture d'une partie du manuscrit, et de largement compléter ma compréhension de l'environnement blockchain. L'arrivée de Sofía Cossar et de Jamilya Kamalova nous a permis de former un petit groupe de travail amical à qui je dois beaucoup, humainement et académiquement. Enfin, Simona Ramos est bien plus qu'une coautrice, je la remercie tout particulièrement pour son accueil à Barcelone et les parties de beachvolley.

Au-delà du cadre professionnel, je veux surtout témoigner mon affection à toutes les personnes qui m'entourent et avec lesquelles je partage tant. Au moment de finaliser mon travail, j'ai d'abord une pensée pour mes ami · es en thèse. Nos échanges réguliers ont permis de construire une expérience partagée et de dépasser les moments les plus durs. La compréhension et le soin que nous avons mutuellement les un · es pour les autres sont inestimables. Je veux aussi exprimer tout mon amour pour Ballek. Ce groupe, toujours présent et attentif, disponible au moindre coup de mou pour se retrouver, faire des heures de belotes, des mots croisés ou des 51 endiablés lors de séjours mémorables ou de soirées plus calmes est un pilier sur lequel je compte énormément. C'est également le cas pour les Biloutes de Paris, et les HX3 en général, soutiens indéfectibles et ami · es pour toujours. Le bonheur de voir nos liens se renforcer par nos proximités, nos projets, nos moments partagés et nos vacances, désormais traditionnelles, est indescriptible.

Je n'ai que tendresse pour les autres personnes que je vois au quotidien ou plus rarement mais qui rythment ma vie. Je pense notamment à Samuel, Matthieu, Alexis, Pierre, Marguerite dont la relecture m'a été si utile, Philou, Loulou, Théotime et Maya. Mes cousin · es sont aussi de ce nombre. Présences indispensables à mon équilibre, iels savent combien iels comptent pour moi et je pense, avec un large sourire, aux bout'chous qui ont récemment élargi nos déjà grandes familles.

Je veux remercier Ulysse pour avoir permis de faire du Domaine des Deux Ânes bien plus qu'un appartement, un foyer. Ce que nous y avons créé est inestimable, un lieu de rencontre, de partage et le socle d'une amitié qui est devenue bien plus que ça. Je lui suis reconnaissant de ses attentions, son humour et son regard qui m'a souvent aidé à prendre du recul.

Mon autre foyer reste celui de mes parents. Leur amour, leurs conseils et leurs attentions ne m'ont pas quitté. Leur aide (et leurs repas !) lors de la dernière semaine de rédaction fut le meilleur exemple de leur soutien sans faille, qui, évidemment, va bien au-delà de cette thèse. Iels savent l'amour que je leur porte et tout ce que je leur dois. Je leur dois notamment mon frère César, la personne dont je suis le plus proche depuis si longtemps. Je le remercie bien sûr pour ses commentaires et son travail de relecture assidu : je lui suis redevable de beaucoup, dans tout mon parcours académique. Mais c'est tout le reste,

les discussions sur tout et rien, les parties de spikeball, les concerts partagés et j'en passe, qui me vient à l'esprit pour évoquer la richesse de notre relation. Il reste la personne vers laquelle je me tourne, spontanément, dès que j'en ressens le besoin.

Enfin, Matilda sait tout l'amour que je lui porte. Elle m'accompagne depuis deux et contribue à mon bonheur quotidien. Sa présence à mes côtés dans les joies et aussi dans les moments les plus durs, sa finesse et sa tendresse me sont indispensables. Elle m'a encouragé à parler de mes angoisses et craintes pour m'aider à les dépasser et a toujours su me guider hors des impasses dans lesquelles je me trouvais. Fort heureusement, notre relation est surtout faite sur des moments bien plus gais et j'ai hâte de ceux qui sont à venir. Je suis chanceux de pédaler à ses côtés pour les vivre.

Résumé :

Dans cette thèse, j'utilise le cadre conceptuel de l'économie politique et institutionnelle pour analyser le choix collectif et l'établissement de constitutions, c'est-à-dire l'ensemble des règles pour décider des règles, dans les communautés blockchain. J'adopte une double approche avec, d'une part, l'utilisation de la théorie économique classique pour évaluer le processus de gouvernance dans les communautés rassemblées autour d'une blockchain (gouverner la blockchain) et, d'autre part, l'identification de la façon dont les innovations permises par les blockchains peuvent être utilisées pour améliorer la coopération dans les groupes (gouverner avec une blockchain). Ces directions se nourrissent mutuellement : à mesure que nous comprenons mieux les spécificités de la gouvernance des blockchains, nous découvrons dans quelle mesure elles peuvent à leur tour être utilisées pour la gouvernance de ressources partagées dans différents contextes. La principale question abordée dans ce manuscrit est de savoir comment les blockchains peuvent être utilisées pour gouverner des biens Communs.

Le manuscrit est composé de cinq chapitres. Il commence par une revue de littérature discutant les notions mobilisées dans l'ensemble de ma recherche et présente ensuite les quatre articles écrits durant ma thèse. Le premier propose une réponse basée sur les communs au problème actuel de la MEV (Maximal Extractable Value) dans les blockchains telles qu'Ethereum. Il conceptualise la MEV comme une nouvelle forme de *free-riding* et explore comment la théorie des biens Communs éclaire les solutions futures pour faire face à ce problme. Le deuxième propose une analyse économique (de type Public Choice) de la démocratie liquide et des enjeux associés à une mise en œuvre basée sur la blockchain. Il se concentre en particulier sur les questions d'échelle et conclut que la démocratie liquide peut être pertinente pour de petites communautés homogènes, mais qu'elle ne peut représenter l'intensité des préférences et n'est donc pas adaptée aux grandes communautés. Le troisième article s'interroge sur les changements paradigmatiques qu'implique une gouvernance des Communs basée sur la blockchain, notamment en raison de l'automatisation et de la transparence. Le quatrième article complète ce travail en s'appuyant sur deux articles de recherche fondamentale sur la gouvernance des biens communs basée sur la blockchain et propose un cadre unifié, reposant sur le cadre d'analyse institutionnelle et de développement (Institutional Analysis and Development Framework, IAD) d'Ostrom dans un nouveau contexte technologique. Une étude de cas fictive des biens communs fonciers au Ghana est proposé pour illustrer comment cette IAD améliorée par la blockchain pourrait être utilisée.

Ces quatre articles forment un corpus qui montre que si les blockchains sont un outil puissant pour garantir une certaine confiance dans les opérations quotidiennes de gouvernance d'une ressource, il ne faut pas ignorer les dynamiques en œuvre lorsque ces règles doivent être modifiées. Cela alimente une relation à double sens : les blockchains peuvent introduire la confiance dans des environnement qui en sont dépourvus mais, dans le même temps, elles ont besoin de l'implication de la communauté, de sa confiance et de ses normes pour faire face à aux évolutions du système.

Descripteurs :

Communs, Blockchain, Choix Collectif, DAO, Economie Politique

Abstract:

In this dissertation I use methodologies from political and institutional economics to analyze collective choice and constitutional setting in blockchain communities. I adopt back-and-forth process between using classical theory to evaluate governance processes in communities gathered around a blockchain (governing the blockchain) and identifying how blockchains' innovations can be channeled to enhance cooperation in groups (governing with a blockchain). These two directions feed on one another: as we better understand the details of blockchain governance we uncover how they may in turn be used to address existing governance challenges in different contexts and complement existing theories, often developed in a different technological context. The main issue addressed in this manuscript is how blockchains can be channeled to govern Common-Pool Resources.

The dissertation is comprised of five chapters. It starts with an extensive literature review surveying the concepts mobilized throughout the manuscript before presenting four papers. The first paper proposes a Commons-based approach to the current issue of MEV (Maximal Extractable Value) in blockchains such as Ethereum. It conceptualizes MEV as a new form of free-riding and explores how the theory of the Commons can inform future solutions. The second paper discusses the economics of Liquid Democracy and the challenges associated with a blockchain-based implementation. It particularly focuses on the issue of scale and concludes that Liquid Democracy may be relevant to small homogeneous communities but fails to account for the intensity of preferences and henceforth is not suited to larger communities. The third paper questions the paradigmatic changes entailed by blockchain-based governance of the Commons, in particular due to automation and transparency. This work is completed in the fourth paper that builds on two foundational research papers on blockchain-based governance of the Commons and proposes a unified framework that methodologically reassesses Ostrom's Institutional Analysis and Development (IAD) framework in a new technological context. A fictitious case-study of land Commons in Ghana is provided to illustrate how this blockchain-enhanced IAD could be used

These four papers form a corpus contributing to analyzing the collective choice process of blockchain-enabled communities. It demonstrates that while blockchains are a powerful tool to provide confidence in the day-to-day operations for the governance of a resource, we cannot afford to ignore the dynamics at play when these rules need to be amended. In these cases, trust and off-chain social conventions regain prominence. This fuels a two-way relationship: blockchains can introduce confidence in trust deprived contexts but, conversely, they need this community involvement and rely and its norms to deal with a changing environment.

Keywords:

Commons, Blockchains, Collective Choice, DAO, Political Economy

Table of Contents

General Introduction

General Introduction

The mutual relationship between technology and social groups dynamics is now well documented (Quan-Haase, 2020; Williams and Edge, 1996). Technology influences on how social groups form, interact and coordinate between themselves. In turn, social norms and structures shape technological development. For instance, technology can ease communication, reduce distances and thus allow for large scale communities to collaborate much more easily. Thirty-five years ago, the advent of the Internet revolutionized cooperation, providing digital tools for communication across the world. Not only has this led to the development of online communities such as blogs and forums but it has also changed the way already existing groups were structured. This change was made even more radical by the development of Web 2.0, social media, instant communication and increasingly complex platform services.

The most recent step in this development of digital coordination tools happened in 2009. Bitcoin, the first-ever blockchain, was created to allow "two willing parties to transact directly with each other without the need for a trusted third party" (Nakamoto, 2008). The groundbreaking innovation of Bitcoin was to provide a way for a decentralized network, made of mutually distrusting nodes, to agree on the state of a financial ledger, akin to double-entry bookkeeping. Until then, no solution had been available to prevent a malicious node to broadcast duplicated transactions, what is often referred to as double-spending. Essentially, a blockchain is a mechanism to ensure consensus in a peer-to-peer (p2p) network.

This thesis presents my research dedicated to discerning how this technical innovation has become a coordination and social one and the new institutional arrangements it allows for. As blockchains now permeate virtually every aspect of our societies that project is too daunting for one person to conduct. My work only focuses on the coordination mechanisms and the constitutional settings for small to medium communities, specifically around the management of the Commons. In particular I have set to understand how such communities can leverage blockchains to coordinate action, facilitate decision-making and enable new forms of constitutional environment. This manuscript presents the main findings of this research. To understand the context of these considerations, it starts with a general introduction that lays out the different fields necessary to grasp this intrinsically multidisciplinary topic. This then leads to the presentation of the original research methods and results.

Blockchain technology and the tools it supports

Created in the wake of the 2008 financial crisis that evidenced how centralized institutions could fail at regulation, Bitcoin was designed to enable digital currencies transactions in a decentralized way avoiding single points of failures. All the transactions are broadcasted to the whole network and this transparency ensures that every node contains a copy of the whole history of the chain. Stored data cannot be removed or edited which is why blockchains are called append-only ledgers. More specifically, the blockchain is made of a single chain of blocks, connected linearly to one another. Each block contains some data (a certain number of transactions for instance) and a reference to the previous block that, in turn, also has a reference to the previous block. That way, modifying an older block changes all the blocks that come after and it is only possible to add data to the chain but not to modify it. The name "blockchain" naturally derives from this database structure.

Because blockchains, were originally designed to support financial transactions, it was paramount that they were highly tamperproof. Notably, the whole conception of the blockchains was made under the assumption that competing nodes would try to maximize their profits. The mechanism design thus relies on competition between the different nodes to achieve an equilibrium. Contrary to centralized databases, the consistency and quality of the data on blockchains is not guaranteed by the reputation or the trust in the institution hosting the data but rather by the economic incentive of the others. By doing so, blockchain systems have managed to replace trust in institutions by rational expectations about economic behavior. This confidence in the outcome of the system is reinforced by cryptographic mechanisms that secure the data with a very high degree of certainty.

But this decentralization raises many coordination challenges, notably in a digital context in which pseudonymity makes accountability difficult. Blockchains propose a tool based on algorithmic and cryptographic technologies and the opportunities they offer reach beyond monetary transactions. Although Bitcoin only allows for the transfer of bitcoins (the currency),[1] the blockchain technology underlying the network can be used to build consensus on virtually any database. Upon this realization, new blockchains were created in the mid 2010s to make the best of this invention. These new blockchains, such as Ethereum, permit not only to record modification on database but also to execute snippets of code, called smart-contracts. All the nodes participating in the network run the same program with the same inputs resulting in the same output. On top of providing a tamperproof decentralized consensus mechanism, new generation blockchains are also the substrate for decentralized computing and automation, creating a whole ecosystem relying

[1] Bitcoin with a capital "B" refers to the blockchain while a lowercase "b" refers to the cryptocurrency.

on conditional transactions and contracting.

Over the last years, the number of smart-contracts deployed on blockchains has increased exponentially and the ecosystem of services that can be accessed is extremely rich. While the majority concerns financial transactions in Decentralized Finance (DeFi), smart-contracts are not limited to it. In fact, the scope of application is widening and a specific type of smart-contracts is of particular interest: Decentralized Autonomous Organizations (DAOs). Made of several interrelated smart-contracts, a "DAO is a blockchain-based system that enables people to coordinate and govern themselves mediated by a set of self-executing rules deployed on a public blockchain, and whose governance is decentralized (i.e., independent from central control)" (Hassan and De Filippi (2021)). The field of DAOs applications range from the management of a private investment fund to crowd-funding of public goods. Decision-making tools such as voting platforms or ways to submit propositions are often implemented within the DAO.

Contrary to other types of smart-contracts, DAOs are really community oriented and are defined as much by the characteristics of its members as by its code. DAOs benefit from the features of the blockchains such as automation, independence from third party, transparency and auditability. Automation and auditability bring certainty in the outcome of the decision-making process and may increase confidence in the system. Although the structure of the community using the DAO does not have to be decentralized, the underlying infrastructure is, and therefore the only centralized aspects that the community has to deal with are those it chooses.

Considering that blockchains are a relatively recent technology, the related academic literature is already well-developed. On top of burgeoning research in computer sciences advancing the knowledge around blockchains and contributing to their development, virtually every other field has addressed the question of blockchains. This illustrates how this technology, called a "new institutional technology" (Davidson et al. (2016a)) has the potential to change practices spanning across many sectors of the society. However, many scholars and practitioners first discussed the extent of blockchain applications in a way that mostly mimicked what already existed elsewhere or, as Davidson et al. (2018) put it, doing "X, but on the blockchain". This approach misses the key innovations of blockchains and fails to address the important question of how using such a specific network structurally alters how people interact.

Researching blockchain(-based) governance

This latter question opened new fields of research, intrinsically cross-disciplinary as blockchains are algorithmic systems based on economic incentives and game theory to allow a community to transact. Among the most important issues addressed are the ones that concern the governance of blockchains (the substrate) and blockchain-based tools (such as DAOs) that are deployed on that substrate. These questions are related but distinct. Because of its decentralized nature, the governance is also decentralized. Changes to the core protocol require majority adoption and discussion of stakeholders to devise strategic orientations frequently happen both formally and informally. Research has demonstrated how entrenched *on-chain* and *off-chain* governance networks were. The former refers to the mechanisms included in the blockchain code itself, to amend its protocol, while the latter refers to all the processes happening outside of the blockchains, either online (through discord chats, forums, blogposts...) or in real life (at conferences for instance).

Describing and understanding the governance of blockchains requires having a precise depiction of the different actors at play and of their institutional environment. In particular, blockchains require some users, called miners, to engage in a lottery process to create the blocks that will be added to the blockchain. The process for mining the new blocks and the specificities of the lottery differs depending on the blockchain but, generally speaking, the miners incur some costs to propose new blocks to the network and are rewarded when their blocks are chosen among the others. Miners are a very important set of actors of the blockchain network because they are responsible for keeping it active. The rewards are made to incentivize as many actors as possible to engage in mining blocks because the resilience of the blockchain relies on the decentralization and competition among the miners. The blockchain community is also comprised of programmers who write and update the code of the blockchain to address potential issues (however, update is only effective if most miners implement it as I will show below). Among them are the creators of the blockchains who often remain involved in the community and may be quite influential in the directions that the blockchain takes (with the notable exception of Nakamoto, the creator of Bitcoin). Some blockchains also have specific roles that are coded on-chain. Examples include validating the blocks proposed by miners or acting as custodians of the network. Finally, most blockchains users do not try to mine but only use the blockchains to exchange with others, using blockchains as a platform for a service (for sending money for instance). Research on blockchain governance maps, for each specific blockchains, the power dynamics, the rules, the habits and the relationships of these different sets of users, including the influence of external factors such as legislators.

This work on the governance of the blockchain network has been extended to the analysis of the governance of smart-contracts, DAOs and other blockchain-based applications that rely on this substrate. Because they depend on how the blockchain works, they may be directly impacted by any changes made to the core blockchain protocol but their governance also faces challenges of their own. The central part of this research is the interplay between the digital tool on the one hand, largely automated and relying on algorithmic constraints and the human community using it on the other hand. This dual nature of the blockchain is found at every level (also called layers) of the blockchain world.

This, in itself, is already a non-trivial result as blockchains are often presented as a technology disintermediating human agency. Not only is this a simplistic approach to what blockchains are but this approach also fails to see how blockchains can be used to enhance cooperation and coordination between individuals. The articulation between these two sides of the governance is complex as the community writes and oversees changes to the code of the DAO and the structure of the community is shaped by the code and what it allows.

A seminal aspect of this entanglement is the role of tokens. A token is a sort of digital asset associated with an address—essentially an account on the blockchain. The most common and famous type of tokens are cryptocurrencies, fungible and transferable tokens. Other tokens are non-fungible and form the category of Non-Fungible Tokens (NFTs) which became rather famous recently; non-transferable tokens or tokens that disappear under certain conditions can all be coded on the blockchain. Most of the interactions on the blockchain world rely, in a way or another, on tokens. This has led to the formation of the word tokenomics, which can be broadly defined as follow: "Tokenomics encompasses the concept of economic system and optimization design to incentivize specific behaviors in a community, using tokens to create a self-sustaining ad hoc economy. It includes game theory, mechanism design, and monetary economics" (Lamberty et al., 2020).

When creating a DAO, coders have to consider of the tokenomics that will underly its governance. There is a back-and-forth process where the mechanism design is conceptualized off-chain, implemented on-chain and then informs the off-chain governance. Tokens can be used to vote, can be earned through participation to the maintenance of the DAO or collectively attributed... The possibilities are endless and are what make blockchain-based tools so promising.

Research on blockchain governance must then take into account tokenomics but also the social specificities of the communities they study. Motivations to use a blockchain-based tool can be quite different depending on the actors. While some want to retain a rather centralized control over the smart-contracts, other explore the world of digital decentralized governance and make the best of the particularities of the blockchains. In that regard, it is important to dedicate detailed attention to the community and how using a blockchain-based tool structures it. Depending on whether the group existed before becoming a DAO or if they formed around the digital tool, the expectations and relationships will be very different.

Another pivotal aspect of the governance of a DAO is the legal context and the broader environment in which the community members live in real life. Because the nodes running the blockchains are distributed between different countries, because the users are anonymous and because sanctioning on-chain may be unfeasible, it is practically impossible to regulate the blockchain itself. However, legislators can still hold users (at least those identified) accountable for some of their actions. For instance, with the boom of DeFi, some financial authorities consider certain tokens as equivalent to financial securities and thus subject to legislation. While monitoring may be difficult, users still face legal sanctions.

They may thus want to influence the development of the DAOs they are engaged in to be in accordance with one legislation or another thus shaping the code and the practices of the DAO. Other less formal norms may also be important to understand how the community reaches an agreement. Blockchain users have their own codes and manners that inform what is expected of others and what is considered legitimate.

Research on blockchain governance needs to examine the economic, technical and social aspects of the DAO in order to dissect the system they study. An interesting outcome of this research concerns blockchain constitutionalism and demonstrates that agreeing on the use of a DAO can sometimes be akin to agreeing on a constitution. While “code is law” (Lessig, 2006), how these laws evolve is decided at a meta level, that can be considered constitutional. This conceptualization also gives scholars an actionable framework to study DAOs. While the most obvious might be law and legal philosophy, economics has historically been able to describe and analyze constitutional processes.

The input of institutional economics and the theory of the Commons

Constitutional economics, a branch of public economics, is dedicated to applying economic methods to describe how people set up the rules of the community they live in, specifically the constitutional process. The foundational book on this matter is *The Calculus of Consent* by Buchanan and Tullock (1962), in which they laid the cornerstones for most of the following Institutional Economics literature devoted to collective choice. This strand became known as Public Choice. Focusing more on the process of reaching agreement rather than on the outcome of the collective choice, this theory seems naturally fitted to the study of blockchain-based communities: both blockchain game theory and Public Choice make the assumption of rational agents agreeing on a consensus. Conceptually, this all relies on a contractual approach in which agents engage in a negotiation relationship before formalizing the terms in a contract. Although blockchains remove the possibility to default and thus reduce the inherent risks of a contract, these economic methods remain relevant to analyze the behavior of blockchains’ users.

The scope of Institutional Economics (including Public Choice) is extremely large and it provides us with instruments to study different aspects of the blockchain community, both at the infrastructure (the blockchain itself) and at the application (DAOs) level. For instance, decentralization induces polycentricity with interdependent nested levels of governance. Institutional Economics also provides us with methods to understand and analyze polycentric governance, notably through the work of the Vincent and Elinor Ostrom. Researching various subjects, they have developed analytical frameworks for the study of institutions in multi-scale contexts. Throughout the manuscript, I adopt the definition of institution of E. Ostrom and Hess (2007). They

> define institutions as formal and informal rules that are understood and used by a community. Institutions [...] are not automatically what is written in

> formal rules. They are the rules that establish the working "do's and don'ts" for the individuals in the situation that a scholar wishes to analyze and explain. (p.42)

The work of Elinor Ostrom was especially focused of Common-Pool Resources (CPR), traditionally defined as rival and non-excludable goods: they can be over-exploited and it is costly to prevent people from extracting the resource. These goods are also referred to as Commons, and will be written with an *s* and a capital *C* throughout the manuscript.[2] These CPRs thus face the challenge of addressing the threat of depletion in a multi-stakeholder context. Elinor Ostrom spent her life demonstrating how governance processes made it possible for communities to solve this issue. In doing so she developed tools, accessible to scholars and practitioners, to understand key features of successful stewardship of CPRs. Her work was later extended by numerous scholars, forming the Bloomington School. They continue to contribute to a better understanding of empirical governance practices found across various communities and extend the theory underpinning the analysis of these practices.

Among them, Bollier (2014) emphasized the role of the community members, commoners and of their active participation in governing the resource, forging the word "commoning". According to him, a Commons is a three-pronged system comprised of a resource, a community of commoners and a set of rules decided by the community to govern the resource and prevent its depletion. Generally speaking, Commons face the risk of free-riding practices where some people exploit the resource without contributing to its maintenance. The rules of the Commons and active commoning allows the commoners to address this challenge, either by reducing/suppressing free-riding opportunities or by reducing their consequences.

Blockchains and the theory of the Commons

The theory of the Commons is relevant to blockchain-based communities because they share many characteristics with the groups studied by Ostrom. In the later part of her life, she concentrated on Knowledge Commons, immaterial resources produced and managed by a community. Unlike natural resources Commons, Knowledge Commons, such as Wikipedia, do not face the risk of depletion but rather of underprovision. In both cases, the challenge lays in coordinating community members to avoid opportunistic behaviors and favor sustainability. Blockchains are an example of such Knowledge Commons, specifically Community-Based Peer Produced (CBPP) Commons. CBPP are resources for which the value derives from information produced in a peer-to-peer network. This indicates that Ostrom's methodology can be applied to examine blockchains and its communities. It

[2]This practice is inspired by Le Roy (2016) who uses it to disambiguate them from the noun commons (plural) and indicate clearly that even with an s, a Commons may be singular. When quoting other authors or referring to a specific concept, I will keep the original typography.

helps analysts to identify which aspects of the collectively decided upon set of rules to look at. They include the boundaries of the community, the different roles in the community, the scope of possible actions, potential sanctions but also what formal and informal rules preside over dispute resolution. It results in a fine-grained depiction of the governance process. This analytical work can be of use to the community in case of crisis in the management of an existing resource or at the design stage of a new CPR.

This aspect is particularly interesting. Indeed, analysis of blockchain-based Commons not only allows to better understand them but, conversely, allows to flesh out the theory of the Commons and adapt it to the specificities of blockchain-based governance, namely automation, decentralization and transparency. This enriched version can then be mobilized to design blockchain-enabled governance.

It is all the more important to have a detailed understanding of how governance may pan out that there are increasingly more DAOs that aim at funding, promoting and managing public goods or CBPP resources. The most famous example might be Gitcoin, a crowdfunding platform dedicated to digital public goods. While most of them are still at a relatively early stage, they benefit from the growth of blockchains and have substantial financial power (mostly through their link with DeFi). They thus have quite far-reaching agency and it is critical that both practice and theoretical research advance hand in hand to maximize the chances that the governance will be successful.

Among the subjects that still require further research is the relationship between blockchain-based decision-making tools and off-chain resources. Automating decisions on the blockchain is easy but enforcing decisions made on-chain on an off-chain system and then validating external data that needs to be recorded is not and brings many challenges. Many are situation-dependent but theoretical analysis can identify the general types of issues that may arise and present potential solutions.

Blockchain-based governance can be analyzed through the following three questions: (i) *why* to use blockchains; (ii) *how* to use them; and (iii) *when* is it relevant to have recourse to a blockchain, that is to say, the conditions favorable for application.. I have already hinted as to why it is natural to consider blockchain-based tools for the governance of public and Commons resources. Blockchains (as infrastructures and the applications it supports) cannot be separated from the question of governance and they offer new opportunities that should not be neglected. Knowledge of how to design and implement blockchain-based governance has been supported by academic research along with hands-on innovation in DAOs. This has allowed to partly address the questions (i) and (ii). Yet, the question (iii) while having received quite some attention recently, is still open.

While the answer may be straightforward for digital resources, and even more so for the *on-chain* ones, it is much more complex in the cases where there is not such an obvious relationship between the resource and the blockchain world. In these cases, introducing an instrument such as a DAO into an already intricate governance system may cause more problems than what it may solve. It may, for example, induce power asymmetry between those capable of understanding, designing and using the DAO and those who cannot. Attention to the power dynamics created by resorting to a blockchain-enabled governance process is of particular importance, and preferably prior to implementation to avoid harmful consequences.

Methodology and scope

The research that I present in this dissertation furthers this two-way relationship between economic theories and blockchain(-based) governance. Throughout the last three years, I have engaged in a back-and-forth process between using classical theory to evaluate governance processes in communities gathered around a blockchain (governing the blockchain) and identifying how blockchains' innovations can be channeled to enhance cooperation in groups (governing with a blockchain). These two directions feed on one another: as we better understand the details of blockchain governance we uncover how they may in turn be used to address existing governance challenges in different contexts and complement existing theories, often developed in a different technological context. This approach has led me to focus on the question of collective choice and, specifically although not exclusively, in the context of the Commons. Using economic methods from different strands of institutional economics and in particular Public Choice constitutional economics and E. Ostrom's Institutional Analysis and Development Framework, I have been able to illustrate how communities may leverage blockchains to coordinate action, facilitate decision-making and enable new forms of constitutional rules. The specificity of my work has been to concentrate on natural resources and to describe how the introduction of blockchain-based tool may facilitate coordination (either participation in elections or governance of a Commons).

This research has been carried out in the context of the BlockchainGov research group, dedicated to studying on-chain and off-chain governance and identifying the ways to support decentralization in governance *of* and *with* blockchains. As I mainly adopt a Commons-based approach in this dissertation, it must be apprehended within this broader context, and be linked with the other contributions of the group. They include work on legal theory of blockchain-based systems, empirical studies and experimentations, work on polycentricity and constitutionalism or on-chain digital identities... While discussed to a lesser extent in my research, these questions are closely related to mine and are a testimony to the interdisciplinary nature of blockchain governance research.

Plan of the manuscript

To situate my methodology in this multidisciplinary context, the manuscript starts with an extensive literature review followed by four papers published or submitted to peer-reviewed journals and to one conference.

The Literature Review provides an overarching discussion of the links between political economy and blockchain systems. Where each paper discusses some specific questions applied to blockchain governance, this chapter situates these different questions with regards to the broader question at play. It starts by giving a rather detailed description of how blockchains and DAOs works in order for every interested reader to comprehend the whole manuscript. It then presents an overview of how the branch of political economy developed tools and methodologies to analyze collective choice for groups. An exhaustive introduction to political economy requires a full handbook and I have selected the theory related to the issue of collective decision-making and how to coordinate to avoid free-riders. The theory of Commons is also reviewed at length. The main contribution of this chapter is to offer an overview of the state of the art literature linking political economy and blockchain(-based) governance. A dozen of papers have already laid the foundations for this rich research methodology. Comparing and discussing their conclusions outlines opened questions for further research. In particular, I carefully criticize existing literature on a Commons-based approach to blockchain(-based) governance to outline how the four papers this complement it and answer opened questions.

The first one, coauthored with Primavera de Filippi and Bruno Deffains, is entitled *MEV or the Tragedy of the Blockchains Commons*. It discusses the issue of Maximal Extractable Value (MEV), a practice that enables certain actors on the blockchain and singularly (although not exclusively) miners, to appropriate value created by others in an unfair way. Their position allows them to copy profitable transactions and replace or manipulate them to ensure profit, at the expense of the original issuer and at the cost of decreased efficiency of the network. This jeopardizes the network as it reduces its throughput and diminishes confidence in the blockchain. We show that this value appropriation is a new form of free-riding enabled by the very mechanisms that prevent other forms of free-riding through automation and competition. Blockchains are CBPPs, a type of Commons describing value creation in a peer-to-peer network, so we build on methods from the Commons to deal with free-riders to propose a community-based approach to solving MEV issues. Doing so, we introduce some important characteristics of the theory of the Commons and how it applies to blockchain communities. We introduce Ostrom's 8 Design Principles and discuss how MEV affects them. These design principles are indicators of sustainable collective governance and underline the importance of participation and community involvement to adapt the governance rules to an evolving context. As MEV modifies the community and its dynamic, we suggest overtly discussing of the expectations of the community towards the blockchain to find a solution likely to be widely adopted. While applying Commons theory in the case of blockchains, it becomes apparent that, while automation is helpful to enforce and ease most day-to-day operations, the off-chain processes is prominent when it comes to adapting the rules. Notably, the evolution of the protocol must be made in accordance with the reasons that motivated the individuals to form a community in the first place, a social contract of sorts. This higher level, called "constitutional level" by Ostrom, is also central in the last papers presented here.

The second paper, entitled *Representation and Intensity of Preferences: A Public Economics Analysis of Liquid Democracy*, focuses on an important part of the governance process: voting. Often times, communities must make decisions regarding the resource that they manage. Depending on the structure of the community it may be taken either by an authority or collectively, through a vote. This vote can happen either by raising hands, by walking in one direction, in the secrecy of a voting booths or online with a digital tool (e-voting). The voting method is often chosen depending on the attributes of the community, notably its size and/or its geographical spanning. DAO-communities, made of pseudonymous users scattered across the globe often rely on voting mechanisms rooted in the DAO code. E-voting facilitates the implementation of different voting methods, from simple majority to ranked choice voting. Among the different voting methods, Liquid Democracy (LD) is gaining momentum in blockchains communities because they allegedly allow for a simple implementation of this once impracticable voting system. LD is mix between direct and representative democracy where each voter can delegate her vote, on one or many topics, to someone else who can, transitively, delegate all the vote she holds. This creates a network of delegation that, supposedly, gives more power to qualified voters. As contracting is at the core of blockchain-based transactions, delegating votes conditionally and automating the outcome of the vote is easy, blockchains are natural candidate for LD implementation. Constitutional economics provides us with methods to discuss voting methods, and analyze whether they are good at representing the intensity of preferences of the voters. In this paper, I apply this methodology to LD and contend that, while it is capable of reducing negotiation costs, LD fails to provide a framework for vote-trading or bundling, both traits essential to the expression of intensity of preferences. I thus conclude that LD is more suited to small scale homogeneous communities than to large scale systems such as national elections. Commons or DAOs are examples of such communities and the last section of the paper addresses the specific challenges of blockchain-based LD implementation. This paper contributes to a better understanding of one of the most formal aspects of the constitutional process, voting methods, in a blockchain-enabled context. The following papers questions other features of collective governance in the context of Commons.

Blockchains for the Governance of Common Goods, written with Primavera de Filippi and Simona Ramos, introduces the readers to blockchain-based tools at the service of commoners. We lay out the conditions at which recourse to blockchain-based tools may be relevant and the challenges it brings to commoning, in particular in the context of natural resources. While traditional Commons governance relies on the capacity for the community to monitor activities and sanction forbidden behaviors, recourse to blockchain changes this paradigm. Behavior on a DAO is constrained by the predefined set of actions made possible by the code. Monitoring thus becomes useless is replaced by *ex-ante* automation. Actions can then be verified *ex-post* to ensure consistency with the whole governance process. Sanctioning may be difficult on blockchains, as members are pseudonymous and transactions are immutable, but social mechanisms may prove efficient. Among the other difficulties of blockchain-enabled governance is the role of oracles, the smart-contracts used to record off-chain data on-chain. Because many of the governance processes are likely to rely on this data, these oracles are extremely important. We encourage communities to rely on cross-validation of external data to avoid any user from illegitimately making advantage of an error on the blockchain. This also makes it necessary to encode, in the code of the DAO, the possibility to amend or cancel some parts of the code, in the event that it would be executed with wrong inputs. This evidences the link between the off-chain governance and the on-chain execution and automation of the code. Building on Ostrom's work, and specifically on the 7 types of rules she identified to be relevant to assess whether and how her design principles are met, we provide a first picture of the dimensions that may be automated *ex-ante* or verified *ex-post* and those that require human agency. This analysis is helpful to delineate the Commons that may benefit from having recourse to blockchain-augmented governance. Notably, this paper shows that in low-trust environments where monitoring may be delicate, blockchains may be adequate. Though they cannot entirely replace trust, they can substitute confidence for it thus reinstating the conditions for a sustainable Commons governance.

The final paper, *A Unified Framework for the Governance of the Commons with Blockchain-Based Tools: An Application to Customary Land Commons in Ghana*, coauthored with Simona Ramos, extends this work and connects it with two foundational papers in the field of blockchain-based Commons governance. Along with the previous chapter, these three papers build on Ostromian theory—and in particular on the Institutional Analysis and Development framework (IAD)—but they focus on different parts of it. In this article, we present a unified approach to provide scholars and practitioners with a comprehensive toolbox. When the three papers are brought together, it appears that some aspects of the IAD are under-researched. To date, existing work has mostly focused on the operational level and has not explicitly engaged with how blockchain-based governance affects the higher levels, namely the collective choice ones. In line with the other papers presented here, we explore this direction that exhibits nested layers of governance, both on and off-chain with interrelations that shape the operational level. We also dwell on the 7 types of rules mentioned above and analyze them in terms of blockchain implementation, evincing the blockchains affordances at play. Consistently with the practice of this field of research, we illustrate our theoretical analysis by a fictitious case study of customary land Commons in Ghana. While the case study is fictitious, the institutional environment, and therefore the rationale for choosing it, is not. We propose the blueprint for a blockchain-based tool to complement Commons governance of rural customary land in a context where customary tenure is threatened by enclosures in a legal pluralism context. This tool should be designed in a bottom-up way, learning from best practices in terms of participatory mapping. We argue that blockchain technology's transparency, automation and resilience can increase the agency of the commoners in an adverse institutional environment and apply our unified framework to exemplify how it can be mobilized. We also raise awareness on the numerous risks associated with introducing a complex digital tool in a non tech-savvy community. The question of digital exclusion, power inequalities and disenfranchisement cannot be overlooked, in particular in the case of gender inequalities. We argue that if properly co-developed, such a DAO could lead to empowerment and valuing secondary users, as was the case in other case studies in Sub-Saharan Africa. It is likely that the conditions are not met today for the implementation of this tool in the short term but we believe that it offers a valuable example of how Commons governance could benefit from the affordances of blockchains.

These four papers form a corpus contributing to analyzing the collective choice process of blockchain-enabled communities. It demonstrates that while blockchains are a powerful tool to provide confidence in the day-to-day operations for the governance of a resource, we cannot afford to ignore the dynamics at play when these rules need to be amended. In these cases, trust and off-chain social conventions regain prominence. This fuels a two-way relationship: blockchains can introduce confidence in trust-deprived contexts but, conversely, they need this community involvement and rely and its norms to deal with a changing environment.

The conclusions for the community are straightforward and consistent with the other findings of the BlockchainGov research group: blockchains users and members of DAOs must actively embrace the human side of the governance of digital systems to avoid potential governance crisis. This disentanglement of the different layers of governance is also necessary for providing communities that are less proficient in blockchains with suitable tools too. Throughout the document I raise awareness on the limitations of blockchain systems. I believe that blockchains are a fascinating innovation that allows for the conception of innovative institutional arrangements that may be empowering and inclusive but the current situation suggests caution. Most of the blockchain transactions to date concern financial markets (Manski, 2017) that reproduce extremely inequal wealth distribution of real-life economies (Sai et al., 2021). What is more, Ethereum and Bitcoin, the two most used blockchains, use energy-intensive technology and consumes increasingly more energy[3], a concern in face of the critical environmental crises the world faces. Therefore, my research is optimistic in terms of opportunities offered by the blockchain technology and more pessimistic in terms of implementation and adoption. I believe important research is still to be carried out to promote sustainable and responsible usage of blockchains. This manuscript humbly attempts to contribute to understanding what such a usage may be.

[3]As mentioned in subsection 1.1.5 this may change for Ethereum.

Literature Review

Literature Review

This chapter proposes a survey of the different strands of literature mobilized in this dissertation to conduct an economic analysis of the collective choice problems in blockchains communities. It builds on the pluridisciplinary research on blockchain governance and on the political economy literature. It is conceived as a theoretical and conceptual toolbox to help the readers navigate the different fields that my research builds upon. It proceeds thematically and first offers a technical description of the blockchain technology. While my research is mostly non-technical, the issues of blockchain-based governance are, to a large extent, constrained by the architecture and the functioning of the technology. I have tried to make it as simple as possible for uninformed readers. After this technical description, I present the issues of the governance *of* and *with* blockchains. This field of research is still ongoing and I have selected the directions that most resonate with my own research specifically those relating to the interplay between on-chain and off-chain governance. Some aspects, less related to my questions are mentioned but less thoroughly discussed. I then present a historical overview of political economy with a focus on constitutional economics. While the scope of political economy is very diverse, I concentrate on the crafting of constitutional rules to provide public goods and the theory of how to deal with free-riders. After this somewhat general discussion of political economy, I specifically discuss Ostrom's theory of the Commons and her analytical framework.

Throughout the review of these two main fields, I outline the conceptual similarities between the foundations of blockchains' mechanism designs and those of political economy. These similarities have been identified early and although recent, the literature applying methodologies from political economy to blockchain(-based) governance is already quite rich. In the last section, I discuss this research field, reflect on its conclusions and highlight the aspects of literature that are still missing. Special care is devoted to the question of Commons-oriented governance where the major contributions of this thesis lay.

This helps introduce the following parts of the manuscript and situates my methodology in a larger school of research. It also evidences the contributions made to the literature and delineates further directions of research.

1.1 Discussing Blockchains

This section first provides a technical description of how blockchains work and the ecosystem they support. It then presents the state of the art on blockchain and blockchain-based governance.

1.1.1 History and Context

Blockchains are, at their core, distributed ledgers that record transfers of digital assets on a digital network without resorting to a central authority to validate the state of the ledger. When releasing the seminal *Bitcoin: A Peer-to-Peer Electronic Cash System*, Nakamoto (2008), created the first blockchain and managed to provide a solution to the following problem: how to have a digital system to exchange e-coins that met the three following criteria: “ (i) security: no one should be able to counterfeit an e-coin or spend the same e-coin twice; (ii) privacy: the payment method should not reveal the customer’s identity, and it should not be possible to trace the previous owners of an e-coin or the previous transaction that were made with it; and (iii) efficiency: the payment infrastructure should be fast and relatively simple and should not require expensive hardware ” (Koblitz and Menezes, 2016, p.88). Research on how to achieve a decentralized monetary ledger had been going on for decades before Bitcoin was invented (Narayanan and Clark, 2017). Chaum (1983) found a centralized solution but whether a peer-to-peer solution was possible remained an open question. The main difficulties were to avoid the “double spending problem”—preventing participants to replicate a transaction and thus spend the same e-coin twice—and to solve the Byzantine’s Generals Problem (Lamport et al., 1982)—which consists on creating a consensus in a network with malicious nodes and potentially unreliable information—but no decentralized solution had been found before.

The reason so much work was devoted to finding a solution to these problems is that double-entry bookkeeping and ledgers were pivotal to the development of international commerce and enlarged the world available to trade in for merchants in the 15th century (D. W. Allen, 2012). At that time, the different trading posts were occupied by people who trusted one another not to steal. Decentralization was built on social capital and structures such as family or religion (Richman, 2006). In particular this facilitated credit between the different members of the merchant community.

In the case of digital currencies however, trust cannot be used as a foundational mechanism to ensure compliance to the rules. Because users are (or may be) anonymous and the scope is broader than a single community, other mechanisms must be devised. In centralized systems, a financial authority (such as a bank), trusted to be reliable certifies the balance of each user and ensures that the money is not doubly spent. However, trust and confidence in the banking system has been eroded after the 2008 financial crisis. The first block of Bitcoin, Nakamoto explicitly refers to a newspaper talking about bank bailouts in the wake of the crisis (Elliott and Duncan, 2009) and Bitcoin was thus developed to provide an alternative to exchange money without having recourse to third parties, considered as single point of failures. Because it could not use trust as an underlying mechanism to prevent fraud, Nakamoto had to come up with other processes. Participating to the work of Cypherpunks who, in the face of increased digitalization of human interactions, set up to provide tools to preserve privacy and build anonymity (Hughes, 1993), Nakamoto focused on cryptocurrencies.

1.1.2 A Technical Introduction to Blockchains

He managed to do so through the help of two main features: cryptography and game theory. Relying on a mathematical modelling of the interaction between the users, considered as rational agents maximizing their profit, this system aims at avoiding any social mechanisms. Although this thesis demonstrates that human-based governance cannot be eschewed, blockchains have certainly been successful at designing a decentralized ledger.

The cryptographic element is two-fold: the first aspect consists in ensuring that a transaction is rightfully emitted (that no one can counterfeit an order) and relies on the public/private key technology. The second is based on hash functions and makes it extremely costly for users to try to modify the chain.

Public/private keys: Based on elliptic-curve cryptography, public/private keys are a pair of strings of character that allow to cipher a message with the help of the private key and decipher it with the public key. The public key must be broadcasted to the whole network so that everyone has it. When Alice wants to send an order on the blockchain network, she ciphers it with her private key (that she must never give to anyone) and everyone can verify that Alice and only her could have written this message (Pilkington, 2016; Swan, 2015). This already addressed the first point of the security issue mentioned above. What is more, public/private keys allow to cipher messages that can only be deciphered by targeted users (whose public keys are known).

Hash functions: Hash functions are mathematical functions that transform an input (a string of bits) into an output called a hash or a digest. Hash functions are extremely easy to run (computing the hash of a large file only takes a few milliseconds on a personal computer) but are virtually impossible to reverse. The most famous one, used by Bitcoin, is SHA-256 and the digest is a 256-bit string. To reverse hash functions, there are no better strategies than to try at random (a strategy also referred to as brute-forcing).[1]

[1] In the case of SHA-256, when you try at random you have 1 chance out of 2^{256} to find the digest. This figure is so small that even if all the computing power on earth was dedicated to finding it, it would take billions of times the age of the universe to do so (3Blue1Brown, 2017).

Blockchains such as Bitcoin combine these cryptographic functions (that both predate blockchains and are widely used outside of the blockchain world) with one a chained structure. To illustrate how this works, let us consider a given state of the blockchain where the last block is B_N and a new block must be added to the chain. I will first present the case of Proof-of-Work blockchains such as Bitcoin and Ethereum and I will discuss other consensus mechanisms afterwards.

Blocks are made of transactions broadcasted to the whole network. Before being included in blocks and, ultimately, in the chain, these transactions are not considered as executed by the network. They usually *wait*, in what is called the public mempool, for someone to include them in a block. To form, or mine, a new block, certain members of the network called miners select a set $\mathcal{S}$ of valid transaction in which the sender can be verified with her public key and has enough money associated with her address to service the transaction. To add the block $N+1$ to the chain, the miner must solve a cryptographic puzzle. In other word, she must find a number $\mathcal{N}$ called a nonce such that the hash function of the previous block B_N, the set of transaction, and of the nonce starts with a certain number m of 0. Mathematically, this means that $\texttt{SHA}_{\texttt{256}}(B_N + \mathcal{S} + \mathcal{N}) < 2^{256-m}$ (where $+$ is the concatenation operator). The difficulty increases with m.[2] To find a working nonce, miners must try as many nonces as they can, as fast as possible because they compete with one another, in parallel, to be the first to mine the next block. This competition is driven by the rewards that miners get when they add a block to the chain. This reward is a lumpsum in the native cryptocurrency (for instance, 6.25 per block at the time of writing) to pay for the energy and hardware costs they incur trying to find the nonce. The probability for each miner to be the first to find a nonce is their share of the total computing power and this is virtually a lottery. The number m is dynamically adjusted depending on the total computing power trying to solve the puzzle so that, in average, blocks are mined regularly (every 10 minutes on Bitcoin, every 15 seconds on Ethereum). When she has found a nonce and thus created a block B_{N+1}, a miner broadcasts the new state of the chain to the network to update the ledger.

However, it is possible that two (or more) miners find a working nonce (quasi) simultaneously. In this case, other members of the network receive two competing blocks, which also means two competing chains, and must decide between them. By design, the "right" chain is the longest, which also means that most work (computing nonces) was spent on this chain. This provides efficient security against manipulation of the chain. Suppose a malicious actor wishes to control which transactions are added to the chain, she selects her own set of transactions and must now engage in a competition with the other miners to be the first to find a nonce. She might be lucky enough to win this lottery but then she must also find a nonce for the following block while other miners, using the mempool, mine a different chain. For her to be able to control the chain, she must be able to mine blocks

[2] Let x be a nonce chosen randomly, $\mathbb{P}(\texttt{SHA}_{\texttt{256}}(B_N + \mathcal{S} + x) < 2^{256-m}) = \frac{1}{2^{256-m}}$ thanks to the definition of hash function.

faster than the others. Statistically, for this to happen for more than 2 or 3 blocks she must control over 50% of the computing power which is unlikely because the blockchain is designed to incentivize miners to engage in the lottery process. To avoid the confusion between competing (few) last blocks, a block (and the transactions it contains) is usually considered valid when at least 6 or 7 blocks have been mined after it. Because it is costly and rewardless to try to find a nonce after a block that will not be included in the chain in the end, it is in miners' best interest to all contribute to the same chain. Similarly, the chained structure makes it impossible to modify *ex-post* a block without having to modify all the blocks mined afterwards which, once more, would be too costly for any actor to engage in. In such a system, consensus on the chain is achieved by the prohibitive costs of not reaching consensus but it only probabilistic. The longer the chain, the more likely it is that consensus will be achieved. This likelihood can be as close to 1 as possible but it remains statistical. This is called eventual consistency.

This mix between cryptography and competition between the miners to be the first to solve the puzzle to get the economic reward constitutes the core of the Bitcoin protocol.[3] This kind of protocol is called Proof-of-Work (PoW) because mining a block requires including a nonce that can only be found after some computational efforts. While extremely safe,[4] the proof being that despite their high capitalization neither Bitcoin nor Ethereum have ever been successfully attacked, this kind of protocol is terribly energy-consuming. As of July 2022, the total energy consumption of Bitcoin was estimated to be comparable to that of Belgium (CBECI, 2022).

Other consensus protocols exist and Bano et al. (2017) distinguish three types of consensus mechanisms: (i) proof-of-work (PoW) protocols; (ii) proof-of-X (PoX) protocols; and (iii) hybrid protocols. In proof-of-X protocols, miners bid something else than energy which can significantly reduce the environmental impact of the blockchains. Conceptually it remains a lottery where miners can win proportionally with their share of the total bid but what is staked vary. In hybrid protocols, mechanisms combine PoW with PoX or other mechanisms. These include Byzantine Fault Tolerant mechanisms (BFT) that have finality rather than eventual consistency but do not scale up well. The PoX category is particularly interesting as numerous efforts are made to reduce the energy consumption associated with blockchains. Wan et al. (2020) and Xiao et al. (2020) provide a survey of these PoX and in specifically of Proof-of-Stake (PoS) protocols: instead of finding a nonce to form a block, block validators—the more general name for miners—stake an amount of their choice of the native cryptocurrency to vouch for a block. There is then a lottery process to choose the block to add to the chain (in proportion of the amount staked) and the associated stake is escrowed. After some time, when the block is far enough in the chain and it becomes apparent that it does not contain illicit transactions, the deposit is

[3]This also explains the name *cryptocurrencies*.

[4]As long as enough computing power is spent on the network, otherwise 51% attacks becomes easy to carry on.

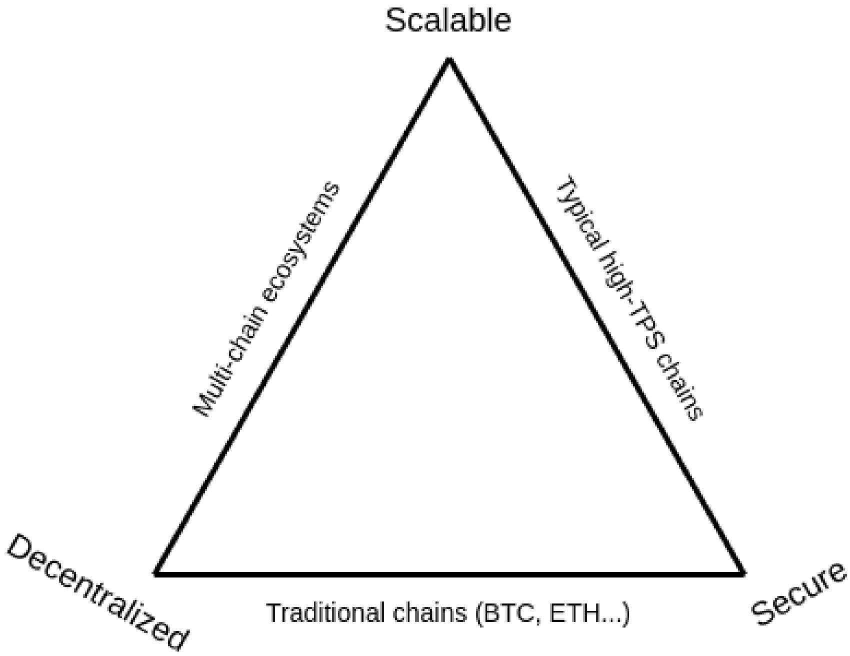

Figure 1.1: Vitalik's Trilemma

Source: Buterin (2021)

given back with benefits to reward block validators. In such a system, attacking the system to rewrite the chain requires having more than 50% of the cryptocurrency rather than of the computing power. In Delegated Proof-of-Stake (DPoS) protocols, users can delegate their cryptocurrencies to other validators who then stake it. Proof-of-Authority (PoA) is built on reputation, users earn the right to become validator and stake their reputation. If they vouch for an illicit block, their reputation decreases and they may lose their position as validators.

choosing between the different possibilities of consensus mechanisms implies a trade-off also known as Vitalik's Trilemma that states that no protocol can offer simultaneously security, scalability and decentralization (see Figure 1.1). Typically, PoW are safe and decentralized but do not scale very well while PoS are decentralized and scalable but are not as safe of PoW. Hybrid solutions are made to escape this trilemma. Importantly, let us note that Ethereum is now transitioning from a PoW protocol to a hybrid system with PoS.

To sum up, blockchains use cryptography to record and certify the data that will be stored in the ledger. In PoW blockchains, cryptography is also at the origin of the security of the consensus mechanisms. In any case, security of the blockchain against manipulation results from incentive mechanisms and competition between block validators. By rewarding them in native cryptocurrency, the mechanism design also implements a form of profit-sharing lowering the risks of attacks that would decrease the overall value of the blockchain. This completes the design of blockchains as systems relying on cryptographic securities and economic incentives to coordinate exchanges between mutually distrusting agents. This little manual in blockchain technology now allows us to move on to describing what the blockchains can be used for and by whom.

1.1.3 The Blockchain Ecosystem: Tokens, Smart-Contracts, DAOs and Other Bits

As ledgers, blockchains can store different type of data that go beyond digital currencies: they allow nodes to share any string of bits on a peer-to-peer network. On second generation blockchains, notably on Ethereum, these strings of bits can be interpreted as code to be executed. This execution requires a virtual machine (called Ethereum Virtual Machine or EVM for Ethereum)[5] but has dramatically broadened the scope of blockchains. Because the language compiled by the virtual machines are Turing-complete (Wood, 2014b), these blockchains act as decentralized computers. Not only can these blockchains bring consensus on digital data but it can also ensure that all the nodes run the same programs, with the same outputs. These decentralized programs are, generically, called *smart-contracts*. Although they had been previously theorized by Szabo (1997), their implementation depended on a substrate that did not exist prior to the invention of blockchains. A smart-contract is essentially a type of *account* on the blockchain. Contrary to other accounts (addresses associated with private keys), smart-contracts accounts contain their code and some storage facility. When a user wishes to execute the code of the contract, it sends a transaction to the account of the smart-contract specifying the parameters of the function that the code will run. This transaction is added to a block and to the chain following the process described in subsection 1.1.2. The diversity in smart-contracts is as large as the one in computer softwares. I here give overview of some of them but focus specifically on those relevant to the rest of the dissertation.

Executing the code is resource-intensive and miners thus incur extra costs. These costs are measured in *gas*, the atomic unit to measure computing resources necessary to run a program. When calling a smart-contract, a transaction must specify a gas price (in ETH, Ethereum's cryptocurrency) and the miner who include this transaction in this block gets paid the gas spent to run the program multiplied by the gas price. In order to incentivize miners to include their transactions, users are encouraged to put high gas prices. Over the network, the mean gas price finds its equilibrium through and supply and demand process and during periods with a very high demand for block space, the price of the gas soars. To avoid being insolvent (in case the execution would loop or be too long), users calling a

[5] For the sake of clarity, this section will adopt the names of the Ethereum components but alternatives do exist.

smart-contract also specify a gas limit.[6] This method of eliciting the transactions included in the blocks is transparent and has its advantages. However, chapter 2 also points out the limitations of such a mechanism that can lead some competent users to artificially increase gas prices resulting in the *de facto* exclusion of some other members. What is more, this method also favors profitable transactions which may be at the expense of non-financial use of the blockchain.

The smart-contracts allow to automate transactions and certify the execution of a code. Because the blockchain is transparent, the code is auditable by all the users and users may have a high confidence in the output to expect. Examples of smart-contracts may include freelance contracting: suppose Alice hires Bob to do a translation for her. She uses a smart-contract to which she sends the payment. The funds are escrowed until Bob sends his work to Alice. When he does so, if Alice is satisfied the funds are released and if she is not, the contract calls to Eve, a third party to rule the dispute. The process is transparent and auditable. Other examples include prediction markets or betting platforms (such as Augur, the most famous one) that release funds automatically depending on certain conditions, such as sport results.

Note that this last example implies having access to *off-chain* data (such as the results from a football game). This is done through special smart-contracts called *oracles*. Oracles are the only way of accessing data from outside of the chain and, as such, they represent a potential point of failure. Indeed, if someone successfully manipulates the data that a betting platform relies on to distribute pay-off, she could steal a lot of money. Oracles reintroduce third parties in blockchains as they require trusting the source of the data. While it introduces vulnerability, this is also necessary to extend the range of blockchains application for blockchains as platforms for socio-economic exchanges. The role of oracles and the challenges associated with validating the data they provide is discussed at length in chapter 5. In the context of natural Commons, digitalization of off-chain information may be sensitive and must considered as legitimate by the users of the system. Strategies to have confidence in oracles either include relying on a trusted provider (such a trusted off-chain institution) or peer-validation of the data, for instance through multi-signatures where different members must vouch for the data in a fashion similar to the proof of stake described above. In the context of natural common-pool resources, both approaches may be relevant but the latter is generally more suited as discussed in chapter 4.

The chunks of code executed on the EVM can be more than smart-contracts called by another account (either a user or another smart-contract). In particular, in an influential blogpost, Buterin (2014) characterized smart-contracts by the fact that they had a bounded number of participants but this does not have to be the case. Let us consider the case of Decentralized Autonomous Organizations (DAOs): “A DAO is a blockchain-based

[6]This implies that although the programming language they use (Solidity for Ethereum) is Turing-complete, the execution is limited in the number of operations and is not Turing-complete.

system that enables people to coordinate and govern themselves mediated by a set of self-executing rules deployed on a public blockchain, and whose governance is decentralized (i.e., independent from central control)" (Hassan and De Filippi, 2021). DuPont (2017, p.159) specifies that "a DAO is a pseudo-legal organization run by an assemblage of human and 'robot' participants" and these two definitions help have a better understanding of what DAOs are and how they differ from other smart-contracts. They are organizations open to participation (potentially under certain conditions) with a, theoretically, unbounded number of participants. Interestingly it also points out that the DAOs are not comprised only of the code but also of its members and the governance process at play between the different actors. As developed in subsection 1.2.2, this definition is close the one of the Commons that I use in the dissertation. Hassan and De Filippi (2021) summarize the unresolved issues around the question of DAOs and their definitions. Their account illustrates that these debates concern the three words in *Decentralized Autonomous Organizations*. They indicate that it is unclear whether the decentralization only concerns the infrastructure of the substrate (*i.e* the blockchain) or if must also concern the governance level. The autonomy of a DAO stems from the automatic execution of its code on the blockchain. However, it is unclear if this autonomy also concerns the governance, in other words, if most of the operations are undertaken by human actors or by algorithmic ones. There also are questions regarding the meaning of the word organization, in particular its legal definition and the status of the code that constitutes it. These questions will be more discussed in the following section.

All this denotes that, despite active research and development in the field, there is still room for interpretation as to what DAOs are. In my research, I choose to adopt a rather human centric definition of DAOs. As far as decentralization is concerned, the infrastructure part is enough and the human governance can be centralized, up to a certain point. While this may not fully benefit from the opportunities offered by blockchains, I contend that DAOs can be used to decentralize and automate certain *off-chain* governance processes that have centralized aspects. Similarly, autonomy in the automation is enough and my definition of DAOs does include organizations where human actors have much more agency than the "robot participants". DAOs with little to no human agency are Decentralized Apps (dApps) (Buterin, 2014). More specifically, I propose to mix the two previous definitions to characterize DAOs as a three-dimension system adding emphasis to the resource governed by the DAO. Organizations have a purpose and DAOs are thus used by a group with an aim. Interestingly, the resource may be the DAO itself, with the purpose of it thriving. With this in mind, the remainder of this manuscript discusses DAOs as a system made of (i) a resource; (ii) a set of actors (human and robots); and (iii) a set of governance rules (partly automated and self-executed). The challenges of DAO governance rules are discussed in the following section.

While Blockchains often have a native cryptocurrency used to reward maintenance of the chain (for instance block validators), DAOs, and dApps usually rely on specific tokens.

Tokens are digital assets that can be exchanged on the blockchain. On a DAO they can also be associated with governance rights and distributed to reward accounts for some maintenance or development work. Much of the interactions on the blockchains are token-based, for instance different tokens can be traded. The exchange rate of the different tokens is decided by market mechanisms. Token creators, such as DAO programmers also decide under which conditions new tokens are created. Typically, native tokens such as BTC (bitcoin) or ETH (the Ethereum native token), are created when new blocks are added to the chain but DAOs can have *ad-hoc* mechanisms but other tokens are generally created by tokens contracts, a smart-contract that releases new token under a set of conditions.

Thanks to the flexibility of the programming language at the base of the blockchains that support smart-contracts, tokens can take virtually any given form. In particular, most that are traded are cryptocurrencies and, as such, are fungible. They usually follow the standard of the ERC20. However non-transferable tokens (representing reputation for instance) may also be developed, as well as tokens that disappear when not used after a certain time to incentivize people to spend them. The most famous type of tokens apart from ERC20 are Non-Fungible Tokens (NFTs), usually following the ERC721 standard. NFTs can also be exchanged but their value is unique as they are non-fungible. As such, they may either be pegged to a unique *off-chain* good (such as an art piece, a collectable good or a real estate property for instance) or be the collectable elements in themselves.

The design choices behind the creation of a token are informed by the expected goal of the token and its users. Because most of the interactions on the blockchain are codified by smart-contracts and self-executing rules dependent on tokens, the behavior of the different actors is predicted by what has been dubbed *tokenomics*. Tokenomics is the prediction and mechanism design of rational agents in possession of tokens. Most of the DAOs have tokens and a tokenomics mechanism design to encourage their growth and guarantee an efficient governance however my research has focused on DAOs where tokens cannot or should not be used as financial assets and be traded and the remainder of the manuscript does not study much this element of DAO governance. Studying the tokenomics of Commons-oriented DAOs is an active research question that complements the work presented hereby.

The generalization of token exchanges has given birth to token finance, also called Decentralized Finance (DeFi). In contrast to traditional finance that mostly takes place through centralized marketplaces and stock exchanges, DeFi does not need intermediaries. Rather, it takes place on decentralized exchange platforms (DEXes), that automatically compute orders and algorithmically set the exchange rates between different tokens and different DEXes may thus have different rates if they do not have the same algorithms. DeFi now makes for a large share of Ethereum usage. DeFi is an important driver of blockchains in general and of MEV in particular and is thus discussed in chapter 2.

1.1.4 Governing the Blockchain World

As blockchains are softwares, they need upgrading regularly either to fix bugs, to prevent undesired behavior or to adapt to an evolving context and make structural design changes. Although the operation and execution of the code on a blockchain is completely automated and decentralized, the process around upgrades and governance of the chain is not. For instance, all major blockchains are open-source projects with their code available on a git repository. This, theoretically, allows collaborators to either contribute to the code and modify the blockchain, or to copy the code, modify it locally and deploy their own version of the chain.

Core programmers retain the rights to accept or not contributions (git push) to the original software branch but anyone can copy their version of the chain. To govern how contributions and evolution of the code is decided upon, blockchains have adopted norms. The Bitcoin Improvement Proposal (BIP) or the Ethereum Improvement Proposal (EIP) are processes through which anyone can submit a written improvement proposal to the community. The proposal is then debated, discussed and audited by the community and the code is peer-reviewed. If the improvement is approved, then the software is upgraded. Note that this already heavily relies on *off-chain* governance because the decision-making process takes place through informal discussions, discords channels and physical meetings.

When the code is edited, users of the blockchain must upgrade their version of the software. Some modifications are rather light and the newest version remains compatible with the previous ones (backward compatibility), therefore all users still agree on the same blockchain. This is referred to as a *soft fork*. Some modifications concern the protocol itself and are more structural. In this case, the upgraded nodes do not accept the blocks created by the previous version which results in splitting the chain. This process is called a *hard fork* which may result is a divided community and two competing versions. This may then jeopardize the security of the chain if there are not enough users to guarantee decentralization. The risk of hard forks incentivizes the community to only adopt consensual improvement proposals. Because all users must individually upgrade their version of the software, adoption of the evolution of the code is necessarily decentralized. When having to choose between two competing forks, users can decide which one they prefer in a process akin to foot voting (Tiebout, 1956) as I discuss in section 1.2.

This concerns the governance *of* the blockchain itself and DAOs and other blockchain-based tools have specific governance challenges. Contrary to traditional software, deploying code on a blockchain implies structural constraints: once added to the chain, a smart-contract cannot be removed (permanence of data on the chain) and can only be altered insofar as it was originally planned. In that sense, Howell and Potgieter (2019b) call for including explicitly *off-chain* governance mechanisms in smart-contracts in order to address unexpected situations. The question is slightly different for DAOs that necessarily have human governance mechanisms. The question is then how the *on-chain* and *off-chain* mechanisms are entrenched.

Interestingly, the mechanisms of DAO and infrastructure governance are mutually dependent as is illustrated by the infamous example of theDAO whose case study is well analyzed by DuPont (2017). Although theorized at the beginning of Ethereum, DAOs were not the subject of much attention or development until theDAO was launched in April 2016. theDAO was a crowdfunding platform on which blockchain users could invest (with the help of cryptotokens), vote on projects to fund before reap the benefits of their investments in proportion with their investment. Voting rights were also proportional to how much each user had invested. Despite threats identified in the code (Mark et al., 2016), theDAO encountered an impressive success, raising about 14% of ETH supply of the time (which amounted to about $250 millions at the time). However, shortly after, theDAO was attacked, using a failure in the code of the DAO. This allowed the attacker (unknown at the time) to steal about a third of the funds. Due to the scale of the attack, the funds invested in theDAO and the influence of some investors the heist provoked a crisis in the Ethereum community and a debate raged as to the appropriate measures to take. In particular, Vitalik Buterin (a founder of Ethereum and a prominent figure in the blockchain community), suggested to hard fork the chain to cancel the attack and remove all the blocks mined after. As blockchains were made to be immutable, this triggered heated discussions, with some users supporting this countermeasure to recover the funds while some argued that immutability of the chain was a feature to be preserved at all costs. To successfully implement this hard fork, the motion had to have most miners' approval as they are the one in charge of implementing it. As DuPont (2017, p.165) puts it,

> Within the next few weeks, with the political clout of Buterin and the Ethereum Foundation behind the decision, a "hard fork" version of the Ethereum software was developed and released to miners. This hard fork created a special "withdrawal-only" contract on the Ethereum blockchain and moved all tokens to it. A majority of miners implemented this software, and the blockchain ledger was updated to effectively erase The DAO.

Some Ethereum users refused to implement the software and continued using the "original" version of the blockchain, with theDAO. The two blockchains parted and both forks still exist to this day: the most widely used Ethereum is the one that erased theDAO and Ethereum Classic is the fork that refused the update.

This example highlights two crucial aspects of blockchain governance. First, the governance of DAOs and the blockchain cannot be separated. The most obvious direction is that modification of the blockchain protocol may affect DAOs but in some cases, DAOs governance crisis can also impact the substrate itself. This has significant consequences for the governance of DAOs and must be taken into consideration when choosing whether to use decentralized tools rather than conventional ones. Chapter 5 explores these questions in the context on natural CPR and the nestedness of governance situation it implies. Second, while blockchains were created to replace human agency by algorithmic governance, the role of some real-life actors, such as influential members or foundations remains critical and shapes the decisions made by the community. It is therefore impossible to analyze blockchain governance without focusing on the social interactions and the positions of the different actors.

Subsection 1.1.2 has already made it clear that miners had a specific role in the governance of blockchains. Because they are in charge of maintaining the network, they have, ultimately, the last word with regards to protocol changes. The right to fork (a feature of Open-Source Softwares and not unique to blockchains) significantly affects governance as it ensures a form of unanimity or, at least, of large qualified majority (Nyman and Lindman, 2013). This also balances the power of miners, because if miners adopt a new version of the chain but users do not use it, the new chain is useless and the older one prevails. This power of the block validators stems from the architecture of the blockchain itself. But as DuPont (2017) points out, other actors have less formal roles but may have as much power. Most blockchains have a foundation that supports the development of the blockchain. While the foundation has no executive power, the example of theDAO demonstrates how influential it remains. Potts et al. (2021) liken these foundations to governments providing a public good and they add that they also serve to increase exit costs associated with forking, contributing to the stability of the blockchain.

Other actors may hold significant power, among which are exchanges platforms and cryptowallets. Most blockchain users do not want to store a private key and access the network directly. Rather they prefer to use a software, often a web-app or a smartphone app, with a good UX to manage their cryptoassets in what is called a cryptowallet. Some of the companies running these apps also allow to exchange cryptocurrencies or offer broker services to use exchange platform, either centralized or decentralized. These companies end up owning a large share of the total supply of certain tokens and this may be a liability. Notably, in PoS blockchains, owning a large share of the tokens makes it easier to manipulate the chain.[7] This gives these companies significant negotiation power in the discussions around the future and the strategic development of blockchains.

While blockchains are virtually impossible to regulate—their execution is automated and decentralized across nodes running in many different jurisdiction—these large companies are not and introduce a new component to blockchain governance which is legislative compliance. As De Filippi and Wright (2018) show, blockchains cannot be regulated and follow the *Lex Cryptographica*. In the wake of Lessig's "Code is Law" (2006), they prove that the code of the blockchain and of its smart-contracts acts as the law in the sense that in constrains the actions of individuals. The "Rule of Law" is replaced by the "the Rule

[7]For instance, per Tezos Stats, consulted on the 15/08/2022, the five largest stakers (accounting for delegation) on Tezos accounted for about 35% of the staking capacity. They are all cryptowallet or staking companies.

of Code" where the national laws cannot interfere. This raises significant issues as far as contracting is concerned because contracts in natural languages are incomplete in order to account for uncertainty while smart-contract must predict every state of the world. This constraint highly reduces their scope while interpretation and flexibility in natural languages provide security to contractors that smart-contracts offer and makes possible to engage in more complex contracts. What is more, smart-contracts are prone to bugs which could result in an unexpected outcome. If engaging in a contractual relationship involving significant investments, agents want to benefit from some form of protection and states may be an efficient protection mechanism (North, 1990).

In their review of the challenges associated with the regulation of blockchains, smart-contracts and DAOs, De Filippi and Wright (2018) recall that although they may directly control blockchains code, there are other ways for states to affect blockchain governance. They build on the "pathetic dot theory" (Lessig, 2006) to explore how states can use norms, market dynamics or hardware to govern blockchains. The role of states with regards to blockchains is also studied by Atzori (2017) who defines blockchain as a "pre-political" organizational theory. Werbach (2017) also defends that blockchains and DAOs need the law. Because blockchains offer services akin to financial services, they should be regulated as such. For instance, many projects get funding through Initial Coin Offerings (ICOs) where they distribute tokens against fiat currency investments. As these ICOs are similar to IPOs, many countries have started regulating them accordingly while still trying to be attractive (Kaal, 2018).

As noted above, regulation of blockchains is facilitated by the large actors that use it. Companies willing to attract investors or to reassure their users that they are protected by the law in case of problem often deliberately have a legal entity in country with a strong legal system. Countries may engage in jurisdictional competition to attract crypto companies (Werbach, 2017) but this ultimately shapes the structure of the smart-contract or DAOs these companies are based on. Similarly, the aforementioned foundations also have a legal status that regulate what they can do or not.

The case of DAOs is particularly interesting as far as governance is concerned because they are really diverse in the services they provide. COALA (2021) propose to regulate DAOs through functional equivalent. This is suggested in order not to prevent innovation *ex-ante* and to have a flexible model. This also allows to design the DAOs in order to "to benefit from legal personality, and for its Members to receive limited liability protection" (p.7) and this model explicitly includes governance clauses. When DAOs are used to regulate off-chain resources in contexts with scarce blockchain-literacy (such as the Commons studied in this dissertation), these legal dispositions may also protect users from algocracy. Danaher (2016) defined the "algocracy [as] a situation in which algorithm-based systems structure and constrain the opportunities for human participation in, and comprehension of, public decision- making." (p.2) and Atzori (2017) specifically raises awareness on this risk in blockchains. A related threat is that of *algorithm authority* which refers to "the power of algorithms to manage human action and influence what information is accessible to users" (Lustig et al., 2016).

This section in general points out that—although blockchains were originally designed to replace human governance by cryptographic functions and game theory—social interactions, network effects and the off-chain world still play a large role. Rather than eliminating the need for trusted intermediaries it has replaced these intermediaries by blockchain actors. De Filippi, Mannan, et al. (2020) evidence this by showing that blockchain-based eliminate the need for trust in the execution of processes but that a network of trusted actors remains necessary for the governance of the blockchain, and ultimately, for the execution of code on the blockchain. They build on Luhmann (2000) distinction between *trust* and *confidence* who defines the former as involving uncertainty while the latter refers to rational expectations. When trusting, there is an intrinsic, deliberate and acknowledged risk of being deceived or disappointed while, in confidence, the risk is not perceived. Rather there is a feeling that the set of potential actions can be foreseen and predicted. They then demonstrate that blockchains are better described as "confidence machines" than as "trustless technologies" because transparency and execution enable confidence in the execution of transactions sent to the network. However, this section has demonstrated that this substrate is also relying on off-chain governance structures that still extensively depend on trusted actors such as miners, foundations or DEXes. They thus suggest that principles of constitutional theory may be relevant to address issues that may emerge in the management of the blockchains. The four papers presented in this manuscript illustrate these challenges in governance designs and provide insights from classical economic theory presented below.

It should, by now, be clear to the reader that blockchains are a complex ecosystem mixing automation, decentralized infrastructures and social networks in a web in relationships that go far beyond the automatic and predictable system originally planned by Nakamoto. With the scope of blockchains applications widening and interacting increasingly with real life institutions, the governance structure of the blockchains has evolved and has become a complex system. Far from considering this dependence on off-chain governance, social relationship and trust as a liability, I embrace it as a rich feature of the network and consider blockchain as one more tool at the disposition of communities to solve coordination problems.

1.1.5 Blockchain-Based Governance: Practice and Politics

The definition of DAOs that I adopt in this manuscript emphasizes that it is used to govern a resource. This section develops how they do so and presents the state of the art literature on how recourse to DAOs and blockchain-based tools shape governance processes for communities with a special focus on the political aspect of blockchain-based governance.

After the failure of theDAO, development of DAOs boomed and many projects appeared (see the twitter thread by @n4motto, 2022). The idea was to benefit from transparency, auditability and automation permitted by blockchains in order to promote participation and democratic processes. Through tokenization, DAOs can grant voting rights to token holders and ensure traceability of implementation. With this promise, diverse DAOs have been created. Some are very simple and are only voting platforms (see for instance Aragon Voice) while others are very large scale metaverses such as Decentraland. The governance entailed by these DAOs may differ widely depending on the type of DAOs but they some common features that distinguish them from other forms of ICT-based governance. Before dissecting the nitty-gritty of blockchain-enabled Commons, I wish to acknowledge that the development of blockchains is, to a large extent, driven by a libertarian agenda and I want to situate my research with regards to this political approach.

DuPont and Maurer (2015) indicate that the specificity of blockchain-based governance is that "Cryptocontracts tend to build social and functional properties *within* the system, whereas traditional contracts require a cadre of individuals to perform these things outside the contract". Lumineau et al. (2021) go further by stating that "Blockchains may therefore be thought of as the first governance form that truly leverages digital technology's computational- and data-based capabilities in ways that reach far beyond 'analog' or traditional forms of social governance." (p.508) They do so by facilitating cooperation and coordination, by supporting not only *procedural* coordination but also *structural* aspects by encoding rights and tokenizing governance. However, they point out the limitations of blockchains-based systems in relationships with a high level of tacitness. They conclude that blockchains have the potential to replace traditional governance, including in situation with high tacitness. As the core of this dissertation will substantiate, I disagree with this statement as I argue the main potential of blockchain is to *enable* and supplement other forms of governance, notably in relation with public governance.

On top of describing how DAO-based governance technically differs from other forms of governance, Reijers, O'Brolcháin, et al. (2016) investigate how relying on blockchains induces a new "social contract"—defined "as a method for justifying political principles by appeal to an agreement made in an initial situation by people who are (broadly speaking) presupposed to be equal, rational, and autonomous" (p.137)—and how this social contract compares to those of Hobbes, Rousseau and Rawls. They argue that blockchain governance fails to account for Rawls' idea of redistributive justice and they contend that blockchain is not a neutral technology and rather that is has significant political implications. In particular they cite Golumbia (2015) who defends that blockchain is "deeply political" and associated with far-right liberalism. The rationale behind blockchain was to get rid of government control, a position commonly held by right-wing libertarians. Many blockchain enthusiasts are optimist that blockchain provide market-based solutions to coordination problems, facilitated by tokenization and the financialization of blockchains.

Discussion on ideals blockchains support has been gaining momentum in the recent past. Notably, Golumbia's polemical article triggered reactions and sparked debate on the imaginaries of blockchains. Swartz (2018) identifies two competing, an incompatible, imaginaries in the Bitcoin ecosystem that contributed to shape blockchains development: *digital metallism* and *infrastructural mutualism*. The former refers to the belief that the money should not be state-backed but derive its value from the market. This has informed a vocabulary of blockchains inspired by metallists such as *mining*. The latter describes a belief, closer to the cypherpunk manifesto (Hughes, 1993), that blockchains should provide a decentralized infrastructure for payment and exchanges and not only for money. The scope of infrastructural mutualism is broader and encompasses non monetary uses of blockchains. In a recent article, Brody and Couture (2021) assess these imaginaries for the case study of the Ethereum community and find three influent ideologies defining it. The first one is the imaginary of a "world computer", considering that Ethereum should be a universally accessible computer for everyone to run any software they want. This approach significantly differs from the monetary one of Bitcoin. In a way, it extends the infrastructural mutualism imaginary "beyond economic usages" (p.552). The second is the "*ethos* of building and experimentation" that promotes the discovery of new applications on the network contrarily to Bitcoin which is much more conservative and averse to innovation. Finally, the third imaginary is the "prevalence of libertarianism". While the first two themes distinguish Ethereum from Bitcoin and create new blockchain-based futures, this one recalls that "rooting a native currency so centrally in its design is a choice, and an ideological one for that matter, that is echoed by the persistence of speculating practices and discourses" (p.557). Their conclusion is that, although it is complex to place Ethereum on a left-right political axis, the community retains aspects of libertarianism but differs from the Bitcoin one thanks to the culture of using Solidity to experiment and broaden the scope of decentralized applications.

I agree with the statement that blockchain are, at their core, political and that the current major ones mostly serve to advance a neo-liberal agenda. However, as I have reviewed in the previous section, there is currently active research to prescribe how the state should and can regulate some blockchain-based activities. In parallel, practitioners and scholars explore how blockchains, as institutions, can be used for non-market applications and whether it is possible to channel the innovation of blockchains to further cooperative, non-financial practices. This research contributes to building new narratives and imaginaries. While they financial ones remain prevalent, I believe it is important to make efforts to support these imaginaries. I strongly agree with Swartz (2017) when she states that "Even if these projects turn out to be vapor, the blockchain is meaningful as an inventory of desire. It is an engine of alterity: an opportunity to imagine a different world and imagine the mechanics of how that different world might be run." (p.184)

My research aims at advancing these efforts and study mostly non-tokenized and strictly non financialized blockchain-based governance, in particular in the context of the Commons. As I will demonstrate in the following sections, the notions of procedural (also called operational) and structural aspects along with the social contract bringing people together will be central in my analyzes. These efforts to delineate non-profit oriented directions for DAOs may be hindered by the competition with other applications and the price of the transaction but competition between blockchains and experimentations to increase the throughput of blockchain transactions on Ethereum[8] may facilitate such applications in the future.

1.2 Political Economy Literature

1.2.1 Public Choice and Political Economy

Mueller (1996) provides the following definition: "Public choice applies the methodology of economics to the study of politics" (p.1). While the field can be traced back to Borda (1781), Carroll (1884), and Condorcet (1785), the foundations of Public Choice are most often attributed to D. Black (1958), Buchanan and Tullock (1962), and Downs (1957) who mostly covered the issues of constitutions, voting institutions and voting mechanisms. Their approach was soon extended to address other topics and other types of institutions, in particular bureaucracy (Niskanen, 1971) and foundations of cooperation for appropriation and provision of public goods (among which Elinor Ostrom's work). An extensive review of Public Choice is beyond the scope of this literature review but I will present the main methodologies and findings of political economy that are relevant to blockchain-based cooperation and that are used throughout my papers. I start with a review of the work on constitutions, voting methods, logrolling and dealing with the free-riders and subsection 1.2.2 focuses on the work of Ostrom.

The foundations of Public Choice: *The Calculus of Consent*

Historically, Public Choice focused on providing game-theoretical models to understand and explain elections. Arrow (1951) first proposed a formal and mathematical definition of voting methods that resulted in his famous impossibility theorem. It states that no voting system can produce an outcome that simultaneously satisfies a minimal set of five axioms including non dictatorship and citizen sovereignty. This result establishes that voting is necessarily imperfect and thus results from a trade-off between mutually incompatible axioms. This approach in terms of trade-off was later developed and transposed in terms of costs in *The Calculus of Consent* (Buchanan and Tullock, 1962).

The authors put the focus of political economy on how individual agents come to an agreement to establish rules that will shape their future interactions. They consider a group that anticipates repeated interactions with one another and the necessity to provide

[8] It is not the place to engage in a discussion of this evolution of Ethereum but sharding and the transition to PoS are detailed in Buterin (2021).

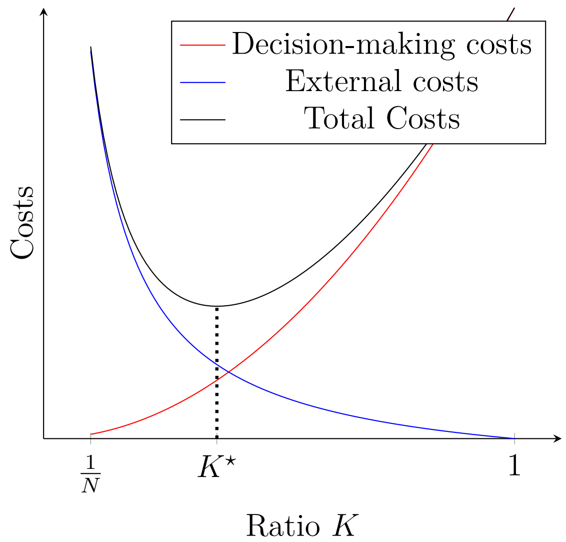

Figure 1.2: Costs of Making Group Decisions

Source: Adapted from Buchanan and Tullock (1962)

public goods (such as villagers needing roads, as in Tullock (1959)). The relevance of this approach for communities creating a governance process and writing the code of a DAO is conspicuous and has triggered a body of research discussed in the next section.

Before engaging in negotiations on a given situation, the group establishes a constitution, *i.e.* a set of rules that specifies how consensus will be reached subsequently. Because Public Choice literature is rooted in a democratic ideal, decisions are taken through voting methods. However, there is no reason why decision should be made by simple majority (*i.e.* 50%+1) Arrow, Tullock, Downs and Black have demonstrated the limitation of this voting method. Rather, Buchanan and Tullock propose a model in which the group (of size N) has to agree on a ratio necessary to vote proposals. They remain in a model of majority voting but the ratio can go from $\frac{1}{N}$ (any proposition is passed without voting) to 1 (unanimity is required). To find the optimal ratio, they propose to minimize the sum of two costs. The first ones are the costs externally imposed by decisions made by the other members of the group and the second one are the costs associated with reaching an agreement. The external costs are decreasing with the ratio K (and are equal to 0 at unanimity) while the decision-making costs are null when no debate is required but increase with K, under certain hypothesis. Their sum is convex and reaches a minimum at $K^\star$ (see Figure 1.2). By adopting this procedure, the members of the group adopt a position similar to the "veil of ignorance" (Rawls, 1971): the decision of the constitutional settings is made *ex-ante* without any knowledge of the position that individuals will have in the group regarding the votes that will happen.

An interesting conclusion that they come to is that no voting rules can be optimal for all possible choices made in the future. $K^\star$ depends of the cost and benefits structure expected from the public goods that the community will vote upon. When the gains/losses are relatively small, the classical $K = 0.5$ is appropriate but for larger stakes, a higher K may be preferable. Another important aspect is the size and heterogeneity of the groups. The more homogeneous the group, the smaller inclusive the optimal ratio (and thus the less inclusive it is). Indeed, when every agent has the same expectation and needs, the external costs are lower. On the contrary, when the group is heterogeneous, the external costs may soar and the optimal ratio moves closer to unanimity. Similarly, decision-making costs depend not only on the ratio but also on the total size of the group. It is harder to come to an agreement with a thousand people than with a hundred in which case the optimal ratio may decrease. However, as I will show in the section on logrolling, this effect may be ambiguous because it may be easier to find 99 people to agree with in a group of one thousand rather than 9 people in a group of one hundred.

Although Buchanan and Tullock suggest to adopt differentiated ratios depending on the type of votes, the goal of a constitution is also to provide a predictable framework and thus stability. In order to achieve Pareto Efficient decisions—a central feature of Public Choice theory such as evidenced by Buchanan (1962) and Rae and Schickler (1996)—the authors argue that the constitution must include other clauses. The first one concerns the structure of institutions and specifically bicameralism. Because direct democracy may be too costly too and long a process in large groups, they study representative democracy. Their model illustrates that, as long as constituencies are different enough in the two Houses, bicameralism is equivalent to much more inclusive voting rules for only a fraction of the cost. By changing the constituencies, bicameralism increases the size of the minimum winning coalition and reduces the opportunity for a group to pass votes at the expense of a larger one.

Logrolling and vote-trading

Another seminal aspect of *The Calculus of Consent* is the importance of vote-trading or logrolling (I use both interchangeably). In a given constitution, numerous votes on different topics will be taken, and the interest groups may change over time, and this creates room for negotiation. Consider an interest group supporting a proposal but lacking a few members to pass it. They will likely try to contract with other voters to convince them to vote in favor of the bill by promising their votes on a future topic. Stratmann (1996) provides the following formal definition:

> A logrolling situation is defined as follows: Let (x, y) and (z, w) be pairs of mutually exclusive issues. Let voter preferences with respect to each pair be separable. Let each voter vote sincerely. A logrolling situation exists if
>
> xPy and zPw, but $ywPxz$

where P stands for social preference as defined by the voting rule employed. (p.323)

Buchanan and Tullock champion logrolling for two reasons. First, they argue that logrolling allows to account for the intensity of preferences: it allows a minority that would be outvoted under the ratio chosen to negotiate with other members and trade their votes, on topics they are mildly concerned with, to win a vote on one they feel strongly about. Their other argument relates to a point made above: the optimal ratio should depend on the structure of the gains and costs but will most likely be fixed once and for all. Vote-trading and accounting for intensity of preferences allows to effectively pass more inclusive bills within a given (unique) institutional setting. Not only do they advocate logrolling but they also defend vote-selling with monetary payment. Their analysis shows that buying votes allows to reveal preferences and reach Pareto-optimal outcomes. However, in his account of logrolling in Public Choice, Stratmann (1996) notes that if logrolling is subject to manipulation (either not revealing one's true preferences or reneging the vote trading), it might not achieve the benefits described by Mueller (1967). Another negative impact of logrolling may be the instability of coalitions. Bernholz (1973) showed that voting systems with logrolling also have cycling, that is to say that there are $n \geq 3$ coalitions $(c_1, .., c_n)$ and for each $k \in \{1..n-1\}$, if coalition c_k (resp c_n) takes place, the coalition c_{k+1} (resp c_1) is preferable. Preferable means that at least one member of the former coalition has the incentive to change and join the new one. As the size of the group and the number of topics increase, the marginal costs of additional members to the coalition decreases and cycle instability is even more salient. As noted by Bernholz, the only way to prevent instability is to have a unanimity rule which, may be very costly in large groups. Despite these theoretical limitations, empirical studies have demonstrated the existence of stable coalitions (notably Mayhew, 1966). This can be explained by the repetitive game-theory: if people are likely to engage in repeated interactions with other voters, reneging at one point may compromise all future coalitions. What is more, Tullock and Brennan (1981) highlight that, contrary to predictions, coalitions are often larger than the minimal winning ones, which brings more stability.

Note that I have not discussed the morality of vote trading yet. Buchanan and Tullock adopt a normative view on the issue. They assert that logrolling and even vote-buying is desirable, produces socially efficient outcomes, and avoids the "tyranny of the majority" by allowing minorities to form coalitions. We have seen that their conclusions should be tempered for theorical reasons but Public Choice says little about the legitimacy of logrolling. Buchanan and Tullock acknowledge that it may raise moral issues, but defend the implicit version of vote-trading that happens daily through parties.[9] Political parties propose programs concerning all aspects of the social life but it is extremely rare that voters have strong opinions on every topic. Rather, they will vote for the party that they

[9] There also are technical difficulties associated with vote-trading when vote are secrets, they are discussed in the second paper.

are more aligned with on the topics they care most about. Voter A may vote for a party because she cares about unemployment benefits and has little to say about geopolitics while voter B may have strong views about the latter but not about the former. If they both vote for the same party, they implicitly trade their votes. This is called bundling and happens regularly in most democracies. The role of parties and their leaders in implicit and explicit logrolling has been underlined by Haefele (1971) and Koford (1982). The question of bundling in order to take into account the intensity of preferences is, I believe, one of the most important contributions of Public Choice to the study of collective choice. Simple majority is only relevant when preferences are assumed to be uniformly spread across individuals and topics, an assumption that seems rather implausible. It is thus important, whenever studying constitutional settings, to devote particular attention to how it accounts for the intensity of preferences.

The relationship this work has with blockchain community is fertile because, on the one hand, it allows us to better understand the constitutional processes taking place in blockchain communities building on decades of research (as I show in chapter 2); and on the other hand it allows for experimentation to test and refine political economy theory where real life constitutional experiments may be impossible to carry on in practice.

Dealing with free-riders

To conclude this partial review of the political economy field and before discussing extensively the theory of the Commons, I introduce the issue of free-riders and the related institutional economics literature. The founding work on the matter is *The Logic of Collective Action* by Olson (1965), a book devoted to understanding how groups organize to deal with free-riders and special interest groups depending on their size. When a group produces public goods, it creates free-riding opportunities because it is in everyone's individual interest to benefit from the public good while not contributing to its provision. The threat of free-riders may deter the group from engaging in the provision of the public good altogether. Olson's contribution is to say that collective action responses to this problem depend on the size of the group. In small groups, monitoring behavior and sanctioning (notably through social mechanisms) free-riders may be relatively easy low so it is likely that the public good will be provided. In medium-sized communities, monitoring and sanctioning may be less efficient and the provision relies on other features of the group. A subgroup (or a single individual) may have an incentive to provide the public good regardless of free-riders if the benefit they derive from it is greater than the costs they bear. It would be cheaper to spread the costs across the whole group but the gains are high enough that they surpass costs split between the members of the subgroup. In this situation the public good will be provided if such a subgroup exists.

Finally, Olson focuses on large groups, the ones where coordination is the hardest. In large groups the threat of free-riding is the highest and the costs of doing so are quite low. Indeed, individual contributions are negligible and defecting from contributing is likely to go unnoticed. Therefore, there are very little incentives for providing the public good. Olson argues that, unless a subgroup still has interest in providing the public good by themselves, the provision of public goods in large groups is almost impossible. He complements this analysis by showing how special interest groups can make advantage of the large group "inertia" to impose a cost on the majority. With Primavera de Filippi and Bruno Deffains, we show that this kind of situation does emerge in blockchain settings, even though the design of blockchains was made to prevent free-riding. The issue of free-riders also underlies Ostrom's theory of the Common at the core of this manuscript.

This quick overview of the contributions of Public Choice (deliberately omitting other topics such as why people vote) informs the scope of my research. It outlines the relevance of using economics and game-theory methods to describe and analyze collective choice process. While some of the conclusions of classical Public Choice may not be applicable blockchain-based systems, the methods are. They indicate important features to look at, such as the expression of intensity of preferences and the mechanisms presiding over constitutional settings, with a special focus on those designed to prevent free-riding. The four papers that constitute the remainder of this manuscript exhibit how they can be applied to the blockchain ecosystem.

1.2.2 Governance of the Commons

While Public Choice was originally developed to analyze national institutions (as illustrated by the focus on constitutions, national voting methods and bureaucracy), a group of scholars started studying institutions at various scales, notably how organizations formed between the market (atomic level) and the state. This section focuses on the work of Elinor and Vincent Ostrom (and other scholars belonging to their school of thoughts) on polycentric systems and the governance of the Commons. It provides a rapid historical account of their research and presents a detailed summary of E. Ostrom's Institutional Analysis and Development Framework (IAD), the theoretical framework she developed to describe governance systems. Other approaches of the Commons are also discussed to offer a comprehensive overview of this field.

Polycentricity

Research on polycentricity can be traced back to M. Polanyi (1951) who attempted to understand the conditions for preserving the freedom of expression, but the development of political economy theory on the matter owes much to the Ostroms. V. Ostrom, Tiebout, et al. (1961) marked the first attempt to demonstrate that polycentric systems with redundant institution and services was efficient in certain situations. Focusing on urban areas police forces, they demonstrated that, contrary to the dominant ideology at the time, different public goods necessitated different scales of provision. This paper initiated a research program continued by Vincent Ostrom and his wife Elinor that resulted in two main outcomes: first they provided a theory of polycentricity and second, they carried out empirical studies to identify and analyze polycentric systems. This empirical research, and in particular Elinor Ostrom's work has become the study of the Commons.

Aligica and Tarko (2012), citing Michael Dean McGinnis (1999) and V. Ostrom (1972) provides the following definition of polycentricity:

> Polycentricity emerges as a nonhierarchical, institutional, and cultural framework that makes possible the coexistence of multiple centers of decision-making with different objectives and values, and that sets up the stage for an evolutionary competition between the complementary ideas and methods of those different decision centers. (p.15)

These different centers may coexist at different scales and be entrenched with one another but they each have a purpose and an operational autonomy to provide a service. Importantly, all these decision centers, either competing or collaborating, are under an "*overarching system of rules*" (Aligica and Tarko, 2012). This larger system is central and often overlooked in the literature about polycentricity and is what bring unity to the system as a whole. It is also what allows users of a polycentric system to freely enter or exit a decision-center (change town for instance, see Tiebout, 1956). This overarching system provides unity, helps define the boundaries of the system and of its users, and is also often responsible for setting the constitutional environment, that is to say the rules to change rules. This unity and consistency of the system is what differentiates polycentric systems from other decentralized systems and also gives the system its legitimacy. V. Ostrom, Tiebout, et al. (1961) emphasized that this legitimacy is derived from "the rule of law" which ensures that all the members of the system are abiding to the same rules. J. Black (2008) claims that the legitimacy of polycentric systems can be pragmatically based (alignment of interests), morally based or cognitively based (a perceived feeling of unavoidability). This distinction is relevant in situations where the concept of "rule of law" may not apply.

As Duhnea (2021) recalls, Ostroms' focus on polycentricity and self-governance is close to Buchanan and Tullock's conclusion that there is no voting method that is appropriate to every situation and therefore that local autonomous systems within a larger constitution may be efficient. The proximity between these scholars was acknowledged by E. Ostrom in "Honoring James Buchanan" 2011. The theory of polycentricity was continued and applied to different systems notably by Michael Dean McGinnis (1999), a prominent member of the Bloomington School founded by the Ostroms. He broadened the scope of polycentricity as a governance theory and completed the work on Public Choice. While he has never mentioned DAOs, it is a natural extension of this work for they are multiple, decentralized and nonhierarchical decision-making centers under the overarching rules of a blockchain.

	Jointness of Use or Consumption	
	Alternative Use	Joint Use
Exclusion easy	**Private good** bread, shoes, automobiles, haircuts, books, etc.	**Toll good** Theatre, night club, telephone service, toll road, cable TV, electric power
Exclusion difficult	**Common-Pool Resources** water pumped from a ground water basin, fish taken from an ocean, crude oil extracted from an oil field	**Public Good** peace and security, national defense, mosquito abatement, fire protection, weather forecasts, "public" TV

Table 1.1: Types of Goods

Source: Adapted from Figure 1.3 E. Ostrom (2005)

Research on this topic already exists and is discussed in subsection 1.3.1.

From Polycentric Systems to the Commons

This focus on polycentric governance led E. Ostrom to study the governance of Common-Pool Resources (CPR). As she recalls in the edited version of the speech she gave upon receiving the so-called "Nobel Prize in Economics" (E. Ostrom, 2010), it is her work on polycentric systems, specifically on the water industry (E. Ostrom, 1965), that was at the origin for her interest for these goods that are neither private nor public goods. Prior to this research, the main economic theory was that there were only two types of organizations and two types of goods: the market was to manage private goods and the state was to manage pure public goods. However, the research on polycentric systems evidenced the limitations of this approach and led V. Ostrom and E. Ostrom (1977) to complement the Samuelson's typology of public and private good (1954). Some efforts had been done by Buchanan (1965) to define club goods and these resulted in the famous Table 1.1 that provided a first definition of CPRs as goods that have high subtractability (using the resource reduces what the others can derive from it) but for which it is costly to exclude other members. In these situations, neither private nor public governance is suited and Ostrom devoted much of her life to understanding the institutional settings associated with the governance of these common goods.

As she recalls in her speech, she developed this theory in a rather simplistic dual approach and this approach was also applied to CPRs. The question of the governance of CPR had been tackled in the famous "The Tragedy of the Commons" (Hardin, 1968) almost ten years before. Using elements of game-theory, Hardin demonstrated that CPR were condemned to overexploitation and depletion. His example is a “a pasture open to all. It is expected that each herdsman will try to keep as many cattle as possible on the commons” (p.2). Suppose only herdsman A puts an additional head of cattle (and surpasses the carrying capacity of the pasture): it decreases the productivity of the pasture as a whole and the cost is shared by all the herdsman but only A reaps the benefit of this extra head of cattle. If every herdsman follows this incentive logic, they each put as much cattle as they can afford which leads to overgrazing and ultimately to the depletion of the pasture. As Hardin puts it “Ruin is the destination toward which all men rush, each pursuing his own best interest[...] Freedom in a Commons brings ruin to all.” His model is akin to the famous prisoner’s dilemma in the sense that collaboration (limiting the size of the herd) would lead to a more efficient output but expecting that the others will act selfishly lead everyone to act selfishly results in a less efficient output. His conclusion, in line with E. Ostrom (2010)’s depiction of the dual approach that predominated at the times, is that to avoid this Tragedy of the Commons, the resource has to be managed under either a private market with individual property rights or with a public authority regulating the Commons. This *de facto* imposes the public/private typology and negates the possibility of other efficient means of governance.

While Hardin does not use the word free-riding, it is the concept at the core of his demonstration. Olson’s results thus indicate that it is possible for groups small or homogeneous enough to implement monitoring and sanctioning mechanisms that will prevent this tragedy of the Commons. Through her research on polycentric systems, Ostrom came to the conclusion that Hardin’s tragedy was nothing but avoidable. Explicitly building on Olson’s work (see E. Ostrom, 2005, pp. 25, 120, 253 for instance) she went developing what has become known as the theory of the Commons. Historically, the notion of Commons dates back to the Middle Age where Commons pasture and rights to forest were enshrined in the *Magna Carta* (Linebaugh, 2009) but were gradually taken away from commoners. The process of fencing Commons and establishing private property thus ending collective governance is known as *enclosures* and will be discussed in subsection 1.2.3.

Conceptualizing the Commons

The research program Ostrom initiated, with other prominent Bloomington School scholars such as Michael McGinnis, James Walker, Roy Gardner, Edella Schlager was three-pronged. It first defined a theoretical framework, grounded in game-theory, then it validated the predictions of the model through experimental studies before engaging in an extensive field work to describe and compare hundreds of case studies through a formal codification of the governance processes (E. Ostrom, Agrawal, et al., 1989). The theoretical work and learnings from the field studies resulted in a theoretical analytical framework called the Institutional Analysis and Development Framework (IAD).

First of all, E. Ostrom, Gardner, et al. (1994) distinguish two types of CPR problems:

Appropriation problems concern how to allocate the production of CPR to community members (and potentially to exclude some members). It is a flow problem, that can be modelled as a static game or a repeated independent game. It can further be broken down into three sub-categories:

- **Appropriation externalities** is when the action of one member to increase its own profit decreases the productivity for all the members. This is typically Hardin's tragedy of the Commons.
- **Assignment problem** is when the production of the resource is not homogeneous (typically some areas of a fishery have more fish) and the challenge is to assign the heterogeneous resource
- **Technological externalities** is when the use of one technology (such as trawlers) imposes a negative externality on all the members.

Provision problems is how to manage the stock of the resource. This can be either from the demand side (appropriation demand) or the supply side (how to maintain the resource). These problems can be represented with a time-dependent repeated game.

These problems can, and are often, nested and interrelated. Identifying the CPR problem(s) is only the first step as the authors define a CPR dilemma as meeting two condition (i) there is a suboptimal outcome, *i.e.* the CPR problem leads to inefficient outcome for the commoners and (ii) it is institutionally feasible to implement a coordinated strategy that will improve the outcome. It is the existence of these alternatives that Hardin did not take into account.

This classification of CPR problems illustrates that CPR situations should not be modelled as static prisoner's dilemma but as repetitive game (either time dependent or independent). Because commoners will manage the resource over a long period, the game can be considered as repeated. Failing to coordinate and comply with the rules at one stage of the game can be costly in the long run if the other participants are able to sanction free-riders. Game-theory predicts that, under some conditions, repeated games can lead to virtually any repartition of the payoff (Friedman, 1971) and therefore avoid the Nash Equilibrium (and the tragedy of the Commons in our case). One of the conditions is that the game is either infinite or that there is uncertainty about the timing of the end which can be the case in the governance of a CPR. Remodeling the CPR problems in such a way allows to predict that individuals with "bounded rationality"[10] may achieve efficient outcomes in face of CPR problems. This is facilitated by the capacity to communicate (at

[10] Michael D. McGinnis (2011) defines bounded rationality as follow: "Individuals pursue goals but do so under constraints of limited cognitive and information-processing capability, incomplete information, and the subtle influences of cultural predispositions and beliefs."

a low cost), to monitor behaviors and to sanction defection (E. Ostrom, Gardner, et al., 1994, part 1).

These predictions are verified in lab experiments and the different conditions are refined. E. Ostrom and J. Walker (1996) present the experimental setting, the two games played (for provision and appropriation), the different conditions and the expected behaviors. As anticipated, in poor institutional settings, where communication is impossible, the resource is often overexploited leading to a tragedy of the Commons. However, when communication is made possible, the outcome is more efficient. Even one-time communication leads to significant improvements but repeated communication is more efficient. The possibility to sanction is also a crucial aspect of the institutional environment and the efficiency of sanctioning mechanisms depends on the possibility to communicate. These conclusions generally apply both appropriation and provision problems. Interestingly for the case of blockchain-based communities, they find that face-to-face communication is much more efficient than computer-mediated communication. However, this point may be tempered by the fact that communication softwares and tools were much less developed at the time.

Because Ostrom's interest in the Commons originally stemmed from empirical work, such theoretical and experimental was only relevant if it matched observations and could be used to analyze governance processes. The analysis of hundreds of real-life situations also allowed the Bloomington School to describe the various ways of designing the complex institutional settings necessary for addressing CPR underprovision or overexploitation problems and it is this empirical research that formed the basis for the IAD.

The Institutional Analysis and Development Framework

First of all, it became apparent that it was necessary to redefine the notion of property. Classical economists usually consider individual property rights without much diversity,[11] but work on CPRs demonstrated that the property regime (private, governmental, community or no property rights) was independent of the nature of the good as a CPR (Bromley, 1986). Schlager and E. Ostrom (1992) also showed that the property rights in CPR governance was a continuum and that property rights systems were best described as *bundles of rights*. Along this continuum, 5 frequent types of right can be placed:

Access concerns the right to enter the resource.

Withdrawal concerns the right to extract some goods from the resource (for instance collect wood or fish certain species).

Management concerns the rights to maintain and shape the resource.

Exclusion concerns the right to control who has the previous rights.

[11] An approach consistent with the legal *numerus clausus* existing in many countries.

DP1 Clearly defined community boundaries 1a. Clear and locally understood boundaries between legitimate users and nonusers are present. 2b. Clear boundaries that separate a specific common-pool resource from a larger social-ecological system are present.	**DP5 Graduated sanctions** Sanctions for rule violations start very low but become tougher if a user repeatedly violates a rule.
DP2 Congruence between rules and local conditions 2a. Appropriation rules are congruent with local social and environmental conditions 2b. Appropriation rules are congruent with provision rules; the distribution of costs is proportional to the distribution of benefits	**DP6 Conflict resolution mechanisms** Rapid, low cost, local arenas exist for resolving conflicts among users or with officials.
DP3 Collective choice arrangements Most individuals affected by a resource regime are authorized to participate in making and modifying its rules.	**DP7 Local enforcement of rules** The rights of local users to make their own rules are recognized by the government
DP4 Monitoring 4a. Individuals who are accountable to or are the users monitor the appropriation and provision levels of the users 4b. Individuals who are accountable to or are the users monitor the condition of the resource.	**DP8 Multiple layers of nested enterprises** When a common-pool resource is closely connected to a larger social-ecological system, governance activities are organized in multiple nested layers.

Table 1.2: Ostrom's 8 Design Principles

Source: Cox et al. (2010) and E. Ostrom (2005)

Alienation concerns the right to pass on (either give or sell) any of these rights.

Although having one of these rights often implies having the ones listed before, it is not necessarily the case (for instance one could consider nue-propriété or *abusus* in French Law as examples of alienation right without access, withdrawal and management rights).

The cross-analysis of the diverse case studies coded by the Bloomington School allowed Ostrom to identify regularities and common structures found in most of the governance institutions (E. Ostrom, 1990). She coined the term "Design Principle" to describe these abstract features. Also referred to as Ostrom's 8 Design Principles (hereafter DP), they are indicators of sustainable governance of a CPR by a community and constitute a list of factors to look at to assess a governance process. These DP are often found in successful CPR but are by no means necessary. The 8 DP are presented Table 1.2 in an edited version by Cox et al. (2010) endorsed by Ostrom .

These indicators can be met through dozens, if not hundreds, types of implementations. In a way, they represent a static assessment of the institutions that indicates whether it is likely that they will result on sustainable governance of the resource but lack the details of the arrangements that lead to whether these DPs will be met or not. Fortunately, Ostrom also provided scholars and practitioners studying the Commons with the tools to do so. As phrased by Michael D. McGinnis (2011):

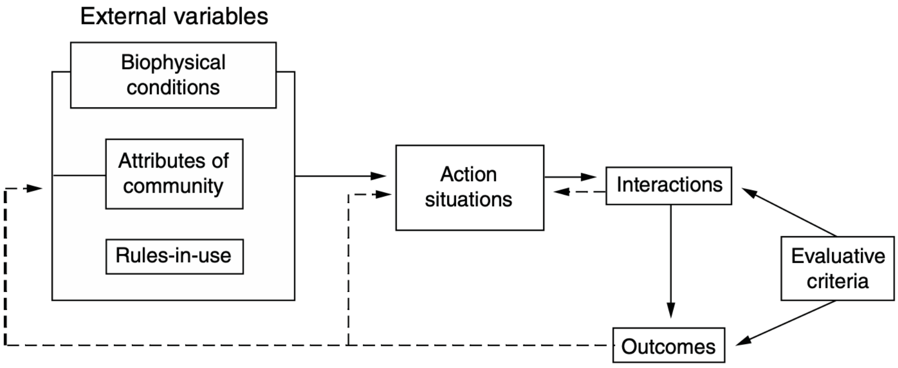

Figure 1.3: A Framework for Institutional Analysis

Source: E. Ostrom (2010, Figure 2)

> The IAD framework assigns all relevant explanatory factors and variables to categories and locates these categories within a foundational structure of logical relationships. Although designed as a tool to simplify the analytical task confronting anyone trying to understand institutions in their full complexity, over time this framework itself has become quite complicated.

Despite this complexity and the apparent redundancy of some elements of the IAD, I here review as thoroughly as possible the formal elements of the IAD as a significant part of the original research presented in this manuscript elaborates on the language and the grammar of the IAD.

Ostrom first defines the system she studies as an *action situation* comprised of the actors and the rules they adopt in relationship with the CPR. This action situation is situated in a broader context that informs and affects it, as described Figure 1.3. The inputs characterize the three traits of the CPR (the community, the resource in its biophysical environment and the rules at play). The outcomes of the governance and their interaction with the external environment are evaluated by the commoners to inform future actions in a feedback loop depicted by the dotted lines.

The central part of the framework is the action situation, “a black box where policy choices are made” (Michael D. McGinnis, 2011, p.172). It can in turn be broken down into different components depicted inside the square in the Figure 1.4. Ostrom conceptualized these internal components in order for them to be consistent with the grammar and the habits of game theorists so that the framework is applicable both experimentally and empirically. The seven variables constituting an action situation are: (i) the participants, (ii) the position they may have, (iii) the actions associated with these positions, (iv) the information available to different positions, (v) the outcomes possible, (vi) the way positions and participants affect outcomes, and (vii) the distribution of the costs and benefits

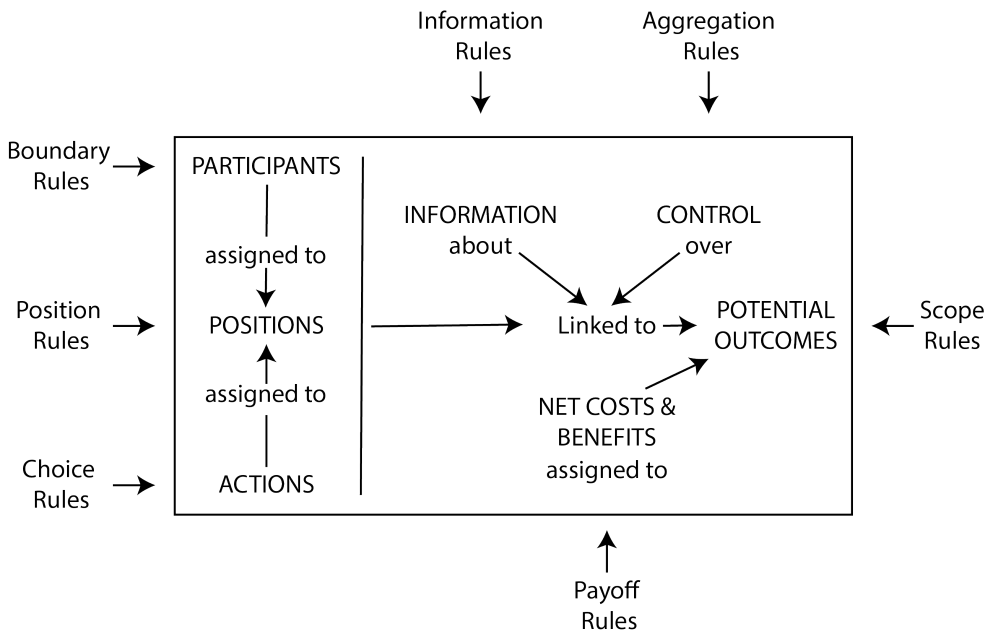

Figure 1.4: Elements of an Action Arena

Source: E. Ostrom (2005, Figure 7.1)

associated with the outcomes to the different participants and positions

To each of these components is associated a *rule* set by the community to specify their potential values. Still using McGinnis' definitions (2011 p.174) there are:

Position rules specify a set of positions, each of which has a unique combination of resources, opportunities, preferences, and responsibilities.

Boundary rules specify how participants enter or leave these positions.

Choice rules specify which set of actions is assigned to which position.[12]

Aggregation rules specify the transformation function from actions to intermediate or final outcomes.

Scope rules specify a set of outcomes.

Information rules specify the information available to each position.

Payoff rules specify how benefits and costs are required, permitted, or forbidden to players.

[12] Ostrom uses *choice rules* while McGinnis prefers *authority rules*.

When applying the IAD framework, one must describe the modalities of implementation of these rules. Typically, the boundary rules are often dependent on criteria such a physical location (membership to a village, a family. . .), personal characteristics (age, sex, ethnicity. . .) or history (past ownership, actions in favor of the resource...). But positions can also be distributed at random, notably for assignment problems or after paying a fee. E. Ostrom (1999) identifies 27 boundary rules and 112 choice rules. Payoff rules crucially define the sanctions and Ostrom notes that; while variations exist, three general types of payoff rules are generally used by commoners: (a) the imposition of a fine, (b) the loss of appropriation rights, and (c) incarceration. Consistently with previous findings, this shows the importance of being able to monitor and sanction defectors to manage sustainable governance. The monitoring rules (part of the information rules) also vary depending on the CPR and whether everyone monitors or if a guard is hired to enforce the rules. In both cases, adequate position rules must be crafted consequently and, in the case of a guard position, the payoff rules must also account for the salary of the guard. This exemplifies how entrenched these rules are and how important it is that that are suited to the local context (DP2).

How these rules will be decided upon by the community depends on many socio-cultural factors as well as on external variables such as related action situations and other institutions. This is mentioned in the DP2, DP7 and DP8 but deserves a section on its own in the IAD. In particular Ostrom distinguishes four choice levels (E. Ostrom, 2005, ch.2) nested in one another as represented in Figure 1.5. The *operational choice* level concerns the rules affecting day-to-day practical operations, *collective choice* level concerns the making of institutions, policy making and specifies how operational rules can be modified, the *constitutional choice* level informs legitimizing the collective choice, deciding who can participate to the lower levels and provides legitimacy to the system in general. Finally, the meta-constitutional level refers to long-lasting principles such as social norms, traditions or external constraints (national law) that the participants cannot immediately modify but that shape all the rules at play.

Lastly, an important feature of a CPR is the role of trust as an attribute of the community. In the wake of economists such as Arrow, who considered trust as an essential condition for contracting and engaging in trade, Ostrom also demonstrates that trust allows to address the threats of free-riders through norms of reciprocity and to overcome social dilemmas.

All these elements form the IAD, an evaluative framework that provide economists, sociologists and anyone interested in the governance of a CPR with tools and methods to describe and analyze an action situation. It is a very formal framework with its own abstract language that can deter new readers but this abstraction has proved useful in an array of contexts overtime and there is still an active area of research to complement the

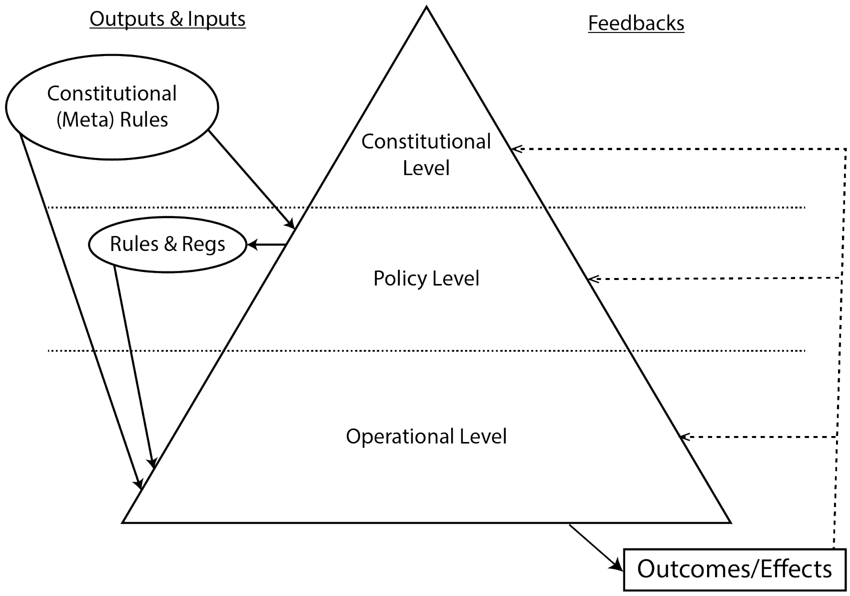

Figure 1.5: Levels of Analysis

Source: Cole (2014, Figure 2)

IAD framework.[13] The chapters 4 and 5 participate to this effort.

1.2.3 Researching the Commons

After a life dedicated to developing a framework for the analysis of natural Common-Pool Resources such as water management systems or fisheries, Ostrom started working on how her work could be applied to other action situations and specifically to Knowledge Commons. Hess and E. Ostrom (2007) edited *Understanding Knowledge as a Commons* that lays the cornerstones for research on Knowledge Commons. Distributed knowledge, such as digital libraries, Wikipedia or Free and Libre Open-Source Software (FLOSS) are Commons in the sense that they are "a shared resource that is vulnerable to social dilemmas" (p.13). Most of the time, Knowledge Commons are non-subtractable: consulting a Knowledge Commons does not prevent others from accessing the information and, according to Ostrom's typology, they face a provision problem while appropriation is relatively easy. In the third chapter E. Ostrom and Hess (2007) demonstrate how the IAD framework may apply. In particular, they underline that defining the entire community may be harder for Knowledge Commons than for physical resources but functional positions such as *content provider*, *users* or *policy makers* can still be identified. The rest of

[13]Research by the Bloomington School on the IAD has led to the development of the Social-Ecological Systems Framework (SES),a revision of the IAD with more emphasis on the biophysical aspect of the IAD. It is beyond the scope of this dissertation to review but the interested reader can find an introduction in M. McGinnis and E. Ostrom (2014).

the framework, including choice levels and the bundle of rights, applies, although some modifications may be required to fit the specificities of Knowledge Commons. Part of the research presented in this manuscript aims at proposing such modifications in the case of blockchains.

In an effort to identify these Knowledge Commons, Hess (2008) notes that they are just one of the seven types of the "new Commons" along with cultural Commons, medical and health Commons, neighborhoods Commons, infrastructure Commons, global Commons, and market as Commons. She further identifies the subcategories of the Knowledge Commons: digital divide, education, intellectual property rights, internet, libraries, public domain, science and peer production. These Commons have been studied by prominent scholars who helped conceptualize Knowledge Commons (Bollier, 2007, 2014; Boyle, 2003). Benkler (2006)'s work on Commons-Based Peer Production (CBPP) is especially relevant to this dissertation. A CBPP is a Knowledge Commons in which the content is open and produced in a peer-to-peer network in a decentralized way. CBPP are thus an organizational way of harnessing individual decentralized knowledge to produce knowledge accessible to all. Most famous examples include Wikipedia, Linux and OpenStreetMap for instance. Blockchains can be considered and studied as CBPP and it is still on ongoing research topic. We contribute to this research in chapter 2.

While clearly related to Ostrom's research, the works on the various "new Commons" also evidences that research on the Commons is still active with different fields of research. Although not directly related to my research that only uses the economic foundations of the theory of the Commons, I want to conclude this section on the Commons by a rapid review of these trends in different disciplines. K. Polanyi (1944) showed that the movement of the enclosures, threatening the Commons in the 18th had been at the origin of the market and that it remained an important concept. This term is now generally used to refer to any threat on a Commons (Boyle, 2003). Because of this link with the market economy, many theorits have studied the Commons as tools to counter neo-liberalism. Le Roy (2016) proposes a dual categorization of the Commons: the "primo-Communs" (ancient Commons) predate the legal system and private property while the "néo-Communs" (neo Commons) are similar to Hess' new Commons in the sense that they try to create alternatives to the market and neo-capitalism within the modern legal framework. Ancient Commons are now rare in the Global North were the legal systems in place for centuries (either Common Law or Civil Law) has facilitated enclosures but they remain frequent in the Global South (although threatened as discussed in subsection 5.4.1).

Among the prominent academics advocating for more neo-Commons is Bollier, a neo-marxist who has proposed a dynamic approach of the Commons based on *commoning*. He moves the focus away from the resource and puts it on the social process of exercising the governance and actively engaging in making a Commons (Bollier, 2014). Although he does not belong to the Bloomington School, he defines Commons as a set made of a resource, a community and a set of rules, an approach that is strikingly close to the elements of an action situation in the IAD. The Commons are seen as a promising tool to promote alternative models in the face of the environmental crises humanity is currently facing. However, the current legal systems are generally not enabling for the Commons and Gutwirth and Stengers (2016) call for legal innovation to stimulate the practice of the Commons. Similarly, Coriat (2015) proposes a role for the state as an enabling institution for the Commons. Philosophers and sociologists Dardot and Laval (2015) have a more anarchist approach, seeing the Commons as way outside of the state and the market.

These different approaches and controversies in the field of the Commons and specifically their legal status and relationship with national institutions echo that of the blockchain and DAOs mentioned subsection 1.1.4. Because blockchain-based tools are still mostly "a-legal" (De Filippi and Wright, 2018), they may be suited to governing and creating neo-Commons without being constrained by legal dispositions (chapter 5 demonstrates what it offers in a context of legal pluralism) and, in turn, literature on the Commons can inform the legislation around blockchain. My approach in this manuscript integrates the role of the government and diverges from the most libertarian positions reviewed here. The next section presents the state of the art in the scholar literature linking blockchains(-based) governance and political economy.

1.3 Blockchains and Political Economy

This section reviews the efforts to use methods from the political economy to characterize blockchain(-based) communities. The previous section showed the relevance of such an approach it represents an active field of research. I start by reviewing the general literature linking political economy and blockchains and then I discuss the extent to which blockchains can be considered and studied as Commons before focusing on the use of blockchains for the governance of the Commons.

1.3.1 The Political Economy of Blockchains

I have already pointed out that blockchains and Public Choice share common features such as a conception of human agents as rational individuals maximizing profit and seeing contracting as a way to reduce costs. This has naturally led to applying elements of political economy to blockchain systems. Davidson et al. (2016a,b) argue that blockchains are an institutional technology and therefore that institutional economics and Public Choice are well-suited to their analysis. In the tradition of the New Institutional Economics (NIE), Davidson et al. (2018) study how blockchains as institutions affect the costs of interaction. In the wake of Coase (1937, 1960) they demonstrate that blockchains are likely to lower transactions costs in the face of uncertainty. In the Coasian tradition, Williamson (1985, 1993) justified the firms as way of controlling opportunism and the authors contend that blockchains are also capable of reducing these costs. Yet, they argue, this does not mean that blockchain-based institutions should be likened to firms but rather that they are a new category in Williamson's typology of "economic institutions of capitalism" made of markets, hierarchies and relational contracting. The new category, that they call decentralized collaborative organization (DCO), has "the coordination properties of a market, the governance properties of a commons and the constitutional, legal and monetary properties of a nation state" (p.16). It follows that blockchains institutions must be studied as a new institution and that tools from political economy help characterizes it.

In a book about Public Choice, Rajagopalan (2019) argues that blockchains must be conceptualized as both rules and constitutional rules because they also frame how the rules will be made. In the following chapter, C. Berg et al. (2019) defend that blockchains are constitutional orders, defined as "rule-systems in which individuals (or firms, or algorithms) can make economic and political exchanges" (p.384). This has two consequences: the first one is that constitutional economics (and most specifically the work of Buchanan, Tullock and Ostrom) can adequately study blockchains, the second is that blockchains constitutional orders are an experimental playground for new forms of institutions. In these new settings, "the rules of the game in blockchain applications are written into the code itself [and] unconstitutional transactions simply will not execute" (p.384). A prominent quality of these constitutional orders, noted by virtually all the authors reviewed in this section, is that of forking. Because blockchains users always have the possibility to fork, it requires all the participants to reach consensus. As noted above, the possibility to opt out is central in the theory of polycentricity (V. Ostrom, Tiebout, et al., 1961) but it is rarely that simple in real life situations.

In the same research group, A. Berg et al. (2018) introduce "crypto public choice - the application of public choice to blockchain technology". They show how the different fields of Public Choice resonate in blockchains such as Olson's theory of interest groups and the provision of public goods. Detailed attention is devoted to blockchain-based e-voting (BEV) and how it affects "crypto-democracy". D. W. E. Allen et al. (2017) and D. W. E. Allen et al. (2018) explore how new forms of voting such as Quadratic Voting—a point-based voting system with a squared cost functions for additional votes theorized by Posner and Weyl (2015)—may reduce costs. C. Berg (2017) discusses how BEV allows to move away from geographical voters' bundles. My work on Liquid Democracy is in the same vein, exploring new institutional possibilities allowed by blockchains and using methods from political economy to assess their potential. Focusing on other constitutional arrangements I extend this work but have less optimistic conclusions for Liquid Democracy.

Other researchers, such as Meijer and Ubacht (2018) have applied NIE to blockchains and characterize the new institutions they form, focusing on trust. They show that blockchain institutions allow to disintermediate trust in highly institutionalized values environment. They postulate that blockchains are control rather than trust mechanisms. They also demonstrate that blockchains increases control over counterparties (third party) but reduces control from a system perspective because it shifts powers to other actors such as miners. That these conclusions are close to those of De Filippi, Mannan, et al. (2020) on trust and confidence (see subsection 1.1.4) that underlie the chapters 2 and 4.

Frolov (2021) proposes an "extended institutional approach" as a reaction to over simplistic analyzes of blockchains that tend to dismiss the role of intermediaries and believe that pure blockchain systems can replace most existing institutions. Consistently with the message conveyed in this manuscript, he champions that "constitutional complexity matters" and focuses on how the assemblage of diverse institutions such as blockchains, markets, and public actors may self-organize into an organized system.

Aiming at reconciling blockchains as constitutional orders in a complex institutional environment, Alston et al. (2022) demonstrate how competing networks (Bitcoin, Ethereum, Tezos or Monero for instance) act as polycentric orders. They use this polycentric approach to explain how the main blockchains have changed over time due to internal processes (detailed by institutional analysis) and external competition (mostly with other networks). Their results on blockchain competitions are similar to those of Lee et al. (2020) who propose a political economy model of blockchain governance inspired by the early models of Downs (1957). My research on the Commons does not dwell on the polycentric side of the IAD and, therefore, complements these papers. A specific discussion of polycentricity in the blockchain Commons, adopting the formal language of the IAD, would be a compelling extension of this dissertation.

Overall, there are several conclusions I draw literature. The first one is that the conceptual proximity of blockchains foundations and political economy is a fertile ground for research. The research program proposed by A. Berg et al. (2018) is still very much open despite ongoing efforts. The second is that it is becoming increasingly clear that blockchains allow to experiment new forms of institutional organizations, in particular new constitutional orders. Interestingly, these new institutions take place both at the infrastructure level—as the governance of the blockchain itself requires new institutions—and at the DCO or DAO level as well. The nestedness of these levels is well described by a polycentric model. Third, blockchain institutions are set in an extremely complex web of other institutions (as discussed in subsection 1.1.4). As blockchains cannot entirely substitute for trust and represent new power dynamics (O'Dwyer, 2015), they should be contemplated as part as a complex web of institutions.

1.3.2 Blockchains as Commons

The previous section has demonstrated that blockchains are polycentric systems that do not match either market systems or public institutions and it is thus logical to apply the theory of the Commons to blockchains to depict and analyze their governance processes. There have been a few attempts at applying Commons framework to blockchains in general or to specific case studies. Listing them, this section discusses their contrasted conclusions and proposes a new perspective on the current state of the art literature.

The first approach of blockchains as Commons was to find the theoretical frameworks most suited to grasp the specificities of blockchains. My research builds on the IAD framework but other ones are useful to study other aspects of the blockchains. Potts (2018) argues that blockchains are well described by a Hayek-Williamson-Ostrom framework that views them as examples of the *innovation commons* described as "a governance mechanism to create a pool of innovation resources with respect to a new idea or technology of uncertain prospect" (p.4) and he proposes an *ad-hoc* institutional framework to analyze innovation commons. Ostrom's insights help characterize these governance mechanisms as Commons. The author contends that that innovation commons are a new category of "the new Commons" and further subdivide them into two different Commons: (i) the first resource is the materials and technology, and (ii) the second is the information produced by the innovation commons. In this research, Potts introduces a conceptualization of blockchains a new type of Commons.

In a conceptually close approach, A. Berg et al. (2018) have also identified the public goods produced by blockchains and identify two: consensus and security. While they do not define these public goods as Commons, this step is taken by Potop-Butucaru (2021) who considers that the blockchain version of the tragedy of the Commons is the risk that block validators stop their participation in the PoW or PoS competition thus lowering the security of the network.

These three papers consider some aspects of the blockchains that pertain to the domain of the Commons but do not engage in a full-fledged definition and analysis of blockchains as Commons. This work is undertaken by Bodon et al. (2019) in *Ostrom Amongst the Machines*, where they argue that blockchains are a Knowledge Commons. They suggest that a Hayekian formalization of blockchains may be relevant to explain how blockchains emerge as spontaneous orders but that Ostrom's theory is necessary to understand their self-governance. They build on Hess's Knowledge Commons and specifically on the "Governing the Knowledge Commons" (GKC) framework by Frischmann et al. (2014) and Madison et al. (2010) for "constructed cultural commons" and the social dilemmas that Knowledge Commons are capable to resolve. The framework allows them to answer six clusters of questions that summarize Knowledge Commons. This allows them to start disentangling the narrative behind blockchains and Commons and the complex institutional environment of blockchains. They also characterize blockchains users and discuss some features such as property rights systems and dispute resolution mechanisms.

Their work is largely extended and completed by Murtazashvili et al. (2022) who develop this analysis and apply it specifically to the case study of Bitcoin. They recall that "'Knowledge Commons' means governance (i.e., rules and norms) of a shared information or knowledge resource by some collective or community." (p.110) This definition alone justifies why scholars study blockchains as Commons. In particular, they expand on the notion of social dilemmas and explain that Commons governance is an institutional way of addressing a social dilemma defined as a trade-off between individual and social welfare.

With this definition, they demonstrate that blockchains solve some social dilemmas and create others. They defend that thinking blockchains as Knowledge Commons helps to give a detailed account of these dilemmas and to distinguish between what relates to Commons governance and what does not in the world of blockchains. To illustrate the relevance of their framework (the six-pronged GCK), they apply it to Bitcoin. Though their conclusions as to whether Bitcoin is Knowledge Commons are ambiguous, their analysis contributes to delineating the different parts of the governance mechanisms of Bitcoin As the authors argue in their conclusion, using the GCK framework, a relatively easily actionable framework, may prove useful to conduct comparative analysis of different case-studies.

Going deeper in the Commons theory of blockchains, Howell and Potgieter (2019a) have applied the IAD to three blockchains: Ethereum, Bitcoin and Sovrin. Although their conclusions may be the most pessimistic concerning the characterization of Bitcoin and Ethereum as Commons, their work is the most thorough to the extent of my knowledge. If Shackelford and Myers (2016) had already assessed Ostrom's 8 Design Principles (DP) for blockchains as action situations, their work remained superficial and did not encompass all aspects of the IAD. Similarly to Murtazashvili et al. (2022), Howell and Potgieter start by explaining why blockchains can be considered as CPRs, mostly from a resource-based perspective: information is non-excludable with a high risk of free-riding managed by a community. They then go on analyzing each of the IAD elements, including the biophysical characteristics, the attributes of the community and the rules-in-use (see Figure 1.3). Their characterization of the community identifies the different types of users such as external app users, coin owners and node operators and also builds on the "bundle of rights" to define software developers as *custodians* with management rights. They advance that the rules-in-use are implicitly derived from rules of open-source community and that the lack of formalization jeopardizes a proper Commons governance. In particular, the technicality of many governance decisions *de facto* excludes many users. Through the characterization of all the components of the IAD (action situation, interactions, evaluative criteria and outcome), they are able to substantiate their assessment of the 8DP and find that:

Clearly defined community boundaries (DP1): there are no boundaries to join the blockchain but that there are high entry costs to the governance process because skills and knowledge are required

Congruence between rules and local conditions (DP2): the conclusions are unclear

Collective choice arrangements (DP3): because only node operators are effectively capable of implementing governance decisions, most users, including coin-owners are excluded from the decision-making process. Note that this would be different in a PoS system.

Monitoring (DP4): there is little accountability to the appropriators (coin-owners)

Graduated Sanctions (DP5): there are no sanctioning mechanisms for rule violation

Conflict resolution mechanisms (DP6): conflict resolution is extremely costly if not impossible due to blockchains' immutability

Local enforcement of rules (DP7): because blockchains are mostly a-legal, this question remains unresolved

Multiple layers of nested enterprises (DP8): the intrinsic distributed nature of blockchains makes it hard for them to be nested in a larger CPR but this does not constitute a limitation to considering blockchains as Commons.

They end up concluding that, while Ethereum and Bitcoin theoretically have all the characteristics of CPR, they fail to meet most of the design principles. This is mostly due to the fact that, in PoW blockchains, appropriators (coin-owners) do not participate as much in the governance as other actors (node validators, software developers, foundations...) and they claim that other blockchains may have better governance systems (notably through PoS). Although I find that their application of the IAD is the most comprehensive to date, I disagree with some of their conclusions. Notably I believe that they have not acknowledged the specificities of the blockchains, in particular in terms of *ex-ante* codification. Therefore, their approach to the fourth and fifth principles may be too conservative. Their conclusion is that "[one] cannot exclude the possibility that stable arrangements outside the IAD framework are possible", thus appreciating that the novel institutional arrangements reached by blockchains may still be sustainable. I believe that extending the IAD to integrate these new arrangements is a promising research project and this manuscript contributes to it.

To summarize this survey, I find that although there are competing approaches to seeing blockchains as Commons, they all agree on the theoretical premises that blockchains as institutional arrangements meet all the criteria for being considered a Commons. Applying frameworks from the Commons theory (either the IAD or Knowledge Commons specific ones) indicate shortcomings in the current governance processes but evidence that this approach should not be general but applied to each blockchains separately as the rules-in-use and the communities may vary. This invites scholars and practitioners to mobilize the theory of Commons to understand and maybe influence the governance of blockchain systems but also to learn from the new governance processes enabled by the automation and transparency of the blockchains.

1.3.3 Blockchains for the Governance of the Commons

Considering blockchains as Commons also makes it natural for the readers to consider whether blockchains can be the support for the governance of a Commons. Ostrom's eighth design principle (DP8) indicates that multiple levels of CPR can be nested which leads to research and experimentation on DAOs as governance tools for the Commons. To the best of my knowledge, the first works in this direction date from March 2015 when Bollier (2015), citing a blog comment by Primavera de Filippi, and O'Dwyer (2015) postulated that blockchains might support some Commons, and specifically commons-based peer-production (CBPP).

This work was followed by attempts to translate the values of the CBPP onto the blockchain in order to leverage the blockchains for the governance of CBPP (De Filippi, 2015). This entails identifying the value metrics of CBPP community and quantifying indicators such as reputation to design reward systems through tokenomics. This was experimented by the project of Backfeed (who stopped and was continued by DAOstack) that aimed at "enabling a new system of values" thanks to blockchain technology (Pazaitis et al., 2017). Consistently with what has been reviewed in subsection 1.1.5, the authors note that, like in the rest of the economy, blockchains applications are largely "associated with the capitalist mode of production" (p.108) and explore how they could, in turn, support *commoning*. Backfeed was a platform with this goal, facilitating coordination and valuing the sharing economy, explicitly integrating a trust layer to its institutional arrangement.

The challenges associated with developing a system of value compatible with the Commons on a blockchain are also analyzed by Cila et al. (2020) in a more general context. They identify 6 design dilemmas that a community of commoners must address when conceiving a blockchain-enabled governance system. They illustrate their approach through a fictional case study of a decentralized energy community that face the different dilemmas. This methodology has inspired Simona Ramos and I in the paper presented chapter 5. The design dilemmas, that are conceptually similar to the social dilemmas mentioned in the previous section and are grouped into three categories: tracking, managing and negotiating as summarized in Table 1.3. The tracking dilemma refers to the transparency of blockchains that may reveal private information. What is more, the permanency of the data recorded on a blockchain compromises the right to be forgotten. These questions are largely debated in the blockchain sphere because they also concern digital identities (Siddarth et al., 2020) and must be considered on case-by-case basis. The managing dilemmas are close to those discussed by Pazaitis et al. (2017) in the sense that they concern the issues associated with the rules of the DAOs and how tokenization may modify the different aspects of the governance process. The dilemmas are how to incorporate non quantifiable social values or how to quantify them without denaturing them. Related topics are how to encourage certain behaviors, either through economic incentives or social pressure (nudge). In case of conflicting interests between individuals and the collective, they claim that the question of how the arbitrage should be made must be answered beforehand. Lastly, the negotiating mechanism refers to the trade-off between human and algorithmic governance: the said arbitrage can be algorithmically implemented through automation or can depend on human

Mechanisms	Design Dilemmas
Tracking	1. Transparency vs. Privacy
Managing	2. Economic value vs Social Value
	3. Quantified vs. Qualified Values
	4. Incentivization vs. Manipulation
	5. Private vs. Collective Interests
Negotiating	6. Human vs Algorithmic Governance

Table 1.3: A summary of the design dilemmas operative per mechanisms

Source: Figure 1 from Cila et al. (2020)

assessment of the context. Because blockchains smart-contracts need to codify *ex-ante* all the potential situations, they may have less scope and flexibility than human agency. They suggest that backdoors, to allow the community to interrupt a smart-contract, may be a promising solution. While they do not provide a guideline to solve the design dilemmas, they raise awareness on the difficulties that must be expected by practitioners. All these trade-offs are interconnected and can be solved along a spectrum of solutions. They also make the following recommendations: (i) it is important to keep a human in the loop with a "kill-switch" in case unforeseen situations happen; (ii) the economic values underlying the tokenomics of the system must be explicit so that any bias in the quantification[14] can be taken into consideration by every commoner; and (iii) the social and ethical values should also be explicitly presented so that everyone can embrace or discuss them. Conceptually, the last two recommendations encourage the formalization of the rules-in-uses at both the operational, the policy, the constitutional, and the meta-constitutional levels. In chapter 5, we concur and show that in certain situation where traditional Commons governance has failed, the formalization of the rules necessitated by a DAO may reinstate trust and confidence and thus facilitate sustainable management.

The most complete effort to date to analyze how blockchains can be used for the management of the Commons—and one that has heavily influenced the previous paper—is the paper "When Ostrom Meets Blockchain: Exploring the Potentials of Blockchain for Commons Governance" (Rozas, Tenorio-Fornés, Díaz-Molina, et al., 2021) who provide an extensive discussion of how blockchains can help manage CBPP and contribute to a governance system that meets Ostrom's 8 design principles. To understand the novelty of blockchain-governance, they build on the notion of *affordances*, as "functional and relational aspects which frame, while not determining, the possibilities for agentic action in relation to an object" (Hutchby, 2001, (p.444) as mentioned by Rozas, Tenorio-Fornés, Díaz-Molina, et al., 2021). They find 6 affordances: (i) tokenization; (ii) self-enforcement

[14] They recall that "Creating an economy where certain elements (e.g. energy produced, services provided, expertise and know-how) have an intrinsic value that can be accumulated or used in transactions is not socially and politically neutral by far" (Cila et al., 2020, p.10).

	Tokenization	Self-enforcement and formalization	Autonomous automatization	Decentralization of power over infrastructure	Transparentization	Codification of trust
Clearly defined community boundaries	✓					
Congruence between rules and local conditions	✓	✓		✓		
Collective choice arrangements	✓			✓		
Monitoring		✓	✓	✓	✓	
Graduated sanctions		✓	✓			
Conflict resolution mechanisms			✓		✓	
Local enforcement of rules		✓		✓		✓
Multiple layers of nested enterprises			✓			✓

Table 1.4: Relationship Between Blockchain Affordances and Ostrom's Design Principles

Source: Table 1 from Rozas, Tenorio-Fornés, Díaz-Molina, et al. (2021)

and formalization; (iii) autonomous automatization; (iv) decentralization of power over infrastructure; (v) increasing transparency; and (vi) codification of trust. Also relying on theoretical examples, in this case community networks, they discuss at length what these affordances can offer in terms of governance services and which of the design principles they can help meet. Their results are summarized in Table 1.4 and it appears that the affordances theoretically allow to meet each of the design principles, making it possible to encode a governance process over a DAO. In their discussion they also point out the need to take into account the limitations of full tokenization and keep human-based governance in the system. Their take is designed to explicitly avoid the limitation of techno-determinism and propose a constructive approach. This work has been extremely influential and has served as a cornerstone in the discussion around Commons-oriented blockchain-based governance. As they mention in their conclusion, many projects already, in practice, build on the methodology they theorized.

This paper has greatly influenced the research presented in this dissertation because it attempts to provide tools to analyze governance processes, but also to inform the conception of future blockchain tools and to frame directions in blockchain-based governance. I happen to share these objectives and hope my research can also contribute in that direction. The papers presented in chapter 4 and 5, build on this work and apply the same methodology to other aspects of the IAD framework than the design principles and identifies potential case-studies. In doing so, I am also in line with another of their paper, where they have completed their work with a discussion of other types of Commons and notably non-rival (digital) global Commons (Rozas, Tenorio-Fornés, and Hassan, 2021). They find similar conclusions as to the potential of blockchain-based governance and call for further research on other types of Commons. My research contributes in the case of natural CPRs.

Generally speaking, the field of a Commons-oriented theory of blockchain-based governance is recent, with the most important papers dating from 2018 onwards (for the working papers) but has attracted a lot of attention for it is a promising direction for the development of non-financial blockchain applications. Time will tell whether diverse communities of commoners will utilize blockchain-based tools but, along with other scholars, I aim to build the theoretical ground for such practices to multiply.

Maximal Extractable Value and the Blockchains Commons

This paper is co-authored with Primavera de Filippi and Bruno Deffains and is a contribution to a special issue of the *Terminal* journal on Blockchains (the original paper was submitted in French). In this first paper, we address the governance *of* the blockchain rather than *by* the blockchain as will be the case in the next ones. We propose a Commons-oriented discussion of a topical issue in the governance of Ethereum, Maximal Extractable Value (MEV), and we wish to add to the current debate on the appropriation of value in the blockchain ecosystem. We call for community involvement and collective decision-making and suggest that in the prevailing situation, blockchain users face a new sort of free-riding. The special issue should be released early 2023.

Abstract

This paper shows how some MEV practices, resulting in unfair appropriation of the value created by all users, by a small set of blockchains actors is similar to free-riding. In particular we demonstrate that this new form of free-riding is made possible precisely by the design of blockchains that aims at preventing classical forms of free-riding. This also entails that non-cooperative game theory is not adequate to solve the issues raised by such MEV practices. We thus turn to cooperative games, in particular in the case of Commons goods. After recalling that blockchains are a specific type of Commons goods we dwell on Ostrom's theory of the governance of the Commons, in particular on her design principles to analyze MEV practices and their impact on users confidence in the network. We then go on proposing new avenues for possible solutions, based on collective participation and we note that a trust-based solution may be efficient to sustain confidence.

Maximal Extractable Value and the Blockchains Commons

P. Poux, P. de Filippi & B. Deffains

2.1 Introduction

Contrary to centralized databases, whose data is stored on a centralized server or on a data center managed by a single authority, a blockchain is a decentralized datastore whose data is replicated across multiple nodes on the network. There are two broad typologies of actors involved in a blockchain network: *network users* and *network operators*. Network users are those who submit messages to the network in order to execute a particular transaction. Network participants can, in turn, be categorized into two sub-categories: those responsible for recording new transactions in the blockchain (*block producers* or *miners*) and those responsible for verifying the validity of these blocks (*block validators*). While the work of validators is relatively straightforward, that of block producers can be very costly in terms of time and energy. Hence, block producers are incentivized through block rewards: a fixed award of cryptocurrency automatically granted to the producer of each new block. In order to account for the fact the block reward decreases over time (e.g. in the case of Bitcoin, the reward assigned to the miners halves every 210,000 blocks mined), block producers are further incentivized through the collection of transaction fees, *i.e.* the fees that network users associate with their transactions to increase the likelihood that block producers will chose to include their transactions into a new block (thus, the amount of transaction fees typically depends on perceived value of each individual transaction and the overall congestion of the network).

As such, a variety of block producers compete to add new blocks to the chain, incentivized through a game-theoretical system designed to guarantee the security of the overall network. Yet, the system only works if there are enough block producers participating into the network, so that no single actor controls more than 50% of the total resources used to produce new blocks. Today, in many of the major blockchain networks like Bitcoin or Ethereum, the number of network operators—both block producers and validators—is in decline. This decline is not only an issue in terms of network governance, but also entails a diminution in network security. Most blockchain networks are currently governed by a few operators with large amounts of resources (e.g. mining pools) which, if they were to collude, would be able to modify the history of the blockchain, thereby enabling the practice of "double-spending" which the blockchain was precisely intended to prevent. Yet, despite this tangible possibility, the risk of collusion remains low because any attempt at performing a 51% attack would potentially jeopardize the overall blockchain network, raising concerns with regards to both the security and the long-term sustainability of the network, which would likely lead to a significant drop in the market value of the associated cryptocurrency. Actors interested in the maximization of their economic profits are thus incentivized to behave as stipulated by the network protocol, in order to maximize confidence in the network operations and its capitalization.

In recent years, new problems have emerged, as new and old network operators began to engage into a new mechanism of value extraction, currently referred to as "Maximal Extractable Value" or MEV. While a 51% attack is easily detectable by the other network operators, and is generally condemned, MEV is much harder to detect because it does not violate any of the protocol rules. Indeed, MEV merely consists of network operators (such as block producers or other network actors with access to the mempool of submitted transactions) profiting from someone else's effort at identifying a profitable transaction, by the capture of the value that would otherwise go to the other network users. The issue with MEV is that it is currently not possible to distinguish it from legitimate trading activity, as it often relies on the same market mechanisms. As such, it is hard to assess the economic impact of MEV, and even harder to design policies that would mitigate its negative effects. In recent years, new problems have emerged, as new and old network operators began to engage into a new mechanism of value extraction, currently referred to as "Maximal Extractable Value" or MEV. While a 51% attack is easily detectable by the other network operators, and is generally condemned, MEV is much harder to detect because it does not violate any of the protocol rules. Indeed, MEV merely consists of network operators (such as block producers or other network actors with access to the mempool of submitted transactions) profiting from someone else's effort at identifying a profitable transaction, by the capture of the value that would otherwise go to the other network users. The issue with MEV is that it is currently not possible to distinguish it from legitimate trading activity, as it often relies on the same market mechanisms. As such, it is hard to assess the economic impact of MEV, and even harder to design policies that would mitigate its negative effects.

One way to think about MEV is as a tax on network users, capturing the value of some transactions that would otherwise go to benefit these users. As such, MEV effectively represents a transfer of wealth from network users to MEV participants. This transfer of wealth is generally not perceived as such by the network users, as it happens 'behind the scenes', and is often not easily detectable. Hence, MEV represents a significant economic challenge, which can potentially lead to a concentration of wealth, and to a decline in the overall value of the network and therefore reduce adoption.

In this paper, we analyze the issue of MEV in light of traditional economic theories of utility maximization and free-riding. Building upon existing Commons theories, we propose to look at public blockchain networks as common-pool resources, which—despite efforts in game theory and mechanism design—remain subject to the tragedy of the Commons. We then look at how Commons theory could help us identify potential solutions to this ineluctable problem that is progressively affecting a larger number of blockchain networks.

2.2 Blockchains as Commons

2.2.1 Introduction to Commons-Pool Resources

Economists usually distinguish between 3 different types of resources management: *public management*, typically managed through a central actor controlling access and use of the resources; *private management,* generally associated with individual property rights and governed by market-based dynamics; and *Commons management,* governed by a collective. The type of management is different from the type of ownership as there might be a Commons management of a privately or privately owned group (and conversely). In the context of a blockchain network, because no one controls the network, and no single authority has the capacity to regulate the operations of the network or the behavior of network participants, public (centrally-governed) or private (market-based) approach are not well-suited to conceptualize how blockchains are governed. The theory of the Commons may therefore constitute a more suitable approach

Elinor Ostrom is regarded as one of the leading thinkers in this field. Through the analysis of hundreds of communities governing different types of Commons, E. Ostrom (1990, 2010) has developed conceptual tools to analyze Commons governance in a variety of contexts. Among these conceptual tools are Ostrom's 8 design principles (Table 2.1) that can be regarded as indicators of what may qualify as good and sustainable governance of a Commons.

To understand whether and how the design principles are met, E. Ostrom (2005) identified a set of key features to examine in governance systems. In particular, she insisted that the focus should not only be on operational rules used to manage the Commons resource on a day-to-day basis. While these operational rules may work in a normal state of affairs, they do not suffice to address exceptional situations or crises that might reveal shortcomings in these rules, and might thus require them to be modified or overseen. The procedures that define the process by which operational rules can be amended have

DP1 Clearly defined community boundaries 1a. Clear and locally understood boundaries between legitimate users and nonusers are present. 2b. Clear boundaries that separate a specific common-pool resource from a larger social-ecological system are present.	**DP5 Graduated sanctions** Sanctions for rule violations start very low but become tougher if a user repeatedly violates a rule.
DP2 Congruence between rules and local conditions 2a. Appropriation rules are congruent with local social and environmental conditions 2b. Appropriation rules are congruent with provision rules; the distribution of costs is proportional to the distribution of benefits	**DP6 Conflict resolution mechanisms** Rapid, low cost, local arenas exist for resolving conflicts among users or with officials.
DP3 Collective choice arrangements Most individuals affected by a resource regime are authorized to participate in making and modifying its rules.	**DP7 Local enforcement of rulesÂ** The rights of local users to make their own rules are recognized by the government
DP4 Monitoring 4a. Individuals who are accountable to or are the users monitor the appropriation and provision levels of the users 4b. Individuals who are accountable to or are the users monitor the condition of the resource.	**DP8 Multiple layers of nested enterprises** When a common-pool resource is closely connected to a larger social-ecological system, governance activities are organized in multiple nested layers.

Table 2.1: Ostrom's 8 Design Principles

Source: Cox et al. (2010) and E. Ostrom (2010)

been defined by Ostrom as "constitutional rules". Whether they are formally written or informally recognized, these rules are crucial because they have the ability to influence the whole operational level. In the context of blockchains, the *operational rules* may be assimilated to on-chain rules, e.g. the blockchain protocol or smart-contract code, while *constitutional rules* are harder to precisely identify because they mostly subsist off-chain.

Though originally developed to analyze the governance of physical Common-Pool Resources (CPR) the theory of the Commons (E. Ostrom, 1990, 2010) was extended to the governance of digital resources (Fuster Morell, 2014; Hess, 2008; Hess and E. Ostrom, 2007). While the challenges that digital resources face are distinct from the natural ones, both must find ways to deal with free-riders. E. Ostrom, Agrawal, et al. (1989) have demonstrated that CPR can face two broad categories of challenges: appropriation (allocation of the resource) and provision (contribution to the stock of the resource). While natural resources can pertain to either (or both at the same time), Knowledge Commons are almost exclusively facing provision problems. This paper shows that MEV is an exception to this rule.

Some authors have already analyzed blockchains from the perspective of the theory of the Commons. For example, Shackelford and Myers (2016) have shown that blockchains essentially respect Ostrom's 8 principles, although these conclusions are tempered by the work of Howell and Potgieter (2019a) who point out the risk of the concentration of power in the hands of certain actors. Rozas, Tenorio-Fornés, Díaz-Molina, et al. (2018) were among the firsts to apply the theoretical framework of the Commons to the blockchain world, showing that blockchains were suitable candidates for Commons governance. Poux et al. (2020) further explored the question, investigating how governance of and through blockchain technology may bring a paradigm change from traditional CPR governance because of the new opportunities in terms of ex-ante enforcement and ex-post verifiability that the blockchain provides.

The next section presents a specific type of Commons and demonstrates how it applies to blockchains

2.2.2 Blockchains as Commons-Based Peer-Production

The concept of commons-Based Peer-Production (CBPP) is often credited to Harvard Professor Yochai Benkler, who has written extensively on the subject. In his book *The Wealth of Networks*, Benkler (2006) argues that the rise of the Internet and other digital technologies have enabled a new form of social production, which he calls "commons-based peer-production". Benkler defined CBPP as a new economic model in which the production of information and knowledge is based on decentralized collective action and exchange, rather than on the labor of a few individuals. The term was first coined in the context of the open-source software movement, but has since been applied to other fields such as open content, open science, and open hardware (Papadimitropoulos, 2018).

More generally, CBPP can be described as a new form of economic activity that is based on the collaborative efforts of a distributed network of individuals. The key characteristic of commons-based peer-production is that it is not based on the logics of the market or the state, but on the voluntary cooperation of a large number of individuals that operate according to a separate set of logics, which are Commons-based. The success of this model has been attributed to the fact that it allows for the production of high-quality goods and services without the need for centralized control or coordination.

CBPP is a phenomenon which has been studied by a variety of scholars, such as Bauwens and Pantazis (2018), Benkler and Nissenbaum (2006), Morell, J. L. Salcedo, et al. (2016), and Siefkes (2013) and many others. While there is no established or commonly-agreed definition of what does or does not constitute CBPP, it is generally understood that it operates according to four separate components or criteria (Morell, J. Salcedo, et al., 2015)—two of which refer to the outcome of production and two of which refer to the process by which production is achieved. Regarding the outcome, CBPP always generates a shared resource that is held in common by a group of individuals or by the public at large. Such a resource is usually characterized by a certain degree of *reproducibility* or *derivability*. As far as the process is concerned, commons-based peer-production always involves distributed participation, or what is commonly known as peer-to-peer collaboration, in the sense that it generally employs collaborative means of production. These collaborative methods also tend to rely on decentralized governance structures, rather centralized or hierarchical structures.

The operations of most blockchain networks can be considered as a new form of CBPP, both with regard to the process and output of production. For the former, these networks rely on the collaboration of large numbers of individuals, responsible for the development of software code (i.e. the blockchain protocol) and for the maintenance of the network (i.e. miners and validators). For the latter, the networks allow for the production of a public good, the blockchain ledger, which is the central component of the technology. This characterization of blockchain networks as common-based resources is further supported by the fact that most of the major blockchain networks, such as Bitcoin and Ethereum, are open-source, decentralized, and permissionless—i.e. open for anyone to participate.

However, there are some important ways in which blockchain networks differ from traditional CBPP. First, blockchain networks are often designed to be trustless, meaning that they do not rely on any central authority or trusted third party. Blockchain networks are intended to have a decentralized governance structure, so that no central authority can influence the operations of the network. This is in contrast to traditional CBPP, which often relies on a central authority, such as a foundation or company, to manage the community and the resources.

Second, blockchain networks generally have a native token that is used to power the network. A blockchain's native token gives users an ownership stake in the network and provides a way to align the interests of users with the interests of the network. These native tokens are intended to reduce the opportunities for free-riding, with regard to both over-consumption and under-provision. First, they allow for the establishment of economic incentives to encourage participation in the network. Indeed, most blockchain networks have a built-in mechanism for distributing rewards to those who contribute to the network. For example, Bitcoin rewards miners with newly minted bitcoins for validating transactions on the network. Because miners have a vested interest in the network and are rewarded with bitcoin for their efforts, they have an incentive to contribute to the proper operations of the network, and to help ensure that the network remains secure. These economic incentives are in contrast to traditional commons-based peer-production, which often relies on voluntary labor. Second, a blockchain's native token is often used to pay for the resources required to use the network. That is, individuals who want to enjoy the services of a blockchain network generally have to pay a contribution to those who are maintaining the network. For example, in order to use the Bitcoin network, users must spend bitcoin to pay for the transaction fees, which will be distributed to the miners responsible for operating the network, in proportion to their contribution. This allows for the blockchain network to be self-sustaining, as the native token can be used to pay for the costs of running the blockchain network and guaranteeing a sufficient level of security. This stands in contrast with traditional Commons resources, which generally depend on the voluntary contributions of community members.

Yet, despite these powerful incentive mechanisms, the problem of free-riding is not completely eliminated in most blockchain networks. As we will see in the following section, a blockchain's native token introduces many new opportunities for free-riding, which were not properly accounted for by the designers of these systems.

2.3 MEV and the Tragedy of the Commons

2.3.1 Typology of MEV

The problem of Miner Extractable Value was originally identified by pmcgoohan (2014) who noted that, because they are in charge of curating the transactions to be included within a block, miners have the possibility to frontrun the most profitable transactions submitted to the public mempool[1]. More precisely, while miners generally pick the transactions to be included within a block according to the transaction fees, they can also manipulate the order of transactions, by injecting their own transactions into the block in order to extract profits. This particular type of MEV has been initially defined as "value which can be extracted by a miner from manipulating the order of transactions within the blocks the respective miner creates" (Judmayer et al., 2021, p.1). However, because the process also concerns other actors than miners, the term was generalized to Maximal Extractable Value, to keep the same acronym.

Before describing the actors who engage in MEV, let us first characterize the different forms of existing MEV, which we will categorize according to the impact that it has on the network, and on the network participants. We analyze such an impact according to two dimensions. The first one assesses whether MEV contributes to furthering the objectives of the system as it was originally intended to operate, e.g. by either increasing or decreasing the efficiency of the blockchain network. This dimension can be analyzed in a relatively objective manner, and only concerns costs and congestion of the network. The second dimension is concerned with the perceived legitimacy of these MEV practices, i.e. whether the network participants consider them as "fair". This question is inherently subjective, as it relies on participants' subjective considerations, which might relate to a specific definition of fairness that may not be universally agreed upon.

For the purpose of this paper, we propose a particular approach to "fairness" based on the legitimacy of value appropriation: MEV is considered "fair" when the value that is extracted from the network is a result of one's actual effort to identify the opportunity for value extraction, as opposed to extracting it from the effort of others. In other words, "fair" MEV does not prevent users to reap the benefits of their efforts. This approach is informed

[1]In a blockchain, the public mempool is the pool of possible transactions submitted to the network, before they have included into a block. Miners generally pick the transactions to include within a block according to the transaction fees. Yet, they can also introduce their own transactions into the block they produce in a given order, in order to frontrun/backrun specific transactions.

by Ostrom's second design principle. Cox et al. (2010, p.38) write that "some scholars have pointed to the importance of users perceiving the match between appropriation and provision rules as fair, relating this condition to a principle of equity found in the literature". This means that in a Commons, fairness is related to whether the efforts are rewarded which means that appropriation depriving users of their payoff is considered "unfair". While limited in scope, we find this approach particularly relevant to analyze MEV and we thus propose it to the community for consideration.

We can now go on categorizing MEV according to these dimensions:

Positive impact MEV:

We here identify the MEV practices that increase the efficiency of the network and that are aligned with the original design of the system. We differentiate between those that rely on explicit and hard-coded rewards following specific actions, and those that do not.

Hard Coded Rewards: They are frequent to incentivize certain behaviors in blockchains. The most obvious example being miners getting cryptocurrencies when they mine a block. Similar processes exist on the Application Layer and lead to MEV because it generates revenue at the block level. One example would include Cryptokitties. While the life of cryptokitties relies on market mechanisms, they rely on a creation ex-nihilo. To incentivize users to create them, a reward is handed out to what Zargham has dubbed "Crypto Midwives" (Koch, 2018). Concerning MEV, the most frequent type of such hard coding rewards are liquidation calls:

The most frequent of type of hard-coded MEV are liquidation calls. Lending systems such as Aave or DyDx require borrowers to deposit collateral to cover their operations. When the collateral value falls below a threshold, anyone is allowed to liquidate the position by buying the collateral at a fixed price, usually lower than the market price, so as to pay back the lender. In doing so, the liquidator (who sends the liquidation order) makes some profit, while ensuring that the position does not get uncollateralized. (Qin, Zhou, Gamito, et al., 2021). In this form of MEV, there is a hard-coded reward for the liquidator who has a guaranteed profit when she sends the order.

Market-based rewards: This form of MEV is instrumental to the proper operations of a market; people are rewarded when they intervene in order to guarantee the efficient operations of a particular market system. The most common type of MEV in this category are arbitrage.

Decentralized Exchanges (DEXes) each have different strategies to set the exchange rate between two tokens. Therefore, it may sometimes happen that a significant discrepancy occurs between the exchange rates of the same tokens on two different DEXes. Arbitrageurs can make profit out of this situation by buying low on one platform and selling high on the other one, thereby contributing to re-harmonizing the exchange rates. In this case profit does not result from execution of the transaction itself but from the state of the network at a given moment. While the market may deliberately rely on these incentives, they are structurally different from the previous ones because they are more context-dependent.

These two sorts of MEV stem from, and support the operations of DeFi. They are part of the design of the system and are aligned with its objectives (for instance, providing an efficient decentralized market or creating cryptokitties). Indeed, arbitrage opportunities arise because there are no centralized mechanisms to harmonize the exchange rates across platforms. Arbitrage contributes to the health of the system by incentivizing users to look for profit opportunities to reestablish equilibrium between the exchange rates of platforms. Similarly, in the case of lending protocols, liquidators are doing the useful work of detecting uncollateralized positions and liquidating the collateral to help lenders recover their loan, and are thus rewarded for this work.

Negative Impact MEV:

We here survey the types of MEV that have adverse consequences on the network and its participants. In particular, they derive from asymmetry of power and information that allows certain actors to appropriate value from orders emitted by others. Our categorisation demonstrates that not only are these practices "unfair" but they also reduce the efficiency of the network.

Frontrunning: This form of MEV relies on the possibility for certain actors to push certain transactions before the others. While miners can freely reorder transactions because they are in charge of creating blocks, users who identify MEV opportunities (so-called *searchers*) must compete with other network users, to ensure that their transactions will have priority in the queue. Price Gas Auction (PGA) relies on the fact that block producers will place transactions with the highest gas price first in their blocks. Therefore, when a searcher detects a MEV opportunity it can submit the same transaction with slightly a higher gas price in order to frontrun it. When done repeatedly, this is likely to result in bidding wars, with increasing gas prices that ultimately harm all network's participants. Frontrunning allows block proposers to "steal" profitable transactions, by replicating them (albeit assigning them to their own account) to include such modified transactions earlier on into the block. In particular, arbitrage or liquidation orders are common targets for frontrunning

Sandwich Attacks: These forms of MEV are an evolution of the previous one and concern strategies that not only make profit of the current state of the blockchain but intentionally modify the state, in order to extract value from pending transactions. In a sandwich attack (SA), a transaction (classically an order on a DEX) is wrapped between two additional transactions designed to extract value from the original transaction, at the expense of the original proposer and for the benefit of the attacker (see Figure 2.1). SA use the fact that DEXes orders include slippage to account for the possibility of a change in the market between the time the order was sent and the time it was added to the chain. SA modify the market so that the conditions are within the slippage range of order but are adverse enough for the searcher to make profit (and reduce the profit of the original sender). One negative aspect of SA on the network, on top of contributing to PGA, is that that increase the number of transactions and use more block space, thus reducing the chain efficiency.

Agressive MEV: This type of MEV aims at making a transaction in order to force a profit opportunity at the expense of another user. This is made possible by the asymmetry of power that allows miners and searchers to manipulate the order of transactions. While not exclusively, this type of MEV mostly relies on front or backrunning. They are facilitated by flashloans. Flash loans rely on the blockchain-specific possibility to revert a transaction if the money is not paid back at the end of an atomic transaction. Through the recourse to a smart-contract, loan-emission, operation for which the money is borrowed and loan-reimbursement can be bundled in a single transaction. If at the end of this transaction, the borrower cannot pay the loan back, none of it is executed. This ensures that the lender will be paid back and the borrower does not need to have collateral (Qin, Zhou, Livshits, et al., 2021). Examples include:

Market manipulation: this type of MEV come from the possibility temporarily modify exchange rates by issuing a large-scale and benefitting from the resulting skewed market by shorting (longing) a position. These attacks result in net loss for other of the blockchain (either original issuers or DEXes when they are targeted). These attacks are facilitated by flash loans that grant instant access to the large amount of money necessary for skewing market.

Forced-liquidation: Sometimes, a transaction is not profitable such, but the resulting change in the state of the blockchain result in an MEV opportunity (typically a liquidation). The proposer can thus backrun the transaction, by including an order right after such transaction, for guaranteed profit. Frontrunning generally results in missed profit opportunities for original transaction issuers, while backrunning usually results in losses. Forced-liquidations can also be designed to explicitly manipulate the transactions in a block. Suppose Alice notices that position she holds might become undercollateralized and sends an order to top-up her position and avoid the liquidation. Someone detects this transaction and frontruns it with a set of transactions that will modify the market, make the position undercollateralized and liquidate it before Alice had a chance to prevent this from happening. Flashloans also facilitate this type of transactions by making market-manipulation in atomic transactions virtually free.

Time-bandit attacks: When a block contains enough MEV opportunities, it is in a miner's

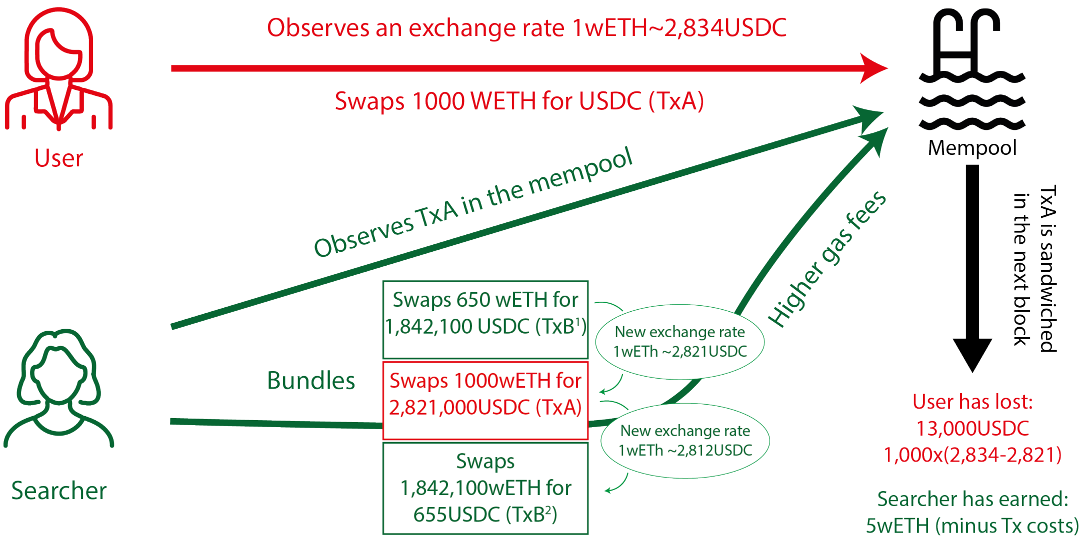

Figure 2.1: Figure 1 Example of A Sandwich Attack

Source: Adapted from Eigenphi-1

rational interest to try and frontrun the block (i.e. trying to mine a new block, incorporating these MEV opportunities at the same height as the previous blockchain) rather than to mine a new block at the end of the chain. This type of MEV is extremely problematic because a successful attempt at doing so would lead to rewriting the history of the blockchain. What is more, it could threaten the operations of the whole blockchain network, because every miner would be economically incentivized to re-mine the most profitable transactions in previous blocks, rather than to extend the chain and include new transactions. Combined with the risk of selfish mining (Eyal, 2015) these time-bandits attacks jeopardize the security and sustainability of the blockchain. This type of attacks is fundamentally different from the three previous ones as they are not done solely through a reordering of transactions but through an actual rewriting of the blockchain history. While they are inherently more harmful than the others MEV practices, they are also much more costly to carry on, as they require a large share of mining power (similar to that required for a 51% attack). Therefore, the remainder of our discussion will not be concerned with time-bandit attacks.

We see that these two types of MEV are very different in nature and in their outcome. On the one hand, the positive ones are necessary for the DeFi market equilibrium to be sustained, as they allow efficient price detection in a decentralized context. On the other hand, negative ones are detrimental to the network, as they result in increased gas fees and take on more block space.

What is more, they allow a set of network participants (block producers or searchers) to monopolize the value that can be derived from the network. Notably, Piet et al. (2022) estimated that miners earn the largest share of MEV thanks to their power and information asymmetry. This makes these practices "unfair" in the sense that we have proposed above.

2.3.2 The problem of Free-Riding in Blockchain Networks

Economists frequently differentiate types of resources based on two metrics: excludability and non-rivalry. A good is excludable if access to it can be restricted to individuals, while a good is rival if it can only be used by one person at a time, preventing others from using it as well. The free-rider problem concerns mainly non-excludable goods, be them public goods or common resources. Since people cannot be excluded from them, the assumption is that, acting in a selfish manner, individuals might be tempted to consume more than they are entitled to and/or contribute less than they ought to. These individuals rely on the others to do the "dirty" work of maintaining and provisioning the resource, without assuming the responsibility themselves. Yet, if most of them behave the same way, they end up destroying the shared resource by over-usage (in the case of rival-goods) or under-provision (in the case of non-rival goods). This dilemma is usually referred to as the "Tragedy of the Commons" (Hardin, 1968).

Despite the introduction of cryptocurrency-based incentive systems, blockchain, as many other common resources, suffers from similar problems. As explained above, blockchains networks have introduced different types of solutions based on cryptocurrency and token economics to solve the free-rider problem. However, the risk of opportunistic behaviors is not totally eliminated from these networks because—paradoxically—these very incentive mechanisms create new avenues for free-riding, which is no longer grounded on over-consumption or under-provision, but rather on an unfair appropriation of value. It does, however, produce negative effects when it comes to resource distribution amongst the operators to the blockchain network. Such an opportunistic behavior consists in "free-riding" on the work of others, precisely by appropriating the value generated by other people's transactions. In other words, it does not break the rules of the network, but it definitely harms the interests of other network users.[2] The issue we identify here results from an "unfair" appropriation of the value in the sense that those who free-ride benefit from the surplus generated by the work of others, who are no longer compensated for having discovered these added-value transactions. Even if this appropriation is not necessarily qualified legally as a theft, it is understandable that the qualification of the act can be interpreted in these terms with important effects on the functioning of the network.

[2]This type of opportunistic behavior can be compared another problem recognized by economic theory, that of parasitism, a well known form of free-riding that consists in placing in the wake of others, relying on the efforts and initiatives of an economic operator, whether a competitor or not, to gain benefits. The parasite is generally a "follower" in terms behavior and adopts the same strategy as those that have had success in an initiative in order to benefit from them without incuring any cost (or at a lower cost).

This approach is also consistent with the work of Olson (1965) on free-riders who showed that, in large groups, a small, well-organized minority could impose a cost on the larger community in what he called a "tyranny of the minority". We contend that MEV is an example of such practice of a new type.

We know that blockchain technology, in particular, has emerged as a potential solution to the erosion of trust in traditional institutions and more generally in online intermediaries, as it allegedly eliminates the need for trust between parties. The underlying principle of blockchain technology and its various applications is that users prefer a technological system that they are confident is immutable, to centralized institutions considered as unreliable. Blockchain aims to mitigate principal-agent problems such as moral hazard or adverse selection that characterize most trust relationships. This has led many scholars to describe blockchain as a "trustless technology" (Werbach, 2018). However, as noted by De Filippi, Mannan, et al. (2020), this approach views this property of blockchain technology only in a negative light (blockchain technology does not need trust to function). The authors suggest a positive perspective considering what blockchain technology produces in order to operate, that is to recognize that "blockchain technology reconfigures trust in society, by contending that the technology does not qualify as a 'trust machine' but rather as a 'confidence machine'" (p.2). This distinction is crucial for our purpose because it allows us to understand that the question is less about the distinctive properties of trust, characterized by a risk and uncertainty (following Luhmann (2000)), than the feeling of confidence which does not seemingly present these characteristics:

> the state of confidence implicitly exists whenever a person engages with another without the need for reflection about the existence of risk or uncertainty, thereby eliminating the need of choosing among alternatives. In that sense, confidence—unlike trust—emerges when an individual believes that the person or system she interacts with does not have the agency to betray her expectations (De Filippi, Mannan, et al., 2020, p.4).

As such, confidence derives from predictability of future events and it is definitely different from the kind of *leap of faith* that is inherent to trust.

Blockchain-based networks generate confidence in the economic incentives and game theoretical schemes that govern the network, grounded on the premise that miners will always act in such a way as to maximize their financial rewards. Combined with the mathematical properties of hash functions and public-private key cryptography this yields high predictability for the users and operators. The perceived automation and impartiality inherent in the protocol of a blockchain-based network becomes a source of confidence. Because the technological infrastructure is not managed (nor controlled) by any social or political institution, blockchain-based systems are often regarded as a superior alternative to many of our current human-led, and therefore corruptible institutions.

If we apply this approach of blockchain as a "confidence machine", the main issue consists in asking to what extent the fact that there can be some unfair appropriation will have a negative impact on the expectations of the network operators because it becomes difficult to be confident in the fact that there will be no *theft* of the created value. In other words, the confidence machine will partially break down and the volume of the activity network may be negatively impacted. From the users' side, we can distinguish between two sorts of expectations. The first concerns how the blockchains work, in particular in terms of immutability, security and tamper-resistance. The second concerns what services blockchains may offer and related to having the confidence that one's transactions will be added to the blockchains. In the MEV context, the immutability confidence is not affected whereas the second one breaks, which brings up a new "tragedy" of the blockchain Commons.

We can see that this approach, based on the distinction between trust and confidence, finds an echo in game theory. Indeed, it appears that blockchain is essentially based on the theory of non-cooperative games (which bases the very nature of the social contract between operators on blockchain). However, we observe that in order to solve the mechanism design problem, it may be useful to adopt the logic of cooperative games. A central aspect that emerged is that for collective and individual interest to align, coordination is sometimes sufficient, but sometimes genuine cooperation is necessary. This particularly refers to the well-known Hardin's problem of the "Tragedy of the Commons" as it is conventionally understood in game-theoretic terms.

Ostrom's work has highlighted that Hardin's conclusion was overly simplistic notably because there are many empirical examples of successful community management that invalidates it. There is also ample evidence from lab-experiments that people are not only rational, narrowly self-interested maximizers. In addition, in many experiments, where self-interest would dictate zero contributions to a public good, many people actually do contribute significant amounts. To quote E. Ostrom (2000) "In all known self-organized governance regimes that have survived for multiple generations, participants invest resources in monitoring and sanctioning the actions of each other so as to reduce the probability of free-riding" (p.138).

This suggests addressing the MEV issue from a Commons perspective.

2.4 Towards a Commons-Based Solution

2.4.1 Existing Solutions

Over the last years, different solutions have been proposed to address the issue of MEV, mostly on Ethereum. We here briefly review the main ones and propose a new direction for the future, before analyzing them through the lens of the theory of the Commons.

Most solutions rely on avoiding the publication of transactions on the public mempool (although not exclusively), in order to lower the negative effects of MEV. This usually implies adding an additional layer between the users emitting a transaction and the inclusion of such transaction in a block. Private relays (such as the Taichi Network) can be used to send the transaction directly to a miner, trusted not to do unfair MEV. Request For Quotes (RFQ) are swap orders that include some metadata (such as the address of the transaction and pre-agreed on price) as a way of securing an order on a DEX to prevent slippage and thus reduce the risk of frontrunning or of SA.

Fair sequencing services, and in particular Chainlink, propose to separate block creation and block validation. Block creation would be made in a 'fair' way to prevent 'unfair' MEV. Chainlink is the most popular one and has a 2-step approach (Breidenbach et al., 2021). In phase 1, it relies on a decentralized network[3] to order transactions before sending the bundles of transactions to miners. In phase 2, a fair sequencing protocol, Aequitas, based on the First-In First-Out principle, prevents transaction ordering.

Currently, the most popular solution to MEV is provided by Flashbots, a company dedicated to furthering research and development on the issue of MEV. As the founders, in particular Phil Daian, were among the first to raise awareness on the issue (Philip Daian et al., 2020), they remain an influential reference to this date in the discussion on MEV. Flashbots main service is MEV-gETH, a software that allows network users or searchers to propose bundles of transactions to block producers with a share of the value going to the miner and the rest to themselves. Bundles are a way of proposing a set of transactions as a whole rather than individually. Execution then becomes "all or nothing", preventing MEV based on transaction ordering.

Miners then select bundles according to gas efficiency rather than gas price, thus decreasing gas price on the network. Moreover, the process is transparent and anyone can join and become a searcher. To help miners sort bundles depending on who proposed them, the auction system is also based on a reputation system. Flashbots is a very specific private relay that, on top of establishing a private communication channel between network users and block producers, also offers bundling and ranking services. On top of proposing this software, Flashbots also collects and publishes data that serves as a reference to estimate the amount of MEV happening over time on Ethereum providing the community with valuable information.

These solutions have been designed for different purposes. On the one hand, the intended goal of Flashbots is to democratize MEV but not to prevent any of it. It does not preclude users from engaging in the front or back-running of transactions, or sandwich attacks; it just requires them to do it in a more transparent and open way. On the other hand, Chainlink aims at eliminating all sorts of transaction ordering and separating block proposition and block validation. This prevents all order manipulation opportunities, including those that may increase efficiency (such as including arbitrage at the top of a

[3]How the this decentralization and decision-making process work is not entirely clear however.

block). One issue might be that the order is based on the time it was received by the nodes and not emitted. The reason for this is that a send-order-fairness "would require a trusted or verifiable client-side timestamp" (Kelkar et al. (2020)) which implies a trusted third-party. However, researchers have raised awareness on the fact that malicious agents might manipulate the network to defer the arrival of certain transactions thus enabling another type of manipulation (Tang et al., 2022). This remains hypothetical, in particular as long as Aequitas is not generalized but these issues must be debated in terms of risks and opportunities by the whole community.

While we have noted that blockchains are CBPP, it is interesting to remark that none of these solutions rely on the community to address the MEV issue. Flashbot adopts a market-based approach that solves the efficiency issues but does not address the those of fairness. Chainlink adopts a radical position by preventing all transaction ordering, fair or not. We suggest that there may be another way, community based, benefitting from the learnings of the Commons, in particular based on cooperative game theory.

2.4.2 MEV and the 8 Design Principles

To understand what a Commons based solution may bring, let us first discuss how the 8 design principles are affected by MEV and in particular the negative one.

Applying Ostrom's 8 design principles reveals that some MEV practices undermine collective governance of the blockchain as a Commons. As shown in Table 2.2, the four first design principles are challenged by these practices. With regard to DP1, the so-called *searchers* who are exploring the mempool to identify profitable transactions are a new position that modifies the standard definition of community boundaries. E. Ostrom, Gardner, et al. (1994) showed how the sustainable governance of the Commons requires a clear identification of the various roles adopted by the community members, as well as a proper understanding of what these roles entail (in terms of rights and obligations) and who can hold them. Currently, the role of searchers and the legitimacy of their activities is not collectively agreed upon, as evidenced by the fact that some consider their behavior unfair. DP2 is particularly challenged as it requires proportionality between the costs and benefits associated with the various rules and local conditions. Users victim of "unfair" MEV have spent efforts and costs to identify profit opportunities, but do not obtain the expected benefits from these. As we have mentioned above, the approach of fairness we have proposed is an indicator of this design principle as we suggest that no situation where MEV renders efforts rewardless should be considered as fair. The issue of collective choice arrangement (DP3) will be tackled more specifically in the following sections, which proposes a more participative approach to solving MEV. While monitoring (DP4) is usually straightforward due to the transparency of a blockchain, it remains extremely hard to detect MEV transactions, despite increasingly numerous community efforts (Flashbots Data, Research Papers...), notably because they do not differ from standard or fair

DP1 Clearly defined community boundaries While the resource is well defined (the blockchain), the different roles, in particular the issue of searchers, are not collectively agreed upon	**DP5 Graduated sanctions** Requires a change a paradigm
DP2 Congruence between rules and local conditions We see that the appropriation rule is not proportional to the costs and that the current status quo does not satisfice users	**DP6 Conflict resolution mechanisms** NA
DP3 Collective choice arrangements For now, most users do not have their saying in MEV	**DP7 Local enforcement of rulesÂ** Guaranteed by automation and distribution
DP4 Monitoring Monitoring of MEV is difficult as the transactions just appear as normal ones	**DP8 Multiple layers of nested enterprises** When a common-pool resource is closely connected to a larger social-ecological system, governance activities are organized in multiple nested layers.

Table 2.2: How MEV affects the 8 Design Principles

Source: Cox et al. (2010) and E. Ostrom (2010)

MEV transactions. Sanctioning (DP5) cannot be easily achieved on-chain because the design of the blockchain itself makes it difficult; yet social sanctioning (such as reputation mechanisms) might prove efficient as long as it is not precluded by the pseudonymous nature of the blockchain. Finally, conflict resolution mechanisms (DP6), local enforcement of rules (DP7), and multiple layers of nested enterprises (DP8) are unaffected by the MEV practices.

Our analysis so far identifies which of the design principles are jeopardized by the practice of MEV. The approach of fairness we have proposed also manifests that as long as "unfair" MEV takes place, the second design principle may not be met. While this is not unsurmountable (the design principles are by no means mandatory), it indicates potential threats to the governance stability. We suggest that, to find solutions that may address these issues, it is worth investigating requires achieving a participative collective-choice arrangements.

2.4.3 The Way Forward

When considering existing proposed solutions, we see that they focus on the operational rules and propose technical solution. For instance, while both Flashbots and Chainlink may technically solve some problems associated with MEV and in particular revitalize the design principles DP1 and DP4, meeting the DP2 and DP3 require community involvement and adoption, on top of technical implementation. What is more, as this short review evidences, both these solutions may create new forms of profit opportunities for some actors (either by generalizing MEV for Flashbots, or for people with the infrastructural capacity to send their transactions before the others), so a trade-off may still be necessary. Knowledge of the governance of the Commons informs us that adoption and collective decision-making must be done in congruence with the constitutional rules. In this case, it means meeting the expectations of the community of users as to what the blockchain should provide and facilitating an informed debate.

While both Chainlink and Flashbots explicitly identify their premises, they are not completely matching and differ on some key aspects such as the notion of "fairness" (see Phil Daian's blogpost on the matter, 2021). In other words, they justify their solutions by different sources of legitimacy. J. Black (2008) typology of legitimacies helps use situate their approach: Flashbot proposes to transform a cognitive (unavoidability) take into a pragmatic one (align the interests of the different users) while Chainlink builds on a moral argument.

The purpose of this paper is to suggest that a solution based on cooperative game theory inspired by the theory of the Commons. Because blockchains have an active community willing to collaborate to reduce harmful effects on the network (be it in terms of efficiency or in terms of "fairness"), learnings from CBPP and other CPRs indicate that cooperation may provide an efficient solution at a relatively low cost.

The blockchain community already has a recent example of such a recent process: time-bandit attacks have been unanimously condemned as endangering the stability of the network as a whole. Therefore, despite not having a technical solution to prevent it, the community as a whole (including powerful mining pools who have the capacity of engaging in such behavior) committed not to do it, to preserve the sustainability of the blockchain.[4] Although it is unsure whether similar engagement may emerge for other sorts of MEV.

Commons approaches usually rely on trust which may seem incompatible with the blockchain rationale. However, existing solutions such as private relays and even Flashbots (through their reputation mechanism) have reintroduced trust to patch the broken confidence that transactions will be included. We take this as an indicator that trust-based solutions are a promising direction to explore.

In that perspective, we have proposed a contribution to define what we consider fair and what solutions to MEV should address. It does not seem to meet neither the definition of fairness by Flashbots nor by Chainlink but we hope it sparks a constructive debate and situate this problem in the larger scope of CBPP governance. While particularly decentralized, blockchains may build on their community to devise coordinated solutions in the polycentric system without relying only on market mechanisms or technical solutions.

While, by definition, this approach should be bottom-up and we cannot indicate what direction it should take, we can recommend looking at the ostromian literature to adopt

[4]To this day, no time bandit attack has ever been detected. Although it is hard to monitor them, this likely indicates that the commitment is generally respected.

best practices. Because transacting on a blockchain is a repetitive game, and that it is in everyone's interest not to lead to generalized unfair appropriation of value to preserve the value of the chain, cooperative game-theory and collaboration may prove promising.

2.5 Conclusion

Blockchains such as Ethereum were designed to allow their users to rely on the quality of their incentive and security mechanisms by ensuring a safe, immutable and transparent network that requires no trusted actors. To this end, they rely on non-cooperative games that encourage actors to maintain the network in exchange for rewards. This system, by integrating in its design the risks of free-riders, has made it possible to eliminate them through the development of unbreakable protocols.

Yet, this very strong codification of blockchains has also allowed the emergence of other types of practices, respecting the terms of these protocols, but akin to free-riding. In particular, the Maximal Extractable Value (MEV) has recently received significant attention. Although many solutions are being developed and deployed, research around MEV remains relatively scarce due to the novelty of the topic and often focuses on its technical aspects. We propose an approach focused on the theory of the Commons to understand whether it could lead to a new form of solutions.

First, we propose a typology of MEV practices that distinguishes between their consequences on the network (objective) and those on the users (subjective). In order to characterize the latter, we proposed an approach in terms of equity based on the fair reward of efforts. This allows us to explicitly define the unfair practices of MEV. This definition then leads us to develop our two main contributions to this field of research.

The first was to demonstrate that MEV is a new form of free-riding. This form, specific to blockchains, was made possible by the fact that blockchains do not rely on trust, replacing it with confidence in the functioning of the network. This new type of free-riding, although distinct from those classically threatening resource governance managers, also compromises the stability of the network and constitutes a real liability for its future.

Our second contribution was to link this issue to the theory of the Commons. This field of research analyzes and explains how communities collectively governing a resource manage to limit opportunistic behaviors, notably through cooperation and the establishment of social values such as trust or reputation. Based on this theory, we identified the main lessons it could bring to the current situation regarding MEV.

In particular, the co-development of a community solution, reintroducing a form of trust, could be promising. This approach is all the more meaningful that blockchains are themselves Commons. We contend that the solutions currently proposed reintroduce a form of trust without explicitly stating it, which could lead to asymmetries of power.

In order to carry out our analysis, we have also evaluated MEV with regard to Ostrom's 8 Design Principles of good governance of a community. This allowed us to highlight that the governance of blockchains as a decentralized Commons was undermined by these practices and that none of the solutions available today could, in their current state, resolve these issues.

We therefore propose a solution expressly based on cooperation and social (and no longer economic) mechanism as we have shown that there are many reasons to explore this avenue. The main difficulty lies in the fact that we cannot make recommendations regarding the form that such a solution should take since it must come from the community and meet its expectations of the blockchain in order to restore the confidence of users in the network. We hope that this paper contributes to fueling the debate.

The Calculus of Liquid Democracy

After this initial work on MEV, the remainder of the manuscript focuses on governance *by* the blockchains. The paper presented in this chapter draws on the *Calculus of Consent* to study Liquid Democracy as a collective choice tool depending on the context. Of the four papers written during my dissertation, it is the one the has the most distant relationship with blockchain communities because it addresses theoretical considerations of a collective choice mechanism independently of the technology that implements it. However, as developed in the article, Liquid Democracy is intrinsically connected to blockchains because the renewed interest in Liquid Democracy as a voting tool can be linked to the boom of DAOs and blockchain-based e-voting. I that sense, a blockchain implementation of Liquid Democracy could be a building block for blockchain-enabled governance as discussed in the other papers.

The paper is presented is the form will be submitted to the Journal of Institutional Economics. The literature review at the beginning of the paper overlaps the one in chapter 1 but specifically extends on the question of voting methods and on the literature on Liquid Democracy.

Abstract

Following an increasingly large corpus of literature championing blockchain-based voting systems and, in particular, Liquid Democracy, this paper proposes a theoretical analysis based on political economy on the issue completing the current literature which focuses more on technical issues. Differentiating between Liquid Democracy as a voting tool and as a new form of democracy, I argue that the former offers the opportunity to vote for more inclusive decisions and to better reflect voters's intensity of preferences delegation and logrolling. However, the latter does not benefit from these positive outcomes as it faces major limitations at large scales because it fails to provide a framework for bundling and for legislative work. I conclude that, for now, Liquid Democracy is more suited to local democracy or small-scale homogeneous groups than to larger-scale systems (such as national constitutions). Along the paper, I discuss blockchain-based examples of Liquid Democracy to illustrate the analysis and link it with recent literature.

Representation and Intensity of Preferences

A Political Economy Analysis of Liquid Democracy

P. Poux

3.1 Introduction

Democracy relies on the people expressing preferences over policies. To do so, citizens (or at least those allowed to do so) have the right (and sometimes the obligation) to vote regularly for local, regional or national elections either directly or, more frequently in Western democracies, for candidates who become their representatives. However, the way the voting system is designed can influence how these preferences are accounted for through two mechanisms that might be entrenched. The first one is the long-known Condorcet Paradox (Condorcet, 1785), later on refined by D. Black (1958), and by the Arrow Impossibility Theorem (Arrow, 1951) that states that it is impossible to design a voting system that is "fair" (in the sense that it meets five basic principles).

The second, beyond how votes are counted, is that the way votes are casted may also influence the outcome of an election. This has been illustrated in the recent US elections (Salame, 2020, see for instance) and has triggered research on voter suppression (Hajnal et al., 2017) or on the recurring issue of gerrymandering. Many factors may influence the voting capacity of citizens; adopting the language of the 'pathetic dot theory' (Lessig, 2006), these factors can pertain to the domain of the law (who can vote), the architecture (where polling stations are located) or the norms (whether voting is perceived as being important by members of your community). It derives when a voting system chooses an aggregating and a decision-making function, it has consequences that will influence turnout and the country's political dynamic. Such voting systems must make trade-offs in terms of costs and efficiency that may not be considered optimal by all.

Consequently, there have been numerous works studying or advocating voting systems reform. In particular, with the emergence of digital technology, remote voting through digital systems (or e-voting) became possible and was experimented in various settings (Gibson et al., 2016). The reasons to do so included cutting down the costs of elections, generalizing access to votes (reduce voter suppression) as well as technology enthusiasm. E-voting comes with considerable challenges and risks—as illustrated by most famous controversy over the 2000 US Presidential Elections in Florida (Lobo, 2004)—and there has been continuing research to overcome these challenges (Gibson et al., 2016).

Since the emergence of blockchains in 2009, there have been many calls for Blockchain-based E-Voting (hereafter called BEV). Blockchains are a way of ensuring distributed, reliable and immutable data storage between nodes. An increasingly large number of people believe they represent a major opportunity for e-government (Batubara et al., 2018) and in particular e-voting. On Scopus, the abstract and citation database, the number of papers including the words "blockchain" and "voting" increased from 1 in 2015 to 190 in 2020 (Scopus, 2020). Despite numerous unanswered questions and challenges concerning the adoption of such a technology (Taş and Tanrıöver, 2020), many publications promote blockchain-based e-voting systems. Some even go beyond a purely technical proposition and argue that BEV could enable a radical shift in democracies towards more direct forms of representation. In particular, there has been a resurgence of interest in Liquid Democracy (first described by Carroll, 1884), a form of voting where representation is either direct or delegated transitively in a very liquid manner, in the hope that it would yield better representation and more participation.

Considering the radicality of these propositions, there is still relatively little research on the political consequences of such changes. Yet, throughout history, numerous scholars have studied why and how people vote, providing us with methodology and framework to analyze organizations and constitutions. Among the most prominent scholars to have used economics tools to analyze constitutional structures are James Buchanan and Gordon Tullock in *The Calculus of Consent* (1962).

While some of the conclusions drawn in their book are rooted in the technological context at the time of writing, the methodology remains relevant and proves to be extremely informative about BEV and Liquid Democracy (LD). This paper aims to initiate this field of research. Neither E-Voting nor LD depend on blockchains—nor on any particular technological implementation for that matter—and the issues addressed in this paper pertain to theoretical political economy rather than applied economics.

Using a political economy framework, I analyze the effect of LD on voting costs and representation focusing on the question of the intensity of preferences and representation structures. I show that, as a voting system, LD could effectively reduce costs and allow for more inclusive decision-making and may help reflecting the intensity of preferences of voters through logrolling. Blockchain-based systems may automate the process and create a transparent and auditable vote-trading marketplace, thus reducing the risks of manipulation or corruption. However, even if people are better represented under LD, there are no guarantees that delegating votes to more informed citizens will lead to better decision-making for the group. Extending the analysis to LD as a new form democracy reveals serious shortcomings in the capacity of voters to engage in direct or indirect vote-trading. Moreover, I recall that we are yet to find a system that is faithful to the ideal of LD and offers institutional room for independent legislative work. I then study small-scale communities and argue that, e-voting is more suited for local democracy than for national issues.

Liquid Democracy has historically been discussed alongside with specific technical implementations because it requires a digital system to be implemented. Most recently, many blockchain enthusiasts have pointed out that blockchains are natural candidates to be the substrate for the voting mechanisms that are explored in this paper. Consistently with the state of the art literature, this paper thus includes a technical implementation section where I discuss blockchain-based implementation to add a discussion of practical governance issues to the theoretical analysis carried out in the paper.

The remainder of the paper is structured as follow: in section 3.2, a literature review presents the major works in the field of institutional economics that influenced this research. An extensive review of LD is also carried out before presenting blockchains and in particular BEV with its *caveats* and unresolved issues in the hope to familiarize the reader with these concepts. Section 3.3 is devoted to applying institutional economics analytical tools to LD as a voting tool and as a new form of democracy before discussing implementation in terms of scale and technology. Finally, the results are summarized and discussed in the Conclusion.

3.2 Literature Review

3.2.1 Political Economy

Analyzing voting dynamics through formal mathematical modelization dates back to the 18th century with Condorcet (1785) who showed that majority voting was not transitive. In the founding *Social Choice and Individual Values*, Arrow (1951) completed this paradox with the impossibility theorem that states no rank order voting system can meet the five following criteria: (i) Non-dictatorship (no single voter can decide) (ii) Unrestricted domain (be deterministic and not context-dependent) (iii) Independence of irrelevant alternatives (preference between two choices should not depend on third choices) (iv) Monotonicity (social preferences are monotonous with respect to each individual's preferences) (v) Citizen Sovereignty (every outcome of the vote is theoretically achievable). Yet, most democracies rely on rank order voting because the conditions of the impossibility theorem are rather restrictive and not met in real life. D. Black (1958) showed that, under reasonable assumptions on preferences (unidimensional and single-peaked), majority voting meets all of the five criteria.

In *The Calculus of Consent*, Buchanan and Tullock (1962) retain the hypothesis of unidimensionality and single-peaked preferences and discuss voting rules under these conditions. Among the numerous topics addressed in their book, I concentrate on two arguments particularly important for our discussion. The authors mostly consider votes between two alternatives and can therefore ignore the impossibility theorem which does not stand in that case. However, unlike Black, they do not give particular importance to the majority rule. In turn, they discuss the optimal ratio $K^\star = \frac{R}{N}$ required for a motion concerning the whole group to pass where $N \in \mathbb{N}^\star$ is the size of the group and $R \in \{1..N\}$ is the number of voters supporting the motion. Note that the group will decide on a political constitution in the perspective of sustained cooperation, collaboration and provision of public goods. Inspired by Neumann and Morgenstern (1947), they rely on a game theory approach and build on the notion of equilibria of repetitive games.

When $R = 1$, anyone can propose a motion that will be automatically voted and will entail a group action. In that case, all the other members of the group are expected to bear the cost of a policy that will most likely only benefit its originator. On the contrary, if $R = N$ then unanimity is required for a motion to pass. In that case, the motion will benefit all members of the group, otherwise they would not vote for it.

However, when unanimity is required for a motion to pass, the cost of reaching consensus and cooperating is high as bargaining with all the members is required. In turn, when $R = 1$, no bargaining at all is required. Therefore, there are two costs to be expected:

External Costs imposed by decisions taken by and benefiting other members. These costs $C_E(R, N)$ are decreasing with respects to R

Decision-Making Costs imposed by the costs of bargaining. These costs $C_{DM}(R, N)$ are increasing with respects to R

Thus, there is an optimal $\frac{R}{N}^\star$ that minimizes the total costs $C_{Tot}(R, N) = C_E(R, N) + C_{DM}(R, N)$ and it is this ratio that the authors try to identify given the type of decisions the voters have to make. Note that, since N is a characteristic of the group, only R can vary. This optimal ratio depends on cost structure and will therefore be higher if external costs are likely to exceed decision-making costs. This is why a higher proportion of voters is often required to modify a constitution than to pass a bill.

Following this analysis, Buchanan and Tullock conclude that there are no reasons why $\frac{R}{N}$ should be 0.5. They also contend that a simple majority only makes sense under the assumption that all agents have equal preferences on all matters, in which case the majority should be chosen because that will yield the highest social output. However, they recall that most people have strong interest for some questions and a lesser one for others issues.

Suppose for instance that $N = 2$ and the individuals (n_1 and n_2) need to agree on two issues A and B. There are cases where n_1 is always better off with $\overline{B}$ rather than B (same goes for n_2 and A) but both are better off with (A, B) rather than $(\overline{A}, \overline{B})$. This is an example of the famous prisoner's dilemma. However, contrary to the original prisoner's dilemma, there is room for negotiation and agents can coordinate to ensure that both A and B are passed. n_1 renounces to block B if n_2 does so for A. More complex examples with $N > 2$ are presented in the book but it is enough for this discussion to limit ourselves to this simplified version.

What follows is that most people would be willing to renounce their favored outcome on the issue of least interest to guarantee their preferred outcome on the most important one. This leads to one of the major conclusions of *The Calculus of Consent* which is a call for *logrolling*. Indeed, according to the authors, the prisoner's dilemma emerging in political settings can be solved through vote trading, as shown above. In this case, achieving an outcome more favorable than the Nash equilibrium of $(\overline{A}, \overline{B})$ is possible because there are successive votes on different issues instead of a one-time choice and because vote trading (either direct or indirect) can be undertaken. More specifically, it only works if the horizon of votes is long enough so that any betrayal in the cooperation will be offset by losses in future collaboration. Although this conclusion is rather different from the Arrow's Theorem, this somehow echoes the limitations of rank order voting where voters are unable to express the intensity of their preferences.

In a later part, Buchanan and Tullock explore representation structures for unicameral and bicameral parliament to avoid manipulation by a small group and ensure that a ratio of K at the parliament faithfully represents the same ratio in the total population. It is also the concern for good representation that gave birth to LD as discussed later.

Lastly, among the various fields of research building on *The Calculus of Consent*, one is particularly important for us: discussing the vote market. While Buchanan and Tullock champion vote-trading, they do acknowledge that vote-buying might raise moral questions. Specifically, they insist that vote-trading offers must be completely transparent in order for the voters not to be and feel manipulated and that vote-buying might not offer such guarantees. This central argument of the book has laid the ground for further political liberalism, such as Parisi's Political Coase Theorem (Parisi, 2003). Extending Coase's conclusions (1960), he claims that if there are no transaction costs and if the market for votes is complete, then a socially Pareto-optimal equilibrium will be achieved independently of the voting system. This stance has been challenged (Munger, 2019) but provides an interesting extreme position to bear in mind when thinking about vote markets.

Other libertarian authors (Posner and Weyl, 2015) have explored alternatives to express intensity of preferences and a market for vote-buying, such as Quadratic Voting (QV). Under QV, people would be able to buy more votes on subjects they feel more concerned about, with the price being a quadratic function of the number of votes. This is of importance for us because blockchains scholars such as D. W. E. Allen et al. (2017, 2018) claim that blockchains can implement new forms of democracy, in particular QV. Quadratic Voting is already extensively discussed, including by economists, and this paper will not address it. Rather it complements D. W. E. Allen et al. (2017) in their study of "crypto-democracy" and analyzes another form of preference aggregation.

3.2.2 Liquid Democracy

Liquid Democracy (LD) is a relatively recent concept and is still not consensually defined which makes it hard to specify exactly what is being discussed. Inheriting from delegative and proxy voting theory, and sometimes still called by these names, LD can define either a voting mechanism, an evolution of participatory democracy or a new form of democracy (Paulin, 2020). Another difficulty comes from the fact that there is relatively little academic research dedicated to the subject and a lot of the documentation comes from gray literature (B. Ford, 2014).

Although they can be traced back to Carroll (1884), the principles of LD were firstly conceptualized by Miller (1969) when proposing a method for "direct and proxy voting in the legislative process". The idea was to make the best of the (then relatively new) computers to foster more direct democracy, to allow for better representation and to increase participation. In such a system, each citizen could decide to delegate their vote to anyone who would effectively become a representative. Those entrusted with the most votes would become legislators. People could, at any time, decide to withdraw their delegation and vote for themselves.

According to Miller (1969), it is impracticable for everyone to be an expert on all issues and it is more efficient to delegate votes to more knowledgeable persons that one believes to be aligned with her ideas. What is more, representative democracy does not reflect the mantra *one person, one vote* and LD would reflect more faithfully the will of the citizens. As recalled by Green-Armytage (2015), this paper remained relatively unnoticed, with the notable exceptions of a discussion by Shubik (1970) and a similar contribution by Tullock (1972). It is only with the boom of computerization that the idea of proxy voting gained significant momentum.

Tullock (1992) made a proposal rather close to the one by Miller (1969) based on a device linked to a television to follow parliamentary debates. Citizens could then decide to give their vote to any representative or vote directly. This work was extended by Alger (2006) who demonstrated that his proposition allows to overcome the tradeoff between "the representation of a legislature stemming from a voting system and either constituent services or government stability" (p.2) and that, provided that the system follows a few ancillary rules, it is a better form of representation. Interestingly, Alger (2006)'s proposal is explicitly designed to be implemented when voting for a legislature and for operating the said legislature, as the two are too entrenched to be designed independently.

Parallelly, B. A. Ford (2002) and Green-Armytage (2005) introduced a new element in proxy voting: transferability of proxies. Not only were people allowed to delegate their votes to an expert, but that expert could, in turn, delegate her vote and all those she had received to someone else. Adding this aspect Blum and Zuber (2016, p.4) propose the following definition:

> Liquid democracy is a procedure for collective decision-making that combines direct democratic participation with a flexible account of representation. Its basic model consists of four components that can be stated as follows: All members of a political community that satisfy a set of reasonable participatory criteria (adulthood, baseline rationality) are entitled to:
>
> (I) directly vote on all policy issues (direct democratic component);
>
> (II) delegate their votes to a representative to vote on their behalf on (1) a singular policy issue, or (2) all policy issues in one or more policy areas, or (3) all policy issues in all policy areas (flexible delegation component);
>
> (III) delegate those votes they have received via delegation to another representative (meta-delegation component);
>
> (IV) terminate the delegation of their votes at any time (instant recall component).

Besides the meta-delegation, Blum and Zuber (2016) mention another aspect of LD: delegation per topic. Originally mentioned by Miller (1969), delegation per topic is now widespread in the literature (B. Ford, 2020; Green-Armytage, 2015). While this aspect is usually connected to LD as a voting method, but Blum and Zuber (2016) link it to a broader political system that I discuss in subsection 3.3.2.

Implementations of LD and academic literature on the subject remain rare. Paulin (2020) reviews them and proposes to differentiate LD as a voting tool and a new form of democracy. According to him, very few initiatives are considered to truly amount to LD.

Blockchains are one of the reasons that explain the ever-increasing interest in LD. If the idea of proxy voting stemmed from the development of novel communication processes, blockchains offer a very promising platform for LD. Indeed, proposals are now flourishing (C. Berg, 2017; Fan et al., 2020; Kashyap and Jeyasekar, 2020) but most remain rather technical and focus on implementation issues but, to the best of my knowledge, a theoretical political economy analysis of such a proposal is still to be undertaken.

3.2.3 How Blockchains Work

Blockchains are peer-to-peer distributed ledgers—generally referred to as Distributed Ledger Technology (DLT)—recording transactions in an append-only way. Transactions are grouped into "blocks" and then added to the "chain" of previous blocks. The specificity of blockchains is that they are, by design, transparent, verifiable and permanent in the sense that it is extremely hard to modify their records. This high security is achieved through encryption and hash of the data and of the blocks; this ensures that tampering attempts can be detected by various members of the network (Vujičić et al., 2018). The process of adding and encrypting blocks relies on a lottery that guarantees decentralization and that consensus is achieved without the any form of central authority.

Decentralization, transparency and security through encryption were the main features of the blockchain technology as devised by Nakamoto (2008), created to support Bitcoins, a decentralized cryptocurrency. At the time, the information recorded in the blocks was mostly a financial ledger. But the establishment of the consensus mechanisms design for DLTs has since fostered for the development of new ideas about decentralized governance.

Increasingly complex forms of interactions over blockchains have been made possible over time with the development of new blockchains. For instance, Ethereum was the first blockchain with the capacity to compile a Turing-Complete programming language (Wood, 2014b), opening ways for distributing virtually anything that carries value through blockchains. In particular, it made it possible to code smart-contracts that had first been described by Szabo (1997) but were impracticable at the time. Smart-contracts are self-executing chunks of code that are recorded into a block. Once they are on the blockchain, they are as immutable as the blockchain is.

However, this security can also be a weakness. Blockchains are tamper-resistant when the attacking parties have less than 50% of the stake (depending on the consensus mechanism, it may be value, hashing power etc.), but when nodes reach consensus on a modification, the whole structure and protocol of the blockchain can be amended. Therefore, the governance of the blockchain (as an infrastructure) has consequences for all the ecosystem living on top of the blockchain. The governance of blockchains takes place both *on-chain*, through code implementations, and *off-chain*, by the means of formal and informal institutions (De Filippi and McMullen, 2018).

3.2.4 Blockchain-Based Organizations

As the technical opportunities offered by blockchains increased, the field of applications widened and has been considered to revolutionize virtually every field of society.[1] It includes classical and new forms of economic organizations (Davidson et al., 2018) either in the market economy or for more Commons-oriented organizations (Troncoso and Ultratel, 2020). Blockchain-based organizations can either rely on blockchains to supplement coordination, automation and decentralization of off-chain processes or be fully distributed over a blockchain. In all cases these blockchain-based or blockchain-enabled organizations

[1] A significant overview can be found in De Filippi and Wright (2018).

require a rather complex set of smart-contracts. That necessarily raises many coordination challenges and entrenched difficulties (Howell and Potgieter, 2019b).

More importantly, blockchains bring up challenges and opportunities for government. Atzori's account of these issues remains one of the most complete to date. She notes that:

> Broadly speaking, the advocates of decentralization tend to have in common the same dissociative attitude towards centralized institutions [...] Many enthusiasts simply promote the blockchain as a more efficient, decentralized and consensus-driven public repository, which can have a number of applications in order to make citizens less dependent on governments, yet within a society that is ultimately founded upon the State authority. (Atzori, 2017)

This dichotomy is found in particular in the literature around Blockchain-based E-Voting (BEV). Indeed, among the champions of voting on blockchains are crypto-anarchists (De Filippi and Wright, 2018) but also many who could be characterized as "reformists" for whom BEV is to be used in our democracies just as a tool. Most of the papers presented in the following section belong to the reformist strand. BEV could merely be a voting tool but it could also be a first step to creating institutions outside of the State framework and new forms of democracy. These two approaches have very different consequences that this paper lays out to analyze their implications within a framework of institutional economics.

Whichever purpose it serves, a blockchain-based organization will necessitate governance of the organization and of the technology it relies on (De Filippi and McMullen, 2018). Governance of blockchains can be either distributed, decentralized or, in practice, rather centralized in the hands of foundations or central parties (Howell and Potgieter, 2019a). As I discuss later, ignoring the challenges of governing the blockchain leaves a significant blind spot in the analysis. This is all the more true as the term "blockchain" covers various implementations in terms of consensus mechanisms and publicness. Each implementation yields its own governance challenges and the choice of the type of blockchain to host a blockchain-based organization, let alone a voting system, implies assumptions and specific challenges.

3.2.5 Blockchain-based E-Voting

Gibson et al. (2016) provide an interesting history of online voting and its challenges and recall that "As the internet evolves, then so also do the remote voting systems built upon it" (p.280). It is, therefore, not a surprise that blockchains, which have been dubbed as the Web 3.0 (Wood, 2014a) are considered for e-voting.

E-Voting and Blockchain-based E-Voting (BEV) must solve the same problems as other technologies. As underlined by Lessig (2006, pp. 141-143), there are extremely challenging difficulties. In particular, the system must simultaneously ensure anonymity in the vote (discussed in subsection 3.3.2), transparency and verifiability to ensure that the vote is not modified not to forget the issue of digital identity, detection of fraud or coercion. Additionally, the issue of unique and singular digital identities is a challenge in and of itself (Siddarth et al., 2020).

Osgood (2016) cites Norden and Famighetti (2015), a report showing that, in the 2016 US Presidential Elections, "43 out of 50 states used EVMs [Electronic Voting Machines] that were at least ten years old [and] notoriously easy to hack and tamper with". However, despite these well-known and unresolved issues, Osgood (2016) is optimistic about the potential of BEV to solve these issues. By design, blockchains are difficult to tamper with and offer a level of security and transparency that may revolutionize collaboration between actors. An interesting nuanced and extensive account of using blockchains for e-voting is provided by Dhillon et al. (2019).

Osgood (2016) is not the only optimistic scholars as numerous authors such as Hanifatunnisa and Rahardjo (2017), Hardwick et al. (2018), Hjálmarsson et al. (2018), Kshetri and Voas (2018), Takabatake et al. (2016), and Yavuz et al. (2018) have proposed designs and implementations of BEV. The booming interest in BEV all around the world is, thus, undeniable.

Despite its challenges, at least in practice, great hopes lie within the blockchains-enthusiasts community. My goal is not to discuss these propositions nor BEV in general but rather to apply the analytical framework of institutional economics to BEV, as it gathers significant momentum worldwide at the time of writing.

3.2.6 Institutional Economics and Blockchains

While a fairly recent and developing field, the foundations of an institutional economics analysis of blockchain-based organization have been laid out by a few recently-published papers. Wagner's volume (2019) comprises two chapters analyzing the legacy of Buchanan and Tullock in the field of blockchains.

In chapter 17, Rajagopalan (2019) focuses on the technical aspects of blockchains. He follows Lessig (2006) and De Filippi and Wright (2018) in their conclusions that the code entails "constitutional constraints" and recalls that distributed ledgers are mostly a new way of reaching a consensus.[2] He then applies their framework to cryptocurrencies, a form of club goods. In this paper I seek to extend this work to other applications of blockchains, specifically voting platforms.

In chapter 18, C. Berg et al. (2019), following the definition of crypto Public Choice (A. Berg et al., 2018), go beyond cryptocurrencies and explore the possibilities of "institutional cryptoeconomics", claiming that blockchains offer the opportunity to try new constitutional orders. Blockchains thus constitute methodological tools to explore potential arrangements

[2]Which is exactly the problem Buchanan and Tullock (1962) addressed.

and new sets of rules. I will attempt to further this work by proposing a first analysis of a Liquid Democracy constitutional order relying on a blockchain.

By extending the conclusions of the above-mentioned papers to a concrete constitutional proposal, this paper contributes to furthering the field of institutional economics analysis of blockchain implementations.

3.3 A Political Analysis of Liquid Democracy

According to D. W. E. Allen et al. (2017), every institution is situated within the technological context of its time. When constitutions were drafted, no one could have possibly imagined the advent of the Internet and blockchains, which have since opened tremendous possibilities. Nonetheless, the analytical framework devised by political economy at the end of the 20th century remains relevant for addressing new technologies in relationship with politics and voting matters.

This section analyzes Liquid Democracy in the light of the issues presented in the literature review. It first concentrates on Liquid Democracy as a voting mechanism without changing the way the legislature works before extending our discussion to a modified institutional context. The discussion addresses both general LD and its blockchain-based applications, focusing on the new governance challenges that a shift towards LD could entail.

3.3.1 Liquid Democracy as a Voting Tool

Let us first consider the case of LD used as a voting mechanism. To be clear, let us take the case of a group of people who need to vote on different issues and make decisions that are binding for the group. Such a group might, for instance, be a parliament or more simply a group of shareholders for a company. Closer to the blockchain world, it can also be token holders of a DAO.[3]

In that group, voting rules follow the four principles described by Blum and Zuber (2016) and reviewed in subsection 3.2.2: (i) citizens can vote directly, (ii) they can delegate their votes on one, some, or all areas to a representative, (iii) delegation is transitive, and (iv) delegation can be terminated at any time.

Reassessing the Epistemic and Egalitarian Arguments

Blum and Zuber (2016) propose a "normative democratic theory" framework to assess the advantages of a voting system through 2 criteria: (i) the epistemic account assesses how

[3]DAOs are communities of blockchains users managing an asset made of smart-contracts and relying on participative governance processes.

good a system is at discovering the best solutions and (ii) the egalitarian account refers to how well citizens are represented in this system. For instance, enlightened absolutism would rank very high on the first account, and very low on the second one. They argue that LD outperforms traditional representative democracy on both accounts. I retain their two-pronged framework but I propose to complement their analysis and discuss their conclusions. According to the analytical elements of *The Calculus of Consent*, some points seem to back their position.

First off, for a given voting rule (a ratio of voters required to pass a bill) decision-making costs are likely to be reduced through delegation and concentration of votes while external costs should not change. Indeed, LD allows a citizen to delegate her vote to an expert she "trusts" to be more informed and aligned with her views. Classically, an expert receiving votes is called a "guru". Everyone can have 0 guru (vote directly for each subject), 1 guru (delegate all her votes to one guru) or several (1 for each area for instance). Let us assume that each guru has p votes on average ($p-1$ voters delegated her votes to her); then to represent a ratio of K, only $\frac{R}{p}$ gurus out of $\frac{N}{p}$ need to agree before a decision. In that case, the cost structure becomes $C_{Tot}^{LD}(R,N,p) = C_E(R,N) + C_{DM}(\frac{R}{p}, \frac{N}{p})$. Because $C_{DM}(\frac{R}{p}, \frac{N}{p})$ is increasing w.r.t. both R and N, $C_{Tot}^{LD}(R,N,p) \leq C_{Tot}(R,N)$ for $p > 2$.

This does not necessarily imply that the optimal ratio will increase[4] but it is possible to increase the chosen ratio while still reducing total costs meaning that LD will pass more unanimous bills. This therefore validates the egalitarian argument: if the voting rule is closer to unanimity then everyone's interest is better taken into consideration.

On the contrary, the epistemic argument has faced strong drawbacks from recent literature. Research from Caragiannis and Micha (2019) suggest that local delegation algorithms might not be good at selecting "better" alternatives. In other words, if there is a vote between two alternatives and that one is objectively better than the other, LD might not be more efficient at selecting it than direct democracy and there are cases in which LD fares worse than the alternative. Even when delegation only goes towards more qualified gurus, worse outcomes could be reached. What is more, Escoffier et al. (2018, 2019, 2020) have shown that reaching an equilibrium is NP-hard under several forms of networks (along which delegation can happen). A NP-hard problem is a problem for which we cannot compute a solution in a polynomial time[5] and we do not know if it is theoretically possible to do so. It is thus computationally difficult to achieve optimal delegation networks and that poses *caveats* for choosing LD. Finally, Bloembergen et al. (2018) try to measure the efficiency of LD and evaluate the gain (previously defined in Kahng et al., 2018) that represents "the group accuracy after delegations versus the group

[4]Proving this requires making assumptions on the second derivatives of the costs functions.

[5]In polynomial time algorithms,the solution is found in a time that depends polynomially on the complexity of the input. They are considered to be reasonably scalable algorithms, opposed to exponential ones.

accuracy achieved by direct voting". This proves to be inconclusive as the gain can take all the values possible, which means that the accuracy can either increase or decrease, making the epistemic argument precarious.

In the language of Public Choice used in this paper, these complexity results translate as follows: it is unsure that a LD vote will result in a Pareto-dominant situation.

Blockchain-Based Vote-Trading Platforms and Logrolling

Another reason why blockchain-based LD could help the group adopt more socially efficient bills is through logrolling and vote markets. I mention in the subsection 3.2.1 that *The Calculus of Consent* argue that trading votes is necessary, in particular for minorities to still be represented on the subjects that concern them most thus avoiding a "tyranny of the majority". However, vote trading remains subject to conditions. Voters will be extremely reluctant to trade votes when opportunities are not clearly announced and that there are risks of manipulation. In particular, most voting systems have the essential requirement of preserving vote secrecy which makes it impossible to verify that votes have been casted according to the contract. Nonetheless, for some parliamentary votes or small groups decision-making, secrecy is not required nor even desirable. This applies to holding representatives accountable, for example. In these cases, open vote-markets could be beneficial. *The Calculus of Consent* do discuss the conditions necessary to engage confidently in logrolling. Two of them are transparency and certainty of execution.

Blockchains create new opportunities in that regard: they allow for the organization of a transaction platform for votes as blockchains are appropriate for the markets of "complete contracts" (Davidson et al., 2016b). Vote trading can be considered to be as complete as possible: all the states of the future world pertaining to the contract can be considered and logically described within the code of the contract. So, we could imagine a platform on the blockchain on which voters would openly advertise their votes enabling open logrolling with a guarantee that there will be enforcement of the trade.

Suppose two votes on subjects A and B are planned and voter i publicly announces that she is willing to redeem or vote on A against a vote for B. Voter j sees this and engages in the vote. A smart-contract is used to ensure that j holds two votes on the first issue and i two for the second. Voter secrecy could still be preserved with i and j voting confidentially (as if there was no vote-trading) but with two votes on their respective subjects. Note that, in this case, transfer of vote is different from vote delegation as defined in LD democracy. Indeed, delegated votes are revocable while votes in vote-trading contracts are not. Vote-trading smart-contracts should thus be designed specifically if authorized by the constitution.

This two persons/two subjects situation could soon be generalized. Smart-contracts could be designed to automate vote-trading. We could even imagine a platform where people could identify other people with non-aligned strong interests and start trading campaigns advertising for vote-trading opportunities. If that was to be implemented, that would, once more, back the egalitarian argument. Indeed, not only would everyone's voice be heard but they would also be heard in proportion to the intensity of their opinions. However, it would require everyone to rank their preferences on all subjects. Literature on Single Transferable Vote (STV) which also requires to rank all the preferences always recall that it is rather complex to ask voters to rank all the options when the list is long (Endersby and Towle, 2014; Tideman, 1995).

The Calculus of Consent also state that (monetary) vote-buying is an efficient way of revealing social preferences at the scale of the group. Vote-buying raises more social concerns than logrolling and vote trading but is not condemnable *per se*, according to the authors. If public advertising of vote trading opportunities and automation of such exchanges are possible, a market for votes could emerge, either implemented within the voting platform or parallelly. In this case, the issue of complete ordering of preferences may raise another type of issue: arbitrage.

Suppose i identifies an arbitrage opportunity: she trades votes with j on subjects A and B, that is to say i gives her vote on A to j against her vote on B and x in a currency (most presumably a cryptocurrency). If i later trades votes with k, yielding her vote on subject B and $y < x$ for a k's vote on A, then i made money ($x - y > 0$) and j's preferences are not taken into account (and j lost x). In the case of a market with perfect information, which is the case of a blockchain platform, equilibrium should be reached revealing aggregated social preferences. However, although vote-trading opportunities are complete contracts, it is unsure that an equilibrium similar to swap markets for cryptocurrencies can be achieved.[6] Voters do not always act rationally and the market for vote-trading may therefore not be competitive and rational and it may not lead to Pareto-efficient situations (Caplan, 2003; Casella et al., 2012; Frey and Eichenberger, 1991). This calls for caution in the design of the vote-market raising serious concerns about monetization of votes.

Should vote-buying and marketplace be illegal, one of the advantages of blockchain-based platforms is that they are transparent, making it possible to monitor forbidden transactions. On the contrary, automation and decentralization on blockchains make it virtually impossible to prevent smart-contract from being executed or illegal market places from running thus making enforcement challenging. In the case of accountable members of parliament, it is likely that social pressure and the risk of losing their position would be enough to deter them from engaging in illegal activities. However, these safeguards might be less efficient in the case of larger communities with fewer guarantees, making it hard to effectively ban vote-buying.

For parliamentary groups, the transparency of blockchain-based platforms is also useful

[6] However, on distributed swap markets, temporary disequilibrium may exist. Equivalent on a vote market may have disastrous consequences.

to hold its members accountable to their constituents. Transparency helps to reduce the risks of corruption and lobby-induced logrolling increasing the moral legitimacy of vote-trading.

In conclusion, adopting blockchain-based Liquid Democracy as a voting mechanism could help reduce decision-making costs between actors thus favoring a more inclusive threshold to pass bills. Contrary to direct democracy where the intensity of preferences is not taken into account and logrolling is difficult, LD allows to trade votes and structurally enables vote-trading. Recourse to blockchain-based platforms offers technical solutions to ensure that vote-trading is made openly with the possibility to offer auditable logrolling smart-contracts while still preserving vote secrecy when necessary. The risk of a monetary market for votes raises important theoretical and moral issues that must be carefully addressed should a group decides to adopt a blockchain-based LD voting system.

Algorithmic theory warns us that recourse to LD does not guarantee a more efficient outcome than direct democracy, making virtually impossible to compare the two systems under the epistemic account. Nonetheless, our analysis proves that the egalitarian argument does hold and that not only more unanimous decisions are made but that intensity preferences are also better accounted for.

3.3.2 Liquid Democracy as a New Form of Democracy

I now extend the analysis to the cases where Liquid Democracy is not only a voting mechanism but also a new form of democracy. There is no consensus yet on what it means to adopt Liquid Democracy as a new form of democracy. Almost all the authors discussed in the literature review propose different alternatives, but they all share one common feature: LD is used as a voting mechanism by all citizens who can express their votes on all issues. Therefore, the group is much larger than those previously discussed and, contrary to the examples presented above, voters have to deal with many different issues and do not have the capacity to become experts in all of them, making delegation more necessary and likely[7]. Along with LD, some institutions remain necessary (to draft laws, to vote on a budget…). This is where the variations in the propositions are most significant.

Logrolling in Liquid Democracy, Is Bundling Still Possible?

The previous section underlined that logrolling would be easier in the context of LD as a voting method. However, the rationale for engaging in vote-trading when LD is a new form of democracy would be unclear.

[7] In the case of parliament discussed above, representatives must also vote on many issues but this is their main activity with more time to do research on the issues.

Suppose a guru g_i receives $p_{i,A}$ votes for her field of expertise (domain A) but does not vote (or not with as many votes at least) on subject B ($p_{i,B} \ll p_{i,A}$). Therefore, a guru g_i has little to no negotiating power and cannot weigh in to push forth her expertise. She is also extremely unlikely to sacrifice the vote she holds for domain A because she might lose these delegations at any time. Consider two votes on domain A and B planned to happen on two consecutive days and gurus g_i and g_j wishing to engage in vote trading, g_j lending her votes today for g_i's votes tomorrow. Because one key feature of LD is that delegation withdrawal can happen at any time, g_j has no guarantee that she may receive enough votes tomorrow and will not rationally engage in vote-trading. This echoes the point made in the previous section: it is necessary for vote-trading transfers not to be recallable. This should also be the case for all votes held by a guru, but this would contradict the fourth feature of LD as defined in subsection 3.2.2.

Without sacrificing that feature, what will happen is that for each subject, votes will take place independently from other domains. A guru has no way of knowing the intensity of the votes she received and has nothing better to do than to vote according to her expertise. Whichever decision-making rule is chosen (apart from unanimity), a (qualified) majority with weak views could impose a choice to a strongly interested minority. In the current forms of democracy, vote-trading takes place through political parties. They propose election programs that are bundles of varied proposals in the hope that they will gather voters from different sides who consider the bundle in accordance with the issues they value most although different voters might not agree on which parts are positive. Parties are a way of knowingly trading votes: an agent will vote for an ensemble in which there are motions they oppose (lightly) and motions they champion (strongly). As discussed in this section, LD would make political parties obsolete because people would be represented directly and bundling and *de facto* vote-trading would also be out of the question.

Another difficulty would be the chronology of different votes. Buchanan and Tullock typically did not cover transaction and organization costs in their analysis but organizing elections and voting itself is costly for both the institutions and its members even if LD reduces costs. It is therefore impossible to continually consult citizens on different issues and an agenda would have to be devised. It is unclear how election frequency affects turnout (Garmann, 2017) and election frequency impact on logrolling has not been studied extensively. However, it seems safe to assume that if an agent believes the issue she cares most about will not be subject to a vote before long, her interest might be discounted. The question of discounting factor in logrolling calculus has been introduced, although in a somehow different context, by Carrubba and Volden (2000).[8] This adds another difficulty for gurus and voters to engage in vote trading on the behalf of those who confide in them.

[8] Notably, they are interested in logrolling in parliaments and reach the conclusion that the more frequent the elections, the higher the discount factor for MPs as they face the risks of not being reelected.

To the best of my knowledge, the literature on LD has identified its shortcoming in terms of bundling but has never formally analyzed it in terms of its difficulty to reflect the intensity of preferences. For instance, Blum and Zuber (2016) mention briefly the question of bundling and political parties (p.18) but do not provide a detailed analysis. What is more, the solution they propose—delegating votes on broad fields and not just on single issues—does not seem to solve this issue as cross-domains trades would still be difficult.

Institutional Structure and Representation in Liquid Democracy

In the previous section, I asserted that the capacity for gurus to engage in logrolling will depend on the constitutional framework for LD. For instance, I have noted that the issue of the political agenda will be crucial and that whether gurus can lock in the votes they hold in a logrolling contract strongly influences the outcome of the different votes. To further the analysis, let us now focus on what the literature says about different institutional structures in a LD democracy in particular regarding representation of minorities and expression of intensity of preferences.

First off, Miller (1969) proposed to use LD to delegate voting power to representatives, maintaining the concept of a parliament. In practice, if the House has N representatives, the N gurus with the most votes would be Members of Parliament (MPs) and their mandate would last for a given period of time to ensure stability (2 years in the original paper). Citizens would then be able to choose between the different MPs currently "elected". This proposal does not meet the 4 criteria of LD democracy because votes can only be transferred to a very restricted set of gurus. It would, however, solve the issue of vote trading, as MPs receive the votes on all matters. However, as the number of votes a given MP holds at a given time is not guaranteed, engaging in vote trading on votes discussed later in the agenda could not happen as seen above.

Blum and Zuber (2016) propose a solution that is closer to the spirit of LD which is based on "trustees". Instead of continual delegation of votes and immediate recalls, they propose a delegation phase and then a debate phase. During the debate phase, the gurus keep all their votes, and after pondering over the arguments of different sides, vote for all the delegations they hold. Interestingly, a period in which delegations are guaranteed would allow for vote trading but only if the agenda regroups issues pertaining to different domains. One could contemplate mixing this "trustee" proposal with a sort of imperative mandate. A voter could fix objectives to her guru, delegate her vote (on a group of themes or all her votes) unquestionably and without the possibility to withdraw votes within a period, but at the end could automatically recall her vote if the objectives are not met. This would incentivize gurus to take into considerations the preferences of her "trusters".

Smart-contracts are natural candidates for such a delegation although this would require being able to formally codify the expectations which may be complex. This idea could be compared with B. Ford (2020) micro parties who strongly support one priority. Contrary to Miller's proposition (1969), this does not explicitly address the issue of parliamentary work which goes well beyond just voting for laws. MPs are also responsible for legislative work, drafting bills, commission work… and there are no control mechanisms in their proposition to ensure these tasks will be done. Finally, and very questionably, Blum and Zuber (2016) propose to put gurus' deliberation under the oversight of the executive, which would virtually put an end to the separation of powers.

Green-Armytage (2015) proposes a mixed system between direct and proxy voting, close to the one proposed by Alger (2006). Voters elect legislators through an ordering method (he proposes STV) and, on each issue, can either decide to vote directly or to delegate their vote to a "public voter", another name for a guru, of their choice (the gurus can overlap with legislators). The gurus then vote either directly or delegate their voice to another one. This effectively addresses the issue of legislative work including the management of a national budget. However, it does not address the issue of logrolling and vote-trading since voters can always decide either to vote directly or to change the guru they delegate their votes to.

We see that, so far, no proposition for a LD based democracy has managed to simultaneously address the issue of how to maintain the legislative work and reflect the intensity of preferences of the citizens. In their chapter 16, *The Calculus of Consent* discuss one more question concerning parliamentary representation. They show that a bicameral system makes decision rules more inclusive (closer to unanimity) as long as constituencies between the two houses are different enough. When voters can choose which representative to delegate their vote to, this condition of separate constituencies cannot be respected anymore. The argument of *The Calculus of Consent* was that with representation and only one house, 51% of the representatives, each elected by a short 51% of their constituencies could pass laws that effectively favor only 26% of the total population. Arguably, the possibility to withdraw votes and delegate them to another guru nullifies this risk and makes the parliament a faithful mirror of the society. However, it seems unlikely that every citizen will constantly monitor what their gurus do—otherwise they would be better off voting themselves—and there might be cases where a bill is passed that is only supported by less than a majority.

Even if that is not the case, there is another argument for a bicameral parliament: not only does it prevent the formation of minimum winning coalition inferior to $R^\star$ but it also helps pass more unanimous proposals, only marginally increasing decision-making costs and significantly reducing external costs. Among the work reviewed here, only Miller (1969) proposes to have two houses but with voters being able to freely choose their representative in both houses. This essentially makes them redundant and duplicates their costs without bringing significant improvements over a unicameral parliament. One could consider the possibility of combining a traditional Senate with a LD democracy. This would not address the issue of logrolling mentioned numerous times in the LD House but, as mentioned by Green-Armytage (2015) about the legislators, it is likely that the Senate would still rely on political parties. This would reintroduce a form of bundling, although it is unclear how that would interact with the other House.

This section has revealed limitations in LD as a new form of democracy. In contexts where a large community is consulted on many different topics, there are no propositions[9] of a constitution that guarantees a proper framework for legislative work and that allows to reflect the citizens' intensity of preferences through logrolling. Some proposals present adjustments to facilitate logrolling or to resemble representative democracy, but this is always made at the expense of important features of Liquid Democracy. This paper contributes to the literature in the hope that these issues will be taken into consideration in the new solutions that will undoubtedly be proposed in the future.

3.3.3 Liquid Democracy for Local Democracy

The previous sections identified issues that may occur when scaling up LD and using it as a new form of democracy. Most of them, either finding an efficient delegation pattern of trading votes or keeping voting costs low, only get worse with the size of the group. For small groups voting on a small number of consistent issues, it is possible that the drawbacks mentioned above would be outshone by the improvements enabled by LD. Unsurprisingly, all the examples reviewed by Paulin (2020) concern small scale communities. This section moves away from the conceptual standpoint adopted thus far and discusses the practical costs and benefits of local LD.

Let us look at the municipal scale which, in many cases, constitutes the smallest scale for elections. Depending on the country, cities have different prerogatives but they cover only a rather limited and local scope of higher interests for the voters. This is exemplified by a higher turnout in local elections and in smaller cities (Dahl and Tufte, 1973; Frandsen, 2002). The relatively small number of subjects to decide upon, the denser network of constituents and the small size of the group can make the limitations less stringent.

Rather, LD in this setting could allow for more participatory democracy. Voters could be asked to vote more regularly replacing the municipal council on some or all issues. Having a system with both a municipal council and LD could bring some of the security assurances provided by the bicameral system. Direct democracy at a local scale has existed in Switzerland for a long time and the previous sections have shown that LD can work in settings where direct democracy is possible. Thanks to delegation, the general turnout for direct solicitations is likely to be higher while making it possible for people to engage in local vote-trading.

Even more so, in smaller communities, people are more likely to know well and be aligned with their gurus on several issues, thus reducing the risks of not being aligned with

[9] As of the end of 2021.

their vote-holder. That would make it easier for gurus to engage in formal or informal logrolling as they could provide more guarantees about the votes they hold.

Unfortunately, there are no examples of local governments relying on Liquid Democracy (yet) but this indicates that LD is more promising as an extension and improvement of local direct democracy than an alternative for large scale representative democracy. There are increasingly more examples of groups delegating governance over blockchains exploring their potential and limitations in practice. A blockchain-enabled smart city whose governance would rely partly on LD would be a good way to test the conclusions of this paper.

3.3.4 Governance of Voting Platform and Implementation Challenges

Beyond the electoral dynamics, recourse to digital tools for voting purposes challenges the control of the process. While it is not the scope of this paper to extensively discuss implementation and technical issues, it would be a large blind spot not to acknowledge and identify them.

Some of these difficulties concern e-voting in general while some are more specific to blockchain systems. Among the former, we should note digital identification, non-coercion, trustworthiness, reliability and management of the platform. They have been underlined frequently, in particular by Lessig (2006, pp. 141-143) who calls for transparency in the voting process, a transparency that, he claims, can only be achieved through open-source code so that citizens can verify the election process. But this leaves open the question of the structure of the voting platform; it could be centralized and managed by a state or it could be completely distributed and managed by the community. An election can only be as trustworthy as the tool used to vote. Centralized solutions make sense when there is high confidence in the State. Today, all the states who have implemented a digital identification system have done so in a centralized way with IDs being recorded in central databases (Sullivan and Burger, 2019, p.240). This allows for privacy and control of the rights inasmuch as the States is considered a trustworthy of this data.

However, if the goal of LD is to refocus the democratic process on bottom-up participation and horizontal organization, it is only natural to question this centralized approach and discuss alternatives. Blockchains could provide a distributed solution to some of the aforementioned issues (transparency, monitoring, reliability, horizontal governance) but would raise a new one: governance of the tool itself.[10] A blockchain is either a club good or a public good managed by its users.[11] However, how the power is distributed among

[10]Such an issue would arise for any kind of distributed platforms but, consistenly with the rest of the paper, only blockchains are discussed.

[11]In both cases it is non-rivalrous but exclusion may be easy (private blockchains) or impossible (public blockchains).

them may significantly vary.

Howell and Potgieter (2019a,b) have shown that although blockchains can sometimes be managed as Commons, most of the time there is concentration of power in the hands of a small set of users (the founders, the largest miners, a foundation to name a few). In public Proof-of-Work[12] blockchains such as Bitcoin or Ethereum, block validators grouped in a "mining pools" representing more than 50% of the computing power could theoretically boycott some information and record on the blockchain fraudulent information. Concentration of power poses challenges when blockchains are being used for financial purposes (influent agents of Bitcoin have tremendous economic and strategic power), but the consequences could be even more dangerous in the case of political matters.

Among the possible solutions let us mention using semi-public or permissioned blockchains where only pre-approved agents are authorized to validate the data for instance. This way, one could achieve a level of transparency, involving anonymous and potentially malevolent actors. There is also increasing research to promote alternative and less environmentally harmful consensus mechanisms (such as Proof-of-Authority) but it is unlikely that they will be more tamper-resistant. Another solution might be to rely on side-chains of other large blockchains. For instance, governance of these side-chains could be permissioned to allow for control while the state of the side-chain would be committed to the public blockchain to benefit from its security.

There are countless possibilities, depending on the requirements of the situation. A State-backed election will more likely choose a rather centralized permissioned blockchain, while some groups might need more decentralization. But the discussion needs to go further as, when using an external blockchain, the group implicitly relies on the governance of the blockchain itself thus giving power to agents that might not even have a right to vote in this election. Somehow, this challenges the assumption that blockchains eliminate the need for third parties as the blockchain (both the infrastructure and the governance process) becomes an intermediary in the voting process.

In any case, this will result in a trade-off between security, decentralization and trust. To carefully consider the outcome of this trade-off, we should note that the way people perceive their state is highly dependent on the technology that the public service relies on (Bodó and Janssen, 2021). Once again, the question of scale is highly relevant. A form of distributed ledger without strong technical security (such as a private blockchain) might make sense in small communities with reputation mechanisms and low risks of free-riders while the situation is wholly different for large groups. This is another illustration of Olson's results on the difficulty of avoiding free-riders depending on the size of the group (1965). Conversely, governing collectively the voting platform could increase the level of community involvement and strengthen participation through a sense of increased agency. Technical implementation decisions are thus strongly conditioned by the homogeneity and

[12]The first consensus mechanism which relies on trying to solve difficult algorithmic puzzles.

the size of the community.

As a continuation of this research, classification of blockchain-based governance or e-voting solutions discussing potential implementations depending on the requirements of the community would be extremely useful.

3.4 Conclusion

New technologies make it possible to imagine new forms of governance, governments and decision-making processes. Currently, Blockchains and DLTs are the technologies receiving the most attention and dedicated research, resulting in many propositions for blockchain-based e-voting or constitutional reforms. None of the processes analyzed in the paper are absolutely dependent on blockchains or DLTs and it is possible that LD could be implemented on other technological platforms or that new forms of government derived from blockchains will emerge in the future. However academic and activist literature currently focuses on the topical issues of LD and BEV. While these proposals extensively discuss feasibility and technical implementation, analytical studies of the political consequences are quite rare. This paper contributes with an institutional economics analysis from a Public Choice's perspective.

I first focus on LD as a voting mechanism and find that it is likely to reduce decision-making costs, as less people need to agree, thus creating room for a more inclusive decision rule. However, it is uncertain whether the optimal ratio will actually increase. Moreover, LD naturally offers vote trading opportunities which favors a better representation of the intensity of preferences of the citizens. The paper then extends the analysis to a LD constitution where not only are vote conducted via LD but citizens also engage in legislative decision-making. I argue that LD as a political system does not offer, for now, solutions for vote-trading because delegation by themes and possibility to withdraw delegation at any time make it particularly difficult to engage in logrolling. Additionally, current propositions do not offer satisfying answers to the issue of conducting the legislative, commission and budgeting work that is done by parliaments in present day democracies.

Most of the limitations identified in the paper would not be prohibitive in small homogeneous communities required to govern, say, a public good such as a city. Blockchain-based governance for a community is best exemplified by Democracy Earth, whose goal is to propose a governance model to move "beyond the territorial boundaries of Nation-States" (*Democracy Earth* 2021, p.3) confirming that LD might not be suited for replacing current constitutions *per se* but could be efficient in other settings. Note that the example of the vote on national matters (the Peace Plebiscite in Colombia in 2016) mentioned in Cossar and Berman (2020), concerns a single vote isolated in time and does not capture the issues of vote-trading and intensity of preferences. As such, it cannot constitute a proof of concept for large scale Liquid Democracy. Blockchain-based governance for public good is also consistent with literature on blockchains and the governance of the Commons (Poux et al., 2020; Rozas, Tenorio-Fornés, Díaz-Molina, et al., 2018) which proves that it is appropriate for small to medium communities.

The contribution of this paper to the literature is twofold: firstly, it provides a theoretical institutional economic analysis of Liquid Democracy in terms of capacity to reflect the intensity of preferences. Although this issue has been mentioned in the state of the art literature, it had never been formally analyzed. Secondly, it builds on the existing distinction between LD as a voting tool and as a new form of democracy to disentangle classical arguments and highlights that some of the benefits of a voting mechanism could actually be counterproductive in a large scale constitutional setting.

In a context of increasing defiance towards representative democracies, with the rise of populism, and at a time where voters challenge more and more traditional parties, it is topical to develop this analysis further to other possible forms of democracy. In particular, this research only scrapped the idea of reconciling Liquid Democracy and parliaments and much work on that issue is required. How could moving away from the "one person-one vote" paradigm make it possible to better account for intensity of preferences, for instance via quadratic voting? Further research on the topic should include an extended discussion of blockchain-based voting tools, focusing specifically on the affordances of blockchains and their particularities. The possibilities are countless and blockchains offer a fascinating sandbox to design new governance models. Some are already relevant for the relatively small communities governing a public or common good but national governments raise other issues not yet adequately addressed by the proposals discussed in this paper.

Blockchains for the Governance of Common Goods

Following the conclusions of the previous chapter that indicate that Liquid Democracy may be more suited to small to medium communities this chapter turn such groups. Ostrom has demonstrated that a Commons approach was an efficient third way between large public institutions and private initiatives and we have seen that blockchains can provide services for group coordination. This chapter further explores blockchain-based governance and specifically the governance of common-pool resources, including natural ones. It builds on existing research and, points out the paradigmatic changes entailed by the recourse to a decentralized tool.

This chapter is shorter than the others because it was submitted as a conference paper. It was co-authored with Primavera de Filippi and Simona Ramos and was published as:

Poux, P., de Filippi, P. & Ramos, S. (2020). Blockchains for the Governance of Common Goods. *Proceedings of the 1st International Workshop on Distributed Infrastructure for Common Good*, 7-12

Abstract

This paper analyzes the use of blockchain technology to support the governance of common-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 common-pool resources.

Blockchains for the Governance of Common Goods

P. Poux, P. de Filippi & S. Ramos

4.1 Introduction

Although originally invented as the underlying infrastructure for the Bitcoin cryptocurrency (Nakamoto, 2008), 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 (Konashevych, 2017).

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 4.2), we introduce the traditional work of Ostrom on the governance of Common-Pool Resources (section 4.3) and subsequently analyze 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 4.4). 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 4.5), as well as the challenges inherent to blockchain technology more generally (section 4.6).

4.2 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 (Vujičić et al., 2018). 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" (Szabo, 1997) 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 (Werbach, 2017).

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 (Yaga et al., 2018). 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 and McMullen (2018), 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 infringing the original protocol rules (Reijers, Wuisman, et al., 2021).

4.3 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 (Hess and E. Ostrom, 2007).

Drawing on 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* (E. Ostrom, Gardner, et al., 1994) 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 "to understand the ways in which institutions operate and change over time" (Michael D. McGinnis, 2011). It focuses on an *action-situation* which is the "'black box' where policy choices are made" (Michael D. McGinnis, 2011). 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 (E. Ostrom, 1990) which could each contribute to a more sustainable management of CPRs (although none of them are not *stricto sensu*

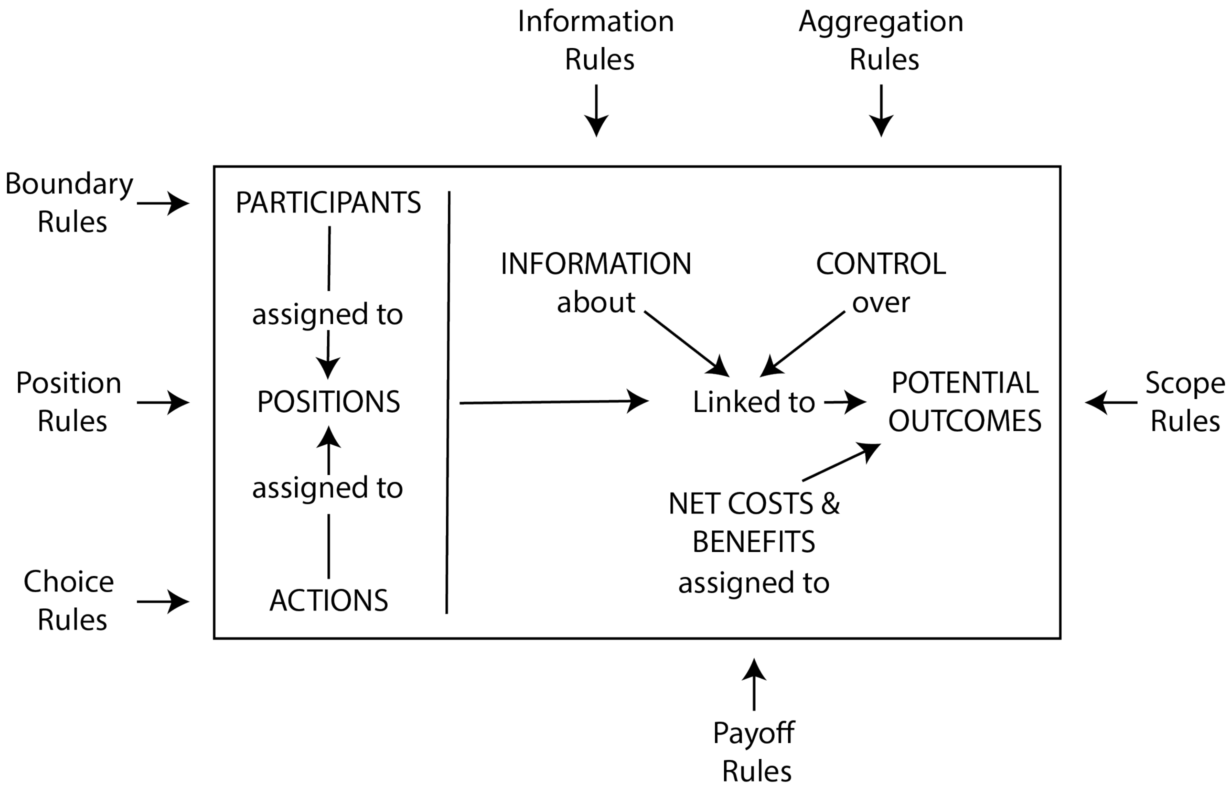

Figure 4.1: IAD and Rules: depiction of an *action-situation*

Source: Adapted from Figure 7.1 from E. Ostrom (2005, p.189)

necessary). The following list of principles has been refined by Cox et al. (2010) and endorsed by E. Ostrom (2010): **(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" (Crawford and E. Ostrom (1995)) 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 4.1. How blockchains can help implement particular configurations of these rules is discussed below.

Some authors have already been analyzing the potential of blockchain technology in light of this specific field of research. In particular, Rozas, Tenorio-Fornés, Díaz-Molina, et al. (2018) 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 and Potgieter (2019a) used the IAD framework to analyze 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. (2020) extensively discuss the dilemmas that could result from a relying on a blockchain governance tool for an 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 behaviors.

4.4 From a "Trust-Based" to a "Proof-Based" System

As previously discussed, E. Ostrom (2000) 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 (Rozas, Tenorio-Fornés, Díaz-Molina, et al., 2018). 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 (Hassan and De Filippi, 2017).

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 (Inoguchi, 2017). 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 analyzing 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 analyze 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 (Provenance, 2015). 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 commercialization cycle. A more advanced 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

[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.

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.

4.5 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" (De Filippi, Mannan, et al., 2020) 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

[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.

(Khaqqi et al., 2018), 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.

4.6 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 (Li et al., 2020). In addition to these technical challenges, blockchain technology also faces 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 (Michael D. McGinnis, 2011).

The interplay between these different rules is an essential component of any governance system. In particular, Rahman et al. (2017) 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 levels, 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 and Potgieter (2019b) 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 8 Ostrom 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) (Cox et al., 2010). Too big a discrepancy between the scales of the layers could cause the costs of relying on a blockchain exceeding 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.

4.7 Conclusion

Drawing on 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.

A Unified Framework for the Governance of the Commons with Blockchain-Based Tools

The concluding chapter of this dissertation builds on the previous ones to propose a unified evaluative framework to analyze and co-design blockchain-enabled Commons governance processes. It extends Ostrom's Institutional Analysis and Development Framework and outlines the new modalities that the governance rules may take thanks to decentralized, transparent automation. This chapter proposes a discussion of customary land Commons in Sub-Saharan Africa. The reader might be intrigued by this case study that is far from being blockchain-ready but it has been included as an indication of what this PhD might have been without COVID-19 and with more empirical work. It is presented in the version submitted that willbe submitted to the International Journal of the Commons after benefitting from the reviews of the jury.

Abstract

In this paper, we propose an evaluative framework to analyze Commons governance situations that use blockchain-based governance tools. Our research builds on a relatively recent field of literature linking the work of Elinor Ostrom and blockchain-based governance and unifies different strands to propose an all-encompassing framework. In particular, we focus on the constitutional level and how decision-making rules are made. We show that they are formal resemblance between blockchain-based systems and the Institutional and Development Framework build on these similarities to provide analytical tools to practitioners. We then illustrate this framework with a fictitious case-study of rural land Commons in Ghana.

A Unified Framework for the Governance of the Commons with Blockchain-Based Tools

An Application to Customary Land Commons in Ghana

P. Poux & S. Ramos

5.1 Introduction

Blockchain technology was used to create the decentralized cryptocurrency Bitcoin in 2009, but it soon became apparent that blockchains had more to offer than just monetary transactions. Not only do blockchains offer a solution to the double-spending problem (ensuring that a digital asset cannot be spent multiple times) but they also provide a secure platform for sharing data in a decentralized and relatively secure way. New avenues have opened up with the development of more complex blockchains (in particular Ethereum) that allow us to automate increasingly complex snippets of code, called smart-contracts, and to host decentralized Apps and services. Dubbed a "general-purpose technology" or a "new institutional technology", which could offer new forms of collaboration and coordination, blockchain has sparked interest across various sectors (Davidson et al., 2018).

In particular, communities have started using blockchains to decentralize decision-making and automate some governance processes. Complex distributed programs on the blockchain allow groups to automate decisions, condition certain actions to a set a predefined requirements, and assign different rights to actors depending on their status or on their past actions for instance.

While many of these blockchain-based decision-making tools serve to channel crowd-sourced investment, the array of applications is broadening. For instance, Troncoso and

Ultratel (2020) discuss blockchain-based platforms for cooperatives, while Decentraland offers a metaverse with a vast number of opportunities for groups to self-organize. Voting platforms are also being developed such as Aragon Voice. In all these examples, blockchains offer an opportunity to create new institutions for people to use.

Governance of the Commons has a long history of creating local institutions for the management of a Common-Pool Resource (CPR). In this context, there is a tremendous opportunity to make the best of what blockchains have to offer to enhance the governance of the Commons. Yet, practical examples of Commons relying on blockchain-based programs remain extremely rare and the tools to analyze and design them are still at a very early stage.

The institutional economics research field, dedicated in part to understanding how people set rules to govern their activities, has not yet grasped the potential of distributed technologies to modify institutional arrangements. Elinor Ostrom's work on the Commons 2011 has allowed scholars and practitioners to describe, analyze and understand a diverse set of Commons governance situations across the world. In her later work, Ostrom extended her analysis to digital Commons (Hess and E. Ostrom, 2007) however there is relatively little research focusing on how the introduction of new technology has modified governance processes for non-digital Commons.

In this paper, we demonstrate that there are many reasons to explore the links between the governance of CPRs and of blockchain-based governance. We propose an evaluative framework, focusing on the institutional and constitutional rules of the commoners communities, to analyze potential use cases. The goal is to identify the conditions where blockchain-based tools could help tackle governance challenges, empower local communities, or ease dispute resolution. To do so, the paper first provides a conceptual analysis and a theoretical framework for using blockchain-enabled tools for governing the Commons. Building on a relatively recent strand of research, we first adapt the classical literature of Elinor Ostrom and the Bloomington School on the governance of Common-Pool Resources to the use of blockchain-based tools. Strengthening existing bridges between these two worlds, we propose a unified framework that specifically addresses the issue of governing Commons that are based outside of the blockchain.

To illustrate our analysis and demonstrate how our evaluative framework can be used, we then propose a fictitious case study on customary land Commons in Ghana. In the Global South, most land is held under customary rights that are either not included or not well described in classical land registries that rely on private property. Traditional land rights in many areas in the Global South tend to consider the communal land as a whole, and see the community's relationship to it as spiritual. The community stewards their land and there are overlapping rights over land plots covering issues such as access to wells or farming rights, whether seasonal or permanent. Governance of this complex set of rights is delicate and builds on tradition, community history, and hierarchy (Alden Wily, 2008).

Customary rights systems often co-exist alongside legal systems inherited from colonial times and this results in a dichotomy and tensions between the *numerus clausus* of the latter and the bundle of rights of the former. Moreover, within these two frameworks there is a discrepancy between *de jure* rules and *de facto* habits. Scholars and practitioners in the field have identified the issues of arbitration and jurisdiction as central in resolving disputes over land rights. These disputes are increasingly frequent due to several factors. First, demographic growth is increasing the pressure on land, which has been worsening in some areas with the accelerating desertification due to climate change. Second, a large-scale global land rush threatens fallow lands and plots with overlapping rights. Lastly, disputes are frequent within communities and even withing families when a rapidly evolving social context clashes with traditional practice. The availability of competing jurisdictions with different legal bases makes it difficult to predict the outcome of arbitration, thus weakening the security of tenure.

Having a reliable, transparent registry based on Commons governance could alleviate these problems according to Alden Wily (2012). It is to that purpose that we propose and analyze a blockchain-based tool. Our aim is not to replace existing governance mechanisms but rather to supplement the tools at the disposal of communities in order to advance their agency.

The remainder of the paper is structured as follow: section 5.2 presents different strands of research upon which our framework is built. In particular, we discuss the Institutional Analysis and Development Framework, developed by Ostrom, before discussing the state of the art research on blockchain-based governance of the Commons. Subsection 5.3.2 introduces our evaluative framework. Finally, section 5.4 contextualizes our case study and applies the framework.

5.2 Literature Review

As this article builds on many different fields, we include here a wide-ranging literature review to help readers navigate the different theories referred to in the paper.

5.2.1 Blockchain Technology

Blockchain represents a decentralized and distributed ledger technology that records transactions between parties in a verifiable and immutable way by storing them in a sequence of blocks. Blockchain technology became widely known in 2008, after the release of Satoshi Nakamoto's white paper establishing Bitcoin as the first blockchain-based cryptocurrency (Nakamoto, 2008). However, proofs on decentralized ledgers had existed in the literature prior to 2008.[1] With the initial goal of providing an alternative monetary system after the 2008 financial crisis, Nakamoto's white paper positioned the idea of recording transactions in a verifiable, permanent and trusted manner, without the need for a central authority/intermediary. Combining elements from cryptography (to resolve the double-spending problem) and from game theory (for the Byzantine General's Problem), Nakamoto's white paper proposed a solution based on a PoW (Proof of Work) mechanism. PoW forms part of the probabilistic-finality consensus mechanism category as it guarantees eventual consistency in nominal conditions. In essence, PoW operates as a lottery mechanism where a node that solves a computationally-intensive random search operation in the form of a cryptographic puzzle is allowed to create a new block and gets rewarded for it.[2] This process is known as mining. The consensus mechanism is crucial for the survival of the system, as it guarantees trust and security.

Blockchains based systems have been dubbed "trustless systems" (Werbach, 2018) because they do not require users to trust any other party. However, recent research by De Filippi, Mannan, et al. (2020), building on the work of Luhmann (2000), has demonstrated that, while blockchains act as "confidence machines", they still involve trusting many actors such as programmers, miners and the overall ecosystem. They do not cancel the need for collaboration and a form of trust. What they do provide are reliable records and automation for transparent processes that may facilitate coordination between distrusting agents. Blockchains are considered immutable although, in reality, they can evolve to better meet the requirements of their users. The extent to which they can evolve depends on the blockchains but the change process goes through both *on-chain* and *off-chain* governance mechanisms. As a blockchain is a protocol over which users agree, it is possible to change this protocol, for instance to change an on-chain rule (e.g. the size of the blocks). The change of the protocol must be coded online and then implemented by all the participants (or at least a large enough majority). How the code evolves is called *on-chain* governance. The discussion on the evolution and strategic decisions concerning the blockchain often involves long discussions and planning outside of the blockchain. Active members of blockchains often meet and use forums and blogs to advocate strategies and new types of decentralization mechanisms. When the community of users of one blockchain cannot agree on a strategic decision, they can decide to split and enforce incompatible versions of the code. Such a split is called a *hard fork*. Community splits can sometimes cause a reduction in both overall security and decentralization of the system.

In general, the main characteristics of a public blockchain are:

Immutability: Once added the chain, the data is permanently accessible and not modifiable

[1] Nakamoto acknowledges derivation from the HashCash scheme introduced in 1997 by Adam Back. Cryptographer David Chaum dissertation proposed a blockchain-like protocol 1982. Further work on a cryptographically secured chain of blocks was described in 1991 by Stuart Haber and Scott Stornetta.

[2] Different concensus mechanisms exist although POW has been the one most widely deployed.

Decentralized: All the participating nodes contain a copy of the ledger. Some participants may decide not to host the full dataset but the data is available to everyone

Consensus driven: A fault-tolerant mechanism is used in blockchains to achieve trust and necessary agreement on a single data value.

Transparency: The whole chain of blocks, along with transactions recorded, are public and freely verifiable by everyone.

Cross-Border Nature: In public blockchains, the system is open to everyone to participate.

The anonymous/pseudonymous nature of network participants: In general, network participants' identity is not disclosed.

5.2.1.1 Smart-contracts and DAOs

The development, and adoption of blockchains increased with the introduction of smart-contracts. Although the term smart-contracts was coined in 1994 by Nick Szabo, its "merge" with the blockchain technology via the Ethereum blockchain in 2013 brought a whole new spectrum of applications and possibilities. Ethereum's implementation of a virtual machine allowed for snippets of codes (smart-contracts) to be executed in a decentralized way without third party interference. A smart-contract is a computerized transaction protocol that executes the terms of a *contract*. The general objectives of smart-contract design are to satisfy common contractual conditions without the need of an intermediary. In other words, it is an automated and immutable (once deployed) piece of code that represents the terms of an agreement between different parties. The obligations are enforced via the consensus process when the parties deploy the contract. Smart-contracts can be combined into complex programs for different purposes. A decentralized application (dApp) is an application built on a decentralized network that combines a smart-contracts and a front-end user interface. Often, the operation and execution of dApps is enabled through oracles. Oracles are data feeds that connect the on-chain system to the off-chain world. In other words, real-world information may sometimes be needed to query data in the smart-contracts. For example, prediction market dApps use oracles to settle payments based on events. Oracles thus introduce information from an external, trusted party into a decentralized system, reintroducing dependence on centralized actors. Oracles are necessary as soon as the scope of blockchain-based activities expands to include diverse services but constitutes a door to the off-chain that is essential to bear in mind. As blockchains are garbage-in/garbage-out technologies, if the oracle provides flawed information, the information will remain flawed forever on the blockchain.

Smart-contracts can also be combined into complex programs called DAOs (Decentralized Autonomous Organizations). DAOs are autonomous organizations, collectively owned and managed by their members, where decisions are made via proposals that the group votes on during a specified period. Compared with traditional centralized organizations, the structure of a DAO is usually flat and fully democratized, with voting required by members for any changes to be implemented. The governance rules of the DAOs are written within the code which cannot be altered after deployment. Human intervention is only possible inasmuch as it has been planned by the programmers. Many DAOs are used to govern assets or manage (investment) funds. DAOs have built-in treasuries, the use of which, stakeholders can vote on. DAOs can also serve as voting platforms, with the decisions either automatically enforced (if doable) or recorded permanently on the DAO. Usually, governance rights are conditional on holding tokens of the DAO. Tokens are digital assets that give a set of rights for a specific use. They are conceptually equivalent to a coin of cryptocurrency but can only be used/spent on a given use. They can sometimes be exchanged for other tokens/cryptocurrency that, in themselves, do not give governance rights over DAOs. Tokens and DAOs are the two pillars of the coordination processes on blockchains. They provide a form of confidence for users who can engage in participation in the governance process with the certainty that everything coded will necessarily happen. In other words, DAOs help solve the principal-agent dilemma through community governance. Agents do not need to trust each other, but rather work as part of a group whose incentives are aligned.

5.2.2 Governance of the Commons

The Commons are traditionally defined as rivalrous but non-excludable goods (Samuelson, 1954). Hardin (1968) mistakenly interpreted "Common Goods" as "Open Access Rivalrous Goods", and theorized that the Commons were condemned to over-consumption thereby calling to privatize them or make them public. However, it was not long before Elinor Ostrom (E. Ostrom, Gardner, et al., 1994) proposed a more dynamic and modern definition of the Commons, later refined by Bollier (2002): a Commons is characterized by a resource, a community and a set of rules presiding over the governance of the resource. Being a Commons[3] is thus an attribute of the community as much as of the resource and emphasizes the importance of governance rules that prevent over-exploitation and guarantees sustainability.

Elinor Ostrom, Nobel Prize in Economics in 2009, founded the field of study devoted to analyzing the governance of the Commons. She proposed a theoretical, experimental and empirical explanation of how the Commons were sustainable globally (E. Ostrom, 1990). With the Bloomington School she continued developing a framework for the understanding of group behavior in the context of Common-Pool Resources (CPR). This resulted in the Institutional Analysis and Development Framework (IAD).

Figure 5.1 provides analytical tools to describe how the Commons (the action situation) works and interacts with the other components of the framework. The IAD identifies how

[3]See Bollier (2002) for a discussion of the letter *s* at the end of the word Commons.

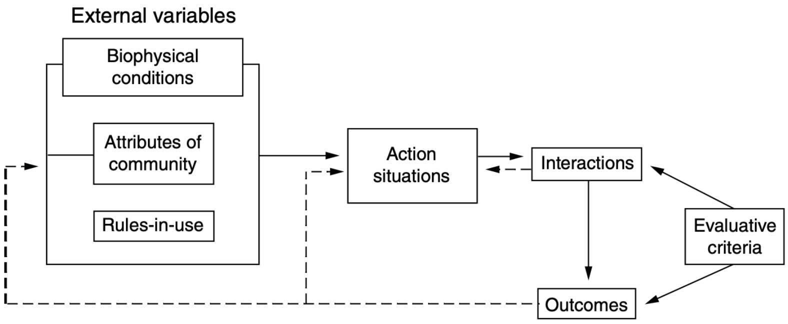

Figure 5.1: A Framework for Institutional Analysis

Source: E. Ostrom (2010, p. 646)

seven types of rules are implemented. These rules concern, the resource, the community and the norms used to govern the CPR. These types of rules are described in Figure 5.2. The Bloomington School looked at hundreds of case studies and identified different modes of implementation for the seven types of rule (E. Ostrom, 2005, ch. 8). This underlined the diversity of situations falling under the classification CPR. For instance, E. Ostrom (1999) identified 27 forms of boundary rules and 112 choice rules. In particular, Schlager and E. Ostrom (1992) showed how the position and choice rules defined a bundle of rights which describes a continuum of rights rather than predefined fixed rights. The bundle of rights ranges from access right to alienation through withdrawal, management and exclusion.

The IAD thus provides analysts with a grammar and tools to adequately understand, describe and access Commons governance. Using this framework and through hundreds of case studies, E. Ostrom (1990) identified eight design principles associated with success in the management of CPRs. The following version has been reassessed and refined by Cox et al. (2010) and endorsed by E. Ostrom (2010):

DP1a User Boundaries: Clear and locally understood boundaries between legitimate users and nonusers are present.

DP1b Resource Boundaries: Clear boundaries that separate a specific common-pool resource from a larger social-ecological system are present.

DP2a Congruence with local Conditions: Appropriation rules are congruent with local social and environmental conditions

DP2b Appropriation and Provision: Appropriation rules are congruent with provision rules; the distribution of costs is proportional to the distribution of benefits

DP3 Collective Choice Arrangement: Most individuals affected by a resource regime

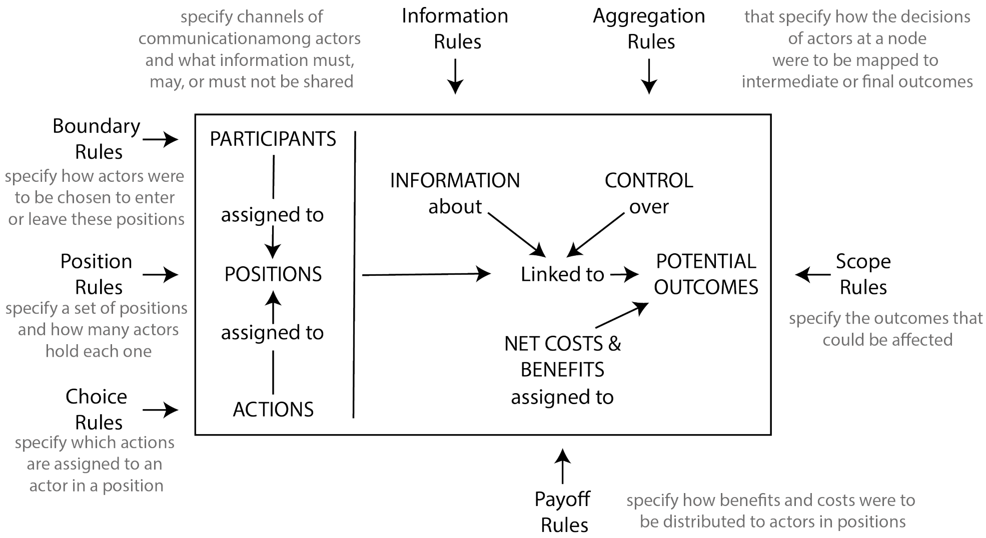

Figure 5.2: IAD, Its Rules and Components

Source: E. Ostrom (2010, p. 651-52)

are authorized to participate in making and modifying its rules.

DP4a Monitoring Users: Individuals who are accountable to or are the users monitor the appropriation and provision levels of the users

DP4b Monitoring Users: Individuals who are accountable to or are the users monitor the condition of the resource.

DP5 Gradual Sanctions: Sanctions for rule violations start very low but become tougher if a user repeatedly violates a rule.

DP6 Conflict Resolution Mechanisms: Rapid, low cost, local arenas exist for resolving conflicts among users or with officials.

DP7 Minimal Recognition of Rights: The rights of local users to make their own rules are recognized by the government

DP8 Nested Enterprise: When a common-pool resource is closely connected to a larger social-ecological system, governance activities are organized in multiple nested layers.

Similarly to the rest of the IAD, these principles are not prescriptive but provide a useful list of features for understanding success or failure in the sustainable governance of a CPR. In situations where sustainable governance is not achieved, identifying how the seven types of rules are enforced and then checking against the eight design principles is a powerful way to identify shortcomings in existing processes and action levers.

Although the earlier work presented here has mostly addressed natural resources, it has been adapted to informational Commons (Fuster Morell, 2014; Hess and E. Ostrom, 2007) such as Free/Libre Open Source Softwares (FLOSS) or peer-produced datasets such as Wikipedia. While the challenges faced by the community differ (over-exploitation for natural resources against non-contribution), they share many features (Fonseca et al., 2018; Potts, 2018)

5.2.3 Blockchains, Governance and Blockchain-Based Governance

Blockchains are ledgers shared by all participants who adopt its code and protocols. As blockchains are intrinsically horizontal systems where all nodes that participate in the block validation process can decide on the evolution of the protocol, blockchains could be considered as Knowledge Commons such as described by Hess and E. Ostrom (2007). However, while advocated by Bodon et al. (2019), this stance is challenged by Howell and Potgieter (2019a). Indeed, they show that the blockchain community can also be hierarchical with founders and first-comers being extremely influential and retaining *de facto*. However, they still conclude that blockchains can be governed as Commons as long as sufficient governance mechanisms are implemented both on and off-chain. Blockchains are also being discussed in the literature as governance tools. In that case we talk of *blockchain-based governance* instead of governance of the blockchains. Research to understand how to best use blockchains for the governance of Commons is quite new and only a few papers have really addressed the issue. Rozas, Tenorio-Fornés, Díaz-Molina, et al. (2018) study a specific type of Commons, namely Community-Based Peer Production Communities with the example of a community sharing the infrastructure for internet access across space. They do not apply the IAD framework but do describe the governance processes of the community. Relying on Hutchby's definition of affordances as "functional and relational aspects which frame, while not determining, the possibilities for agentic action in relation to an object" (2001), they discuss whether blockchain-based governance could offer new affordances for the governance of CPR. They identify six affordances: tokenization, self-enforcement, autonomous automatization, decentralization, transparentization and codification of trust. The authors then assess each of these affordances against the eight design principles to see how blockchain-based governance can help meet these criteria for governing CPR. The result is presented in Table 5.1. This paper provides a valuable first step in the analysis of blockchain-based governance. The authors then extended their work in Rozas, Tenorio-Fornés, and Hassan (2021) which focuses on global digital non-rival Commons. They study various examples and apply the previously mentioned analytical framework to conclude that blockchains could be particularly useful for scaling up and monitoring and tracking while also valuing invisible work.

However, their work focuses on the Design Principles which are useful for analyzing

	Tokenization	Self-enforcement and formalization	Autonomous automatization	Decentralization of power over infrastructure	Transparentization	Codification of trust
Clearly defined community boundaries	✓					
Congruence between rules and local conditions	✓	✓		✓		
Collective choice arrangements	✓			✓		
Monitoring		✓	✓	✓	✓	
Graduated sanctions		✓	✓			
Conflict resolution mechanisms			✓		✓	
Local enforcement of rules		✓		✓		✓
Multiple layers of nested enterprises			✓			✓

Table 5.1: Blockchain-Based Governance Affordances

Source: Rozas, Tenorio-Fornés, Díaz-Molina, et al. (2018), p.22

a Commons *ex-post* but they do not allow us to understand constitutional arrangements. It is the set of rules, anchored in a constitutional and meta-constitutional context, that determines whether the Design Principles are me. These rules serve more as a check list than as an explanatory analytical tool. It is therefore important to further this work to provide analysts and practitioners with more actionable tools.

In complement to this work, Cila et al. (2020) explored the challenges and trade-offs faced by communities using blockchain-based governance tools. Through the example of a "fictional energy community", they identify design dilemmas that communities must solve. The six dilemmas identified fall within three categories: tracking, managing, and negotiating. They are presented in Table 5.2. Many of them emerge because blockchains are coded with a formal complete language while situations in real life might be more nuanced or unexpected events may happen. Formalization and codification of the universe over the code of a DAO may help control, plan for and even prevent conflicts for arising but they may also alter some of the essential social features of the community. The trade-off to achieve depends on the nature of the Commons studied but these dilemmas constitute important *caveats* to take into consideration while designing governance frameworks for CPR.

Lastly, Poux et al. (2020) focus on the grammar of the IAD framework in the context of blockchain-based governance. They show that there are ways of implementing the seven types of rules on a blockchain using a DAO. Depending on the type of the resource (natural or digital), the implementation can be total or partial. In particular, the authors show that relying on blockchain-based governance entails a change of paradigm from monitoring and sanctioning (see design principles 4 and 5) to *ex-ante* automation and *ex-post* verification. They argue that the system thus shifts from a "trust-based system to a proof-based system". The paper shows that it is possible to rely on the grammar and the structure of the IAD to establish governance rules that match most of the design principles and are influenced by the conclusions of the numerous cases studied by the Bloomington School. The discussed above articles pave the way for further research on blockchain-based governance of the Commons each addressing different aspects. Their work can be extended as to understand how blockchains may affect and help govern CPRs.

Mechanism	Design Dilemmas	Definition
Tracking	Transparency vs Privacy (T vs P)	Transparency is an important feature of blockchains that can prevent free-riding but may threaten privacy
Managing	Economic Value vs Social Value (E vs S)	Tokenization transforms social value into economic value and that may weaken the social bond
	Quantified vs Qualified Values (Q vs Q)	Blockchains and IT encodes better things that can be quantified and may alter things that cannot, forcing certain measures or standards
	Incentivization vs Manipulation (I vs M)	How to best use incentives that are both economics (on the blockchain) and social (for the Commons)
	Private vs Collective Interests (P vs CI)	In the case of competing interest, how to decide between private individual interest and the collective interest of the community while avoiding free-riding
Negotiating	Human vs Algorithmic Governance (H vs A)	What equilibrium between on and off chain governance? What checks and balances?

Table 5.2: Dilemmas when using blockchains for the governance of Commons

Source: Cila et al. (2020)

5.3 An Evaluative Framework for Blockchain-Based Governance of Common-Pool Resources

5.3.1 Framework Applicability

As described in subsection 5.2.3, there are theoretical reasons to think that blockchain-based tools can contribute to the governance of CPRs. In this section, we extend the work of Poux et al. (2020) and link it with the other papers reviewed to articulate the different aspects addressed by Cila et al. (2020) and Rozas, Tenorio-Fornés, Díaz-Molina, et al. (2018). Before dealing with the governance rules, we must consider the broader context as depicted in Figure 5.1. Key elements of the IAD include not only the action situation (the Commons) but also external variables, outcomes and feedback processes. We must ponder whether relying on blockchains only modifies the governance processes within the action situation or if other elements of the framework are also modified. Once more, the answer depends on the CPR studied. If the CPR is already digital, even more so if it exists on a blockchain, the biophysical conditions include the code and the data set of the CPR and it may not be changed by the introduction of a Distributed Ledger Technology (DLT). However, when the CPR is natural resource, introducing digital tools can modify the context. This echoes the "managing mechanism dilemmas" (Cila et al., 2020): when digitalizing data, the values and trade-offs may be modified.

Finally, before diving further into the governance rules of the Commons (the action situation), the feedback mechanisms between the outcomes and the external variables may also be affected by automation or by the need to encode data in the blockchain to record off-chain results. These aspects of the IAD had not been discussed clearly in the literature but are essential. Indeed, being oblivious to the wider context could bring unexpected difficulties and failures even if the rules have been carefully thought through. In light of these dilemmas, we present an overall technical framework in which we describe the setting and try to give possible responses to the questions above. In Figure 5.3 we present an overview of the technical layers involved in the execution and operation of blockchains and blockchain-based applications.

In brief, an implementation of a blockchain system (and supporting applications) involves incorporation of a diverse set of layers. A complex ecosystem composed of DAOs which are governed by diverse agents at different layers may involve a more in-depth analysis as to how to design the system. For example, the network layer takes care of discovery, transactions, and block propagation, while the protocol layer is responsible for validating and ordering the blocks the blocks and ensuring everyone agrees on the chain. The application layer is comprised of the smart-contracts, code and dApps that are used by end users to interact with the blockchain network. For an application to be considered a dApp, there are certain rules it must follow (use a cryptographic token, generate tokens according to a standard cryptographic algorithm, be open-source, operate

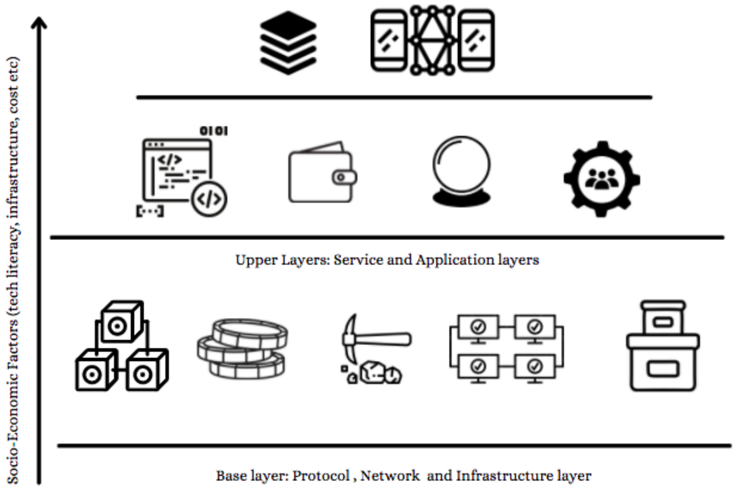

Figure 5.3: Infrastructural Layers: Framework Applicability

autonomously, and have no entity controlling the majority of its tokens, etc.) In other words, the more sophisticated the management of a CPR becomes the more complex the design and implementation is. When it comes to transposing the governance of CPR onto a blockchain, other technologies may also be needed such as IoT (the Internet of Things) or AI (Artificial Intelligence). The implementation of layers as well as other accompanying technologies may demand a higher level of tech literacy and base infrastructure and may imply higher costs of implementation.

5.3.2 The Evaluative Framework

In this section, we review the modalities and rules of the framework and examine their implementation in a blockchain based system. Following Ostrom's grammar we find that:

Boundary Rules: Codification on a blockchain can only come after boundary rules have been determined by the community. In the context of a CPR, this can imply membership to a community (e.g. fishery), living in a specific area, or any other connection that may describe the relationship between the agent and the natural resources. The conditions are numerous but, depending on the CPR, relying on a DAO may not fully substitute for off-chain boundary rules. Nonetheless, once the boundary rule is agreed upon by the community, it can be encoded. It that case, using DAOs does not *per se* add a modality of boundary rule but automates its enforcement. Encoding off-chain boundary rules necessitates identifying community members on the blockchain which raises issues of privacy. One notable exception is when the Commons itself is a DAO. In that case, boundary rules can depend on on-chain criteria and thus be fully dependent on the blockchain and anonymity can be maintained. Similarly, it is possible to implement contribution-based boundary rules without the opportunity for cheating or the need for control can be implemented. Blockchain also allows boundary rule implementation to be perfectly transparent hence providing confidence in the method used to affect positions. Relating to the affordances, boundary rules can be implemented thanks to automatization (although autonomy is not required for this type of rule) and transparentization.

Position Rules: The position rules define the positions that agents can have within a given system. Similarly to the boundary rule, off-chain position rules can precede the implementation of real-world position rules. Positions can also be specified directly on the blockchain. Positions on the DAO can complement positions in real life or mirror them. When roles are subject to voting processes, voting can be done directly on the blockchain, making it easy to record the evolution of the roles on the blockchains. Although security is an important feature of blockchains, examples of mischief or errors in the code of DAOs have shown that it is important to include mechanisms to amend decisions if necessary. This precaution must be taken *ex-ante* so that on-chain governance is at the service of the CPR and does not threaten the enforcement of off-chain governance. This can be done through the affordances of tokenization, autonomous automatization and transparentization.

Choice Rules: Choice rules specify which actions are assigned to an actor in a position. It is doable to assign a set of possible actions to positions on a DAO. For instance, it can be encoded that everyone can make proposals but only a set of elected representatives can decide when to vote or that a set of arbitrators are in charge of solving conflicts. As soon as position rules are encoded, choice rules derive quite naturally. In particular, because of the formal nature of the code used to define actions, the universe of possible actions that a certain position can undertake is preset and constrained *ex-ante*. Once more, this raises the issue of how to link the blockchain world with the off-chain processes. As long as the CPR can be algorithmically governed, the encoding of the position can be complete over the DAO. Otherwise, transposing the position rule defined off-chain onto the blockchain necessitates determining the scope of actions delegated over the blockchain and the role of the oracles. And the issue goes both ways: if there are fields where actions taken on the blockchain may not be automatically reflected in real life, mechanisms to ensure concordance must be developed. Implementation of choice rules rely on the affordances of tokenization, self-enforcement and formalization, autonomous automatization and transparentization. Indeed, positions are linked to tokens that give further rights. Conditional rights rely on tokens. Automation is used to automate decision processes as discussed for the position rule. Finally, formalization and self-enforcement go hand-in-hand with the two previous affordances. This illustrates the *ex-ante* automation change in paradigm.

Information Rules: Information rule is probably the one rule that will be the hardest to delegate on the blockchain. As we have mentioned in subsection 2.1, most of the governance of blockchains happens off-chain. In the case of a natural Commons, the information has to be recorded on the blockchain and the DAO cannot restrict further access to this information. Indeed, if a member of the community has access to information regarding the Commons in real life, restrictions on the blockchains will have no effects whatsoever. In such cases, recourse to blockchain technology does not create new modalities of information rules and does not appear well suited to the implementation of the information rules that must rely on other mechanisms. Nonetheless, if the sort of information rule decided collectively implies making some information available to all members, the transparency and reliability features of blockchains can be valuable. In the case of blockchain-based CPR, some information can be limited. For instance, it is possible to limit access to some documents or information to some positions, while other members can only see the document hash. In these cases, new forms of conditional information rules could be devised to mirror requirements of the digital Commons. In these cases, the affordance concerned is mostly transparentization.

Aggregation Rules: Aggregation rules concern both the mechanisms concerning the enforcement of actions and the decision-making rules (such as majority or unanimity). As mentioned above, DAOs are very well suited to implementing voting platforms. For instance, they could facilitate consultation in a type of rule where concerned actors would be notified and consulted every time a decision has to be made. Actors could also decide the type of decisions they would like to be notified of. There is burgeoning research on decision-making processes over blockchains that propose innovative solutions. For instance, we can mention the *Holographic consensus* used for DAOstack (El Faqir et al., 2020) that helps prioritize proposals on a DAO.[4] Regarding the enforcement of decisions, DAOs can also help automate this. In particular, recourse to smart-contracts, conditioning and certainty of automation makes it possible to design complex rules that have guaranteed execution that does not depend on any actor, thus increasing confidence in the outcomes. We posit that aggregation rules are the type of rule that could most benefit from blockchain-based governance tools, not only in the case of digital Commons but also in the case of natural resources. These new forms of aggregation rules would rely on the self-enforcement and formalization, autonomous automatization and codification of trust.

Scope Rules: are used to characterize the outcomes. E. Ostrom (1999) specifies that "Scope rules are used to limit harvesting activities in some regions that are being treated as refugia. If no appropriation from these locations is allowed, the regenerative capacity of a system can be enhanced" (p.518). In the case of natural CPR,

[4]The holographic consensus is a method for scaling up decision-making in large communities in a way that delegates decision to small groups but ensures alignement with the majority.

scope rules will not benefit from blockchain-based affordances *per se*. However, transparency might be used to record decisions concerning scope rules and to provide an archive of the CPR history. As expected, DAOs are more suited to encoding scope rules in the case of blockchain-based or other digital DAOs, where scope could be algorithmically restricted, benefitting from *ex-ante automation*. In that case, the affordances concerned are transparentization, self-enforcement and automatization.

Payoff Rules: Implementing a payoff rule over a DAO requires assigning value to tokens used in the DAO. This is easily doable through blockchain-based valuation of the tokens (via swap markets) or through valuation of a local currency for instance. For the sake of sustainability, stability should be sought after. Note that the value tokens used for payoff rules (that concern both benefits and sanctions) can (and should) be different from those related to position or choice rules and we do not believe there should be a market between the two in order to avoid plutocracy and prevent the governance tokens to be used as securities. Once these precautions have been taken, complex payoff rules can be implemented. Smart-contracts have been developed precisely to allow conditional transactions to take place on a blockchain. In particular, one could imagine payoff rules that include reinvesting a part of the benefits in the CPR, benefits conditional to future revenues or behavior in order to deter free-riding. Along with aggregation rules, payoff rules are those that can benefit most from the affordances of blockchains. In particular, self-enforcement, automatization and transparentization on top of tokenization.

Therefore, for the affordances that determine the *action-situation* rules are those that relate to execution of code on the blockchain (tokenization, self-enforcement and formalization, autonomous automatization and transparentization). The two others, namely decentralization of power over infrastructure and codification of trust, pertain to another kind of affordances: they concern the external environment. We mentioned that recourse to blockchains modify the external variables; this is true of other ICT solutions but the two latter affordances modify the external variables in a way that is consistent with traditional governance of the Commons. From Table 5.1 we see that they are relevant for the local enforcement of rules (DP7), the multiple layers of nested enterprises (DP8), the congruence between rules and local conditions (DP2), the collective choice arrangement (DP3) and monitoring (DP4). This design principles are all consequences of how the seven types of rules are applied. Therefore, we can refine the analysis of how and why to rely on blockchain-based. This group of four affordances make it possible to propose new modalities for the grammar of the IAD and the two other affordances explain why these new types of rules may be adequate for the governance of Commons because they meet the design principles.

Extending the work of Rozas, Tenorio-Fornés, Díaz-Molina, et al. (2018) to all types of Commons, we thus highlight that some types of rules are better suited to blockchain-based implementation in the general situation. In particular, we note that information rules and scope rules can only be recorded but not necessarily enforced over a blockchain-based tool and still necessitate an off-chain implementation. This underlines the necessity for integrating on-chain and off-chain governance processes as noted in Poux et al. (2020, p.11) on choice levels. The affordances of autonomous automatization and self-enforcement make blockchains adequate for the operational level (which is the day-to-day procedures level). However, off-chain processes are still required, in particular for meta-levels for governance of rule-settings. The choice levels of CPR governance and the governance mechanisms of the blockchain are entangled and described in Figure 5.4. Successful governance mechanisms depend on an intricate and dynamic relationship between the different levels with necessary feedbacks. We extend the work of Cole (2014) which illustrates how the governance process of a Commons respects choice levels where operational rules are decided by policy level and how rules at operational level may evolve and adapt. All of this takes place within a larger constitutional set of rules which depends on the social context. Delegating rules over a DAO for day-to-day actions implies abiding by the rules of the DAO for amendment, evolution and arbitration. The DAO itself is dependent on the rules-in-use of the blockchain. The blockchain-based tool should be at the service of the community, thus the left-bound red arrows on the figure. Poux et al. (2020) underline that for DP3 and DP8 to hold, the CPR community should be able to participate in the governance of the blockchain. Therefore, the policy level informs the DAO governance rules and ensures that the future evolution of the governance process is encoded on the DAO while the constitutional level verifies the adequacy between the community values and the blockchain used.

The article about design dilemmas (Cila et al., 2020) does not directly fit into the IAD framework. However, these design dilemmas raise awareness of the processes at play when using the affordances for the implementation of rules. For instance, boundary and position rules imply digitalizing identities. Although self-sovereign identities are possible over a blockchain and they can preserve a form of privacy without revealing too much information, there is a trade-off between transparency and privacy. Scope rules raise the issue of human vs algorithmic governance and extends the issue of the scope of the CPR (as depicted on the Figure 5.4). Cross-checking the affordances of blockchains against the rules as done in the list above we can see when and where the dilemmas may be an issue. Of course, they might not all happen in all cases but we identify the situations in which they are the most likely to take place. In Table 5.3 we summarize the results. Dilemmas in the context of *managing* are particularly frequent, in particular with the related questions of economic and social values and of quantifying qualified values. These dilemmas touch on almost all the rules, although in different manners. Clearly, all the dilemmas are intertwined and setting for a trade-off in one of the boxes will condition the trade-offs in the others. Unsurprisingly, the affordance of decentralization of power over infrastructure does not match any of the dilemmas because it does not concern the operational level. Although Cila et al. do not specify it, their design dilemmas mostly concern the operational level with the exception of private interests vs collective interests which may, in some cases, relate to

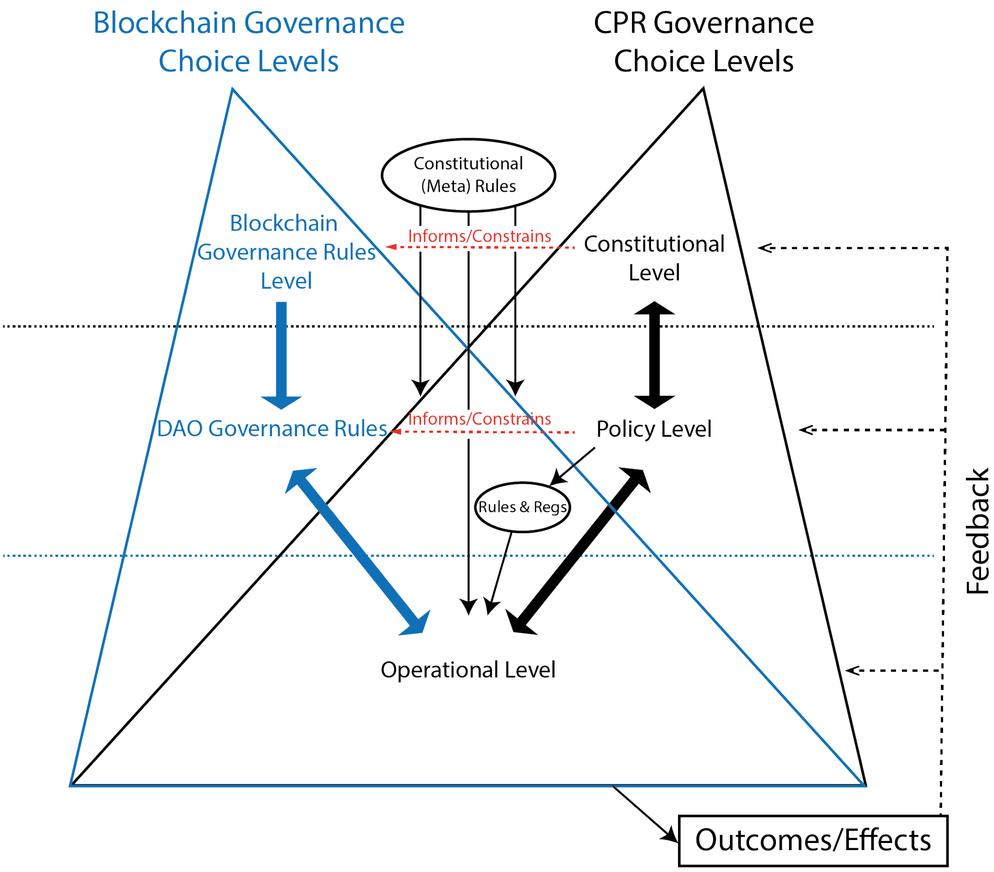

Figure 5.4: Entanglement of Choice Levels for Blockchain Enabled CPR Governance

Source: Right-hand side (in black) adapted from Cole (2014, p.6)

	Tokenization	Self-enforcement and formalization	Autonomous automatization	Decentralization of power over infrastructure	Transparentization	Codification of trust
Boundary Rules					T vs P	
Position Rules	H vs A Q vs Q		H vs A Q vs Q		T vs P	
Choice Rules	H vs A Q vs Q E vs S	H vs A Q vs Q E vs S	H vs A Q vs Q E vs S			
Information Rules					Q vs Q	
Aggregation Rules		I vs M P vs I	I vs M P vs I			E vs S Q vs Q
Scope Rules		H vs A Q vs Q	H vs A Q vs Q		H vs A	
Payoff Rules	E vs S	E vs S Q vs Q I vs M P vs I	E vs S Q vs Q I vs M P vs I		T vs P	

Table 5.3: Design Dilemmas When Using Blockchain Affordances for the Implementation of CPR Governance Rules

the policy level. Similarly, we note that the codification of trust affordance pertains more to the policy level and therefore it is only mentioned once in the Table 5.3. However, the general issue of relying on blockchain-based tools through the codification of trust appeals to the dilemmas of quantification of values and of economics vs social values.

In this section, we have expanded on three strands of research dedicated to analyzing how the Commons could benefit from the decentralized revolution of the blockchains. Recourse to blockchains for the operational level implies a paradigm shift and new ways of implementing the seven types of rules identified to describe an action situation in the IAD. Blockchain-based tools are relevant because they offer affordances. We have presented how these affordances offer new modalities for the rules while keeping in mind the design dilemmas that can emerge when using DLTs. To date, most studies of blockchain-based governance have focused on the day-to-day operations. We have looked at the issue in a broader context and take into account the entanglement of choice levels that are affected by the change of paradigm. The remainder of the paper proposes an application of this framework to a theoretical case study.

5.3.3 Conditions for Application

This evaluative framework can only be applied under certain conditions. Indeed, it assumes that the Commons uses a blockchain-based tool which relies on hypotheses regarding the three components of the Commons: the community, the resource, and the rules. The previous sections discuss the rules extensively, but it is important to also keep in mind the hypotheses regarding the community and the resource.

First, the community must be able to use a complex digital tool. This premise is clearly the most critical one. Access to the tool must be widespread and this is based on two conditions: material and abilities. The former means that most, if not all, commoners should readily have access to a device that allows them to use the blockchain-based tool. This informs design specifications for the software as it is easier to have access to a smartphone app than to a complex computer-based interface. The second condition relates to tech-literacy. Using a blockchain-based tool, even with a very simple UX, requires a certain level of digital literacy. Initiatives in this area are flourishing. For instance, there has been the development of a *no-code* market initiative. *No-code* smart-contracts initiatives aim at assisting nontechnical users in creating and interacting with smart-contracts in their natural language. A prose-based template for smart-contracts, Openlaw, gives the possibility for users to complete a prose-based template and consequently generate contracts transposed to a smart-contracts code on the Ethereum blockchain[5].

Nonetheless, the Digital Divide is a worldwide phenomenon and it often maps socio-economic inequalities (Fuchs and Horak, 2008; Rogers, 2001). Therefore, particular attention should be devoted to whether the recourse to a blockchain-based tool reinforces structural power relationships. The analysis of position and choice rules should explicitly take this issue into consideration in the evaluation and the analysis.

Second, the other aspects of the Commons concern the resource. We have already touched upon the link between the resource and its digital counterpart: data describing the state of the resource, harvest etc. is key in the governance process. This underlines the importance of the oracles and how to validate the data recorded on the DAO. One situation that is also likely to arise is when data comes from sensors (integrated into an IoT network). Such projects already exist[6] although have never been used in the context of a Commons. Automation in the recording, resulting in much more data monitoring than in the example discussed section 5.4, may lead to unforeseen challenges. How this framework can address these issues calls for further research.

[5] `https://docs.openlaw.io/`
[6] See Terra0 for the example of an augmented forest `https://terra0.org/`.

5.4 A Blockchain-Based Tool to Support Governance of Land Commons in the Global South

In this section, we apply our evaluative framework to a theoretical case study in a rural community in Ghana. While the community is fictional, the institutional context and the threats it faces are not. We first introduce the context (subsection 5.4.1) before describing the application of the tool (subsection 5.4.2 and subsection 5.4.3). In these subsections, we consider that conditions discussed above are met and we discuss these assumptions in subsection 5.4.4.

5.4.1 Customary Land in Sub-Saharan Africa

This section reviews the current situation and recent history of governance and management of the land in rural areas of Sub-Saharan Africa (SSA) and Ghana in particular.

A large share of the land in SSA is currently under "customary domain". Alden Wily (2011), citing Deininger (2003), estimates that about 90% of the land is untitled in SSA and that more than 75% is estimated to be customary land. Communal tenure is a "regime of land administration comprising norms, regulations and enforcement mechanisms" (Alden Wily, 2008) not to be confused with property rights. It describes how the land is managed, what the actors and the community members rights are, and why it falls under the category of the Commons described above (Aubert et al., 2019).

In these rural areas, the land is seen as a resource linked to the community (village for instance) in ways that go beyond the definition of individual property and that is part and parcel of the identity of the village and of individuals (Bruce, 1993; Zufferey, 1986). It is a collective resource, deemed inalienable and managed collectively as a Commons (IIED, 1999). Rights to the land are differentiated and two or more users can have (concurring) rights concerning the same plot. For instance, some people may cultivate the plot for a season before leaving it to pastors for their stock to graze. Rights may also include easement such as access to water or the right to gather wood. This diversity of rights fits into the framework of the *bundle of rights* described previously.

How these rights are granted, for how long and under what conditions, depends on the social structure of the community and varies regionally. Local authorities often also play the role of land tenure authorities. For instance, in Ghana, these authorities can be called Stools (in the South), Skins (in the North) or Head of family (in the Volta Region) (Ubink and Quan, 2008). A large share of rural land, although under customary tenure, appears to be unexploited because it has been left to fallow, a necessary process of the traditional extensive agricultural model. This is particularly true in land-abundant areas, while regions with more pressure rely on rotations to regenerate the land (Migot-Adholla et al., 1991). Other areas, such as forests, are considered *res nullius* and thus not recognized as the *res communis* they actually are (Platteau, 1995).

This customary common tenure evolves into a larger country-wide legal environment. These legal environments are often inherited from colonizing countries and are not adapted to traditional practices. They often rely on a private-property-based approach with a *numerus clausus* set of rights not as complex as the reality. As Platteau (1996) notes, increased stress on the land has led many countries to propose formalization policies (often under the influence of the World Bank and other international institutions). Under the influence of the theory of "dead capital" (De Soto, 2000), there have been various attempts to divide communal land into individual plots and to give full private property rights, allegedly to increase tenure security, despite evidence of the contrary (Brasselle et al., 2002). These policies then evolved to take into account some of the customary structures which resulted in recognizing customary social structures and build on them (Toulmin et al., 2000). Local authorities typically become fiduciaries of their communal land that they must manage in the interest of the community members. Inalienability is often legally recognized to secure tenure.

Communal land governance thus takes place in a dual context of traditional rules and governance systems and a more recent and distinct legal framework. This legal pluralism has been identified as yielding significant difficulties and threatening the Commons (Le Roy, 2016). While most practitioners cited here favor a sort of formalization of the customary land rights systems in order to protect communities against land grabbing (Alden Wily, 2012; Cotula, 2012), it is widely agreed that the tools used at present have not managed to secure traditional tenure. Boamah and M. Walker (2016) summarize the process of legal pluralism in Ghana and discuss its consequences. While they focus on urban areas, their analysis remains topical to our case study.

It is also important to keep in mind that, within these legal frameworks, customary land rights systems are not fixed and have a long history of adapting to new contexts (colonization and independence in particular) and are in perpetual evolution (Migot-Adholla et al., 1991) in particular to face new challenges such as increased pressure on land. History has shown customary land rights systems are capable of adjusting which makes it even more topical for communities to retain a form of governance over their land in face of the dire stress due to climate change. Externally imposing this change and the legal pluralism that results often leads to power inequalities being reinforced because affluent and educated members of local communities are able to take advantage of the new laws. In that regard, the analysis of Federici (2011) is significant as she shows how formalization has resulted in stripping women of their rights to land in various countries because men and elites managed to exclude them from the titling process.

In Ghana, the formalization of customary tenure has led to the "curtailment of communal property rights, through a form of feudalism of land relations" (Alden Wily and Hammond, 2001). This assessment illustrates the difficulties that land system policies face. In Ghana, all the land is constitutionally vested in the president but since 1994, the Office of the Administrator of Stool Lands (OASL) has been in charge of administering communal lands. Land Commissions (LCs) are legally responsible for delivering land titles. Stools, skins or families hold allodial titles and must legally manage the land as a trust for the community. Customary land can then be ceded under freehold titles (thus leaving the customary domain and re-entering common law), customary freehold, leasehold, or sharecropping (International Business Publications, 2018). Theoretically, traditional governance is thus acknowledged and customary rights exist alongside common law. However, granting allodial titles and the possibility to then transfer these rights to individuals has led to increased inequalities and has not strengthened tenure security. As Ubink and Quan (2008) explain, although customary lands are theoretically "unsellable", in practice they are indeed sold, often informally, thus lowering the revenue of the OASL that has a redistributive goal. Local authorities often have vested interests and increasingly participate in national affairs, tailoring policies to their local interests. Moreover, there is a "national government's informal 'policy of non-interference in chieftaincy affairs'" (Ubink and Quan (2008, p.203)) making it extremely difficult for populations to contest adverse decisions and mitigating the consequences of pro-community member position of state courts. Barry and Danso (2014) and Kansanga et al. (2018) report an increasing number of conflicts at the community level, including intra-familial ones over. The causes include family or community members (including authorities) selling or fencing plots of lands and thus depriving other members of their rights. This tendency fits with the message of the paragraph-opening quote. The legal framework that sought to protect customary rights and empower communities did not provide enough checks and balances to ensure that those vested with the new rights could not abuse them.

Notwithstanding the difficult question of jurisdiction of state courts for chieftaincy issues, these courts are expensive, crowded and the proceedings time-consuming. This has led to the emergence of Alternative Dispute Resolution (ADR) mechanisms to emerge. Some are state-led, while others are either sponsored by NGOs or by the communities themselves (Yeboah and Kakraba-Ampeh, 2016). While these ADR institutions are more accessible and widely used, they, the diversity of mechanisms available also results in "forum shopping" (Agbosu et al., 2007 as cited in Barry and Danso, 2014) making it much harder to secure rights, build trust at the local level and predict resolution outcome.

In conclusion, the case of Ghana illustrates the trends described generally above. The imposition of a common law legal system onto a customary land rights system results in a dichotomy between the different rights. While the legal framework usually defers the jurisdiction to traditional authorities, this has been done in a top-down way thereby reinforcing the power of elites and endangering the equilibrium of customary systems. Conflicts are increasingly more frequent with competing jurisdiction to resolve them and the lack of common ground reduces the perspectives of community-strengthening bottom-up formalization.

5.4.2 Overall View of the Tool

Subsection 5.4.1 reviewed the situation of customary lands in the Global South and underlined that one of the challenges that communities are facing is the multiplicity of courts in case of conflicts and what courts have jurisdiction. Moreover, records of what actually happens *in situ* may be rare thus proofs may hard to produce even when a trial does take place.

To address the issue of recording local information, many communities have relied on participatory mapping. Building on traditional practices of involving local inhabitants when producing maps (Kroeber, 1939; Mitchell, 2002), Participatory Geographical Information Systems (PGIS) consists in creating geographical information with the help of private citizens who have knowledge of the situation but not of mapping techniques and technologies (Elwood and Ghose, 2011). Participatory mapping makes it possible to record more than mere geographical data and to include local specificities and to more adequately reflect the territory mapped than when an external mapper produces geographic information. There is a relatively rich literature on the empowering effect of PGIS for local communities although what is meant by empowerment is often unclear (J. Corbett et al., 2016) and may refer to both the outcome and the process (J. M. Corbett and Keller, 2005). What matters for our research is that involving community members in the production of local knowledge allows the recording of information that would not be available otherwise. It also adds political clout in the case of claims (in informal settlements in particular). Many communities are thus actively engaging in participatory processes of recording how they live on their lands.

We build on that process that we can assimilate to the Commons-Based Peer Production communities discussed by Rozas, Tenorio-Fornés, Díaz-Molina, et al. to propose a tool to complement the governance of lands Commons. The reason we introduce such a tool is because the sixth, seventh and eighth design principles are not respected. Indeed, we have seen that there is a problem of recognition by the authorities who only partially acknowledge the community sovereignty when delegating the rights to the sole customary chief. Resolution mechanisms are not available and conflicts proliferate. Finally, the layers of governance are not properly nested because the equilibrium of power between the different layers is disrupted.

The concept is to store local information on a blockchain in order to provide a reliable record of governance processes and decisions to help with conflicts. Extending the scope of participatory mapping to include the bundle of rights into the ledger along with oversight and voting rights for members of the community.

More specifically, let us consider a community whose land is under Commons tenure. In order to produce bottom-up information about their land in the face of the threats described in subsection 5.4.1, community members engage in a participatory mapping. Usually, this involves an external GIS expert with resident collaborators. Together, they map physical borders and point of interests along as experienced and lived by the community. The process involves leaving the draft maps on display in a place that is accessible to the whole community for a long time, in the market for instance, for everyone to check what has been recorded, edit it, and agree on the community-produced knowledge. This results in geographical information that is endorsed by the whole community. However, the risk of exclusion is not eliminated as community hierarchy may be reproduced in the consultation process and focus groups and transect walks[7] may also be useful to reach out in order all members of the community.

Usually, this GIS data is stored digitally in a centralized way. The community may store a copy but the permanence of the data may be compromised for various reasons. Therefore, data is often stored elsewhere, frequently by an NGO. However, the community may not have supervision of this data. Using a blockchain to store the result of participatory mapping has already been proposed by Farnaghi and Mansourian (2020). Their prototype offered a solution for consulting community members regarding site selection; our focus, however, is different.

Initial mapping does not have to be done on the blockchain as PGIS techniques are effective and there is no need to introduce more technological mediation. Once the geographical data has been produced, it is stored on a blockchain in a decentralized manner and different community members are given rights over the plots mapped. The concept is not to assign property rights or land titles but rather to record which members have rights pertaining to a plot. Regarding the bundle of rights, as soon as a member has management rights, we can condition any change in the blockchain to the approval or at least to the consultation of this member. Under these conditions, the data recorded on the blockchain would be an adequate record mirroring communal tenure.

Setting up the process would require the following steps:

1. Produce geographical information concerning the area, preferably in a community-based bottom-up process (PGIS). This geographical information should include a physical description of the land but also describe social relationships with the land.

2. Record the geographical information over a blockchain in such a way that the community retain a form a control over the data they have produced and can be confident that the data is transparent and has not been tampered with.

3. Associate community members to plots of lands. The associated rights must span the bundle of rights and allow multiple sets of property rights to be registered for the same plot. By doing this, fewer secondary users are excluded. This requires being able to associate keys to individuals which may necessitate a Public Key Infrastructure

[7] A transect walk is a systematic walk along a path to have a comprehensive understanding of the community and its surroundings.

(PKI).[8]

4. Make sure that all members are notified (when they have access rights) or asked to vote on a decision concerning a plot that they have rights to. In particular, all decisions taken by customary authorities should be recorded. In practice, when authorities take decisions, it is likely that the concerned members will be present. Validating the change on the blockchain would serve to ratify the decision and minute the process.

5. Keep the data up to date, record transactions should a plot be sold to an external buyer, etc.

This immutable, transparent database that prevents unilateral modification and respects community decision-making processes would complement the governance tools at the disposal of the community. It should prove useful at the interface between the community and the other actors such as courts, administrations or potential external buyers. However, all of the steps raise serious implementation challenges that will be discussed in subsection 5.4.4. In line with our belief that we should not disrupt what is already working, we only propose a partial technological solution that relies heavily on existing off-chain governance mechanisms.

Our proposal is summarized in Figure 5.5. In the upper (plain) part, the current situation is schematized. Customary chiefs (stool, skin or family head) are appointed as fiduciaries in the national legal framework and hence receive rights outside of the customary tenure. The Customary Authority Secretariats (CAS) and the OASL have limited effective power because of the vested interests that local authorities have at the national levels, the lack of monitoring power, and the high number of disputes to oversee. The bottom (dotted) part is the tool we propose. The village, as a cooperative manages a blockchain-based tool in which all members (including secondary users) may participate. Transparency and resilience can then be used in case of disputes and to back up claims. The tool facilitates the work of the CAS and of the OASL and reduces the risks of corruption or land grabbing.

The following section applies the framework developed in the previous section to this tool to justify it.

5.4.3 Applying The Framework

First off, let us argue why relying on blockchain-based tools could prove to be useful in the context of land Commons. The *monitor and sanction* paradigm was challenged because an external set of rules being imposed on the land and conflict resolution mechanisms were external to the community. In turn, applying the framework will demonstrate that *automating (and recording) and verifying* works well and may solve some of the problems

[8] A PKI helps to match digital identities to individuals.

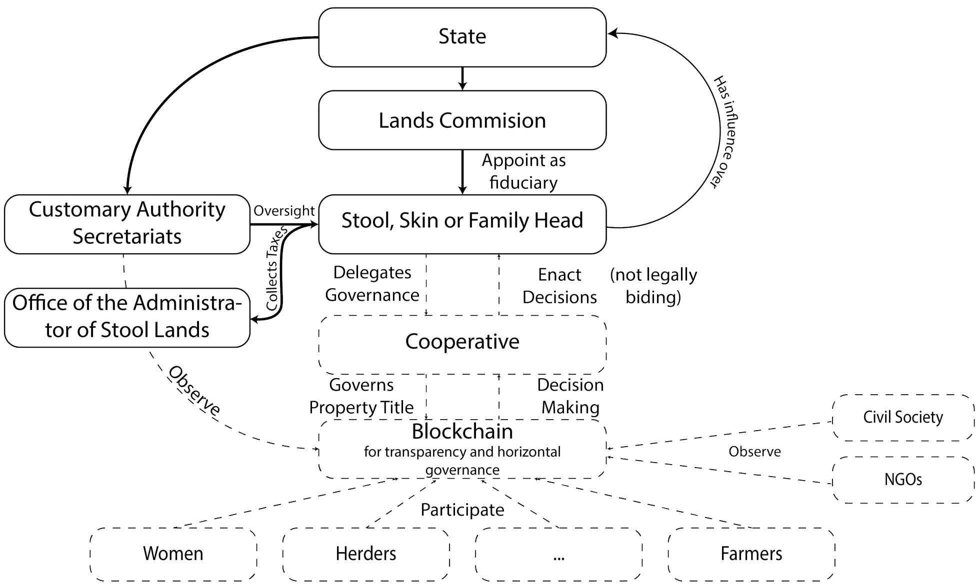

Figure 5.5: Blockchain-Based Tool to Supplement Governance of Land Commons in Ghana

identified above. Consistently with the rest of the paper, we here review general issues but apply them to Ghana when possible.

Let us first consider the types modalities for the seven types of rules.

Boundary Rules: The boundary rules are not changed and are simply encoded onto the blockchain. According to the literature, in Ghana membership to the community is required. That is to say that only members of the community have the rights to participate in the governance of the land. Traditionally, members of families long established in the area are those who participate in the Commons. Newcomers may also be involved although conditions vary. With the rapid demographic transition, rural exodus, and increased mobility, boundary rules might be set to change in the near future. The introduction of our prototype does not prevent any of these evolutions.

Position Rules: Similarly, the blockchain here only serves to record and encode position rules that are in place locally. Usually, elders possess particular positions in the community and firstborn sons have primary exploitation rights. One of the issues might be that the customary position rules exclude a part of the population such as women whose work and rights are often not adequately acknowledged. Our tool might be used to recognize their "invisible work". This issue will be thoroughly discussed in subsection 5.4.4. The positions held by customary authorities are mirrored by the DAO. Given the importance of familial relationship, it would be relevant to offer a way to record lineage and hereditary rights.

Choice Rules: We associate choice rules to position rules in the DAO. In particular, customary authorities have the power to modify which families have rights to certain plots. Checks and balances that exist off-chain should be incorporated into the blockchain. In particular, off-chain decisions should always precede modifications of the blockchain. Other members of the community have the right to record in the DAO any change pertaining to the land they have rights to.

Information Rules: The DAO does not modify the information rules already in use within the initial action situation (*i.e.* the village, its land) but its transparency and auditability makes information available to external agents. As such, it modifies the information rule concerning the Commons. What information is available to whom will depend on the implementation and the type of blockchain but the rationale of this blockchain-based solution is to provide a proof of process to conflict resolution mechanisms.

Aggregation Rules: Here again, the idea is to mirror the aggregation rules used off-chain. Encoding them in a DAO will formalize the process and, as in the case of choice rules, may result in more inclusion with explicit inclusion of all concerned members. It is important that even the authorities should not have the capacity to modify the state of the DAO unilaterally even if they have this right off-chain. Indeed, there often are social control mechanisms that may be hard to codify over the blockchain. We thus recommend validation by multiple other members for decisions taken by the customary authorities. For decisions that require validation by the community, voting mechanisms will be deployed in the DAO. In the case of a rural community, there will be only a few of these a month and sorting out which are the most important ones may not be necessary. Quorum and qualified majority can easily be encoded, as well as veto powers.

Scope Rules: On top of the existing scope rules already at play within the governance process, our tool introduces one new scope rule, already mentioned in the information rule: to what extent is the information recorded in the DAO available to whom. Blockchains offer ways to filter access to information. In this case, it is likely that auditability will be essential for some external actors, including governmental ones but, in order to preserve privacy, free public access should not be allowed.

Payoff Rules: We do not advocate using the blockchain tool for payoff for several reasons. First off, it is unlikely that a cryptomarket will develop quickly in areas that still have unreliable electricity access. Secondly, the land conveys meanings that go beyond monetary value and assigning tokens may reduce social incentives. This is very much in line with the design dilemmas already discussed. This is not to say that the payoff rules will not be modified. A community willing to use our blockchain-based tool should incorporate social (or economic) sanction mechanisms when the state of the ledger does not adequately reflect the reality of the relationship to land, for example if an agent tries to omit a decision from the record or include a fraudulent one. These mechanisms should not only be applied off-chain but also incorporated into the DAO. Indeed, supposing that the social sanction includes being deprived of voting rights or of rights to exploit a plot, this should be adequately reflected on-chain.

Identifying the new modalities, and in particular the Information and Scope Rules, emphasizes that the introduction of a blockchain-based tool modifies the broader context. Going back to Figure 5.2, this particularly affects the dotted arrow between the outcomes and the external variables.

Let us now consider how these new modalities of implementation may positively affect the situation through the lens of the design principles. On top of the boxes presented in Table 5.1, we have also noted that the affordances of transparentization and self-enforcement help for fulfill DP8. The latter is also relevant for DP6. We present the results Table 5.4. The proposed DAO would address the issues of unmet design principles by providing a tool at the interface between the community and the broader institutional context. How the feedback loop is affected is described by the affordances. In particular, self-enforcement and formalization in the DAO allow the ad-hoc rules of the community

	Tokenization	Self-enforcement and formalization	Autonomous automatization	Decentralization of power over infrastructure	Transparentiza-tion	Codification of trust
Clearly defined community boundaries	Only community members can participate					
Congruence between rules and local conditions	Local rules retain the priority	Modularity in the DAO offers allows to encode local rules over		Increases local sovereignty		
Collective choice arrangements	Congruence between off-chain Policy Level and DAO Governance is assured through ex ante control mechanisms in the DAO			Possibility to host a node increases collective agency		
Monitoring		Transparency of decisions	Ex-ante coding of the possible outcomes concerning plots to avoid illegal (trans)actions	Increases trustworthiness	Yes	
Graduated sanctions		Once sanctions are voted and collectively decided, they are automatically enforced	Sanctions should not be automated			
Conflict resolution mechanisms		Formalization inscribes the situation in a given legal framework, reducing uncertainty and institutional confusion	Not relevant in this case		Transparency facilitates conflict resolution by providing information to courts	
Local enforcement of rules		Formalization of rules increases the legitimacy by recording local processes		Local hosting of the database increases legitimacy		Protects against malevolent agents empowering the community
Multiple layers of nested enterprises		Formalization inscribes the situation in a given legal framework, reducing uncertainty and institutional confusion	Increases community autonomy		Transparency facilitates conflict resolution by providing information to courts	Increases legitimacy

Table 5.4: Blockchain-Based Governance Affordances Applied to Land Commons

Source: Adapted from Rozas, Tenorio-Fornés, Díaz-Molina, et al. (2018), p.22

to be formalized in a flexible manner that can still be audited, when necessary, by conflict resolution committees. The decentralization of power over infrastructure empowers the local community, who remains in control of their data, while benefitting from the reliability offered by blockchains technology. The goal is for governmental institutions and potential buyers to recognize the DAO as a description of the rights of the different members of the community over the land. Codification of trust helps secure land tenure for communities as land-grabbing attempts will necessarily occur off-chain and will not be recorded on the DAO. The "confidence machine" increases the confidence into what is recorded while reducing confidence in what is unrecorded, in accordance with our objectives.

Lastly, we point to how the design dilemmas could be addressed. Because the resolution would eventually depend on a co-development process with the communities involved, we only highlight the stakes associated with the dilemmas.

As far as the transparency vs privacy dilemma is concerned, the main issue will concern dealing with users' identity in order to preserve privacy of the community members while ensuring that only right-holders can undertake given actions within the DAO. This dilemma also relates directly to the scope rules as we have noted previously. The extent to which the data is available to external members is an essential question. Should it be available to arbitrators (or judges) only in the case of dispute, or should the information be freely auditable by some government agencies? These are issues that will require trade-offs. The type of blockchain used for implementation will be informed by the community-made decision.

Concerning the economic value vs the social value, we recommend limited recourse to tokens as we believe the set of values predates the introduction of the blockchain-based tool in this case and that our tool should be as neutral as possible in terms of community values. Similarly, the we recommend not using the blockchain-based tool for payoff in order to avoid as much this dilemma.

The GIS data recorded over the blockchain is not quantifiable in itself however, it can easily be affected by these dilemmas as some quantifiable information (such as area, length of tenure, etc.) may be associated with this information. Bearing in mind that this tool is proposed to tailor rights-recording solutions to local situations, standardization to quantified values should be avoided as much as possible.

The incentivization and manipulation dilemma is highly correlated to the two previous ones in the way originally described. In our case, it extends to how to incentivize every agent to use the blockchain-based tool systemically. Incentives over the blockchain could take the form of reputation tokens (non market-valued) that would also necessitate integration in the social value system and be linked to manipulation.

The balancing of private vs collective interests is at the root of the proposed tool. The aim of the tool is to rebalance the situation from conflicting private interests towards the

Commons and to provide a tool for common resolution of conflicts over land plots. In our case, the resolution mechanisms to arbitrate between private and collective interests would be competent jurisdiction with the DAO record serving as a basis for the decision.

As Figure 5.4 indicated, off-chain governance choice levels and blockchain governance choice levels intersect. We have noted that the way the community decides to resolve the transparency dilemma will inform the choice of the blockchain and, ultimately, the levels of blockchain governance rules. Similarly, the type of DAO will follow concertation within the community, as indicated by the two red arrows on the figure. This will also address the human vs algorithmic governance dilemma.

This section has illustrated how the framework discussed in the paper may be applied to a land Commons. Because the tool is still at a theoretical level, the analysis remains superficial but points to what will be critical in the success or failure of such an initiative.

5.4.4 Challenges in Implementation

So far, we have assumed that the conditions were met for the community to use a DAO. This fictitious case study has allowed us to illustrate our framework and to provide an example of evaluation and design for blockchain-enhanced governance mechanism.

Subsection 5.3.3 identifies the potential limits for applying this framework. This section diagnoses the limitations in the land Commons case study.

We have seen that the introduction of new technologies in areas with low levels of (digital) literacy and scarce access to electricity can cause technological exclusion or lead to algocracy (power in the hands of people who can code). To avoid creating or reinforcing inequalities and proposing an inadequate solution, we believe that co-development of the solution should take place with the community, local civil society, and practitioners in the field of participatory tech-based solutions.

First, there is the general issue of user experience for interacting with the tool. Computers are not widely available in rural SSA but access to mobile phones is much more frequent. Therefore, a mobile-phone-based interface should be favored for accessibility. Ideally, this would be implemented both in the form of an app for smartphones and with an interface working via text messages. These already exist for the management of savings accounts and could be imitated. Importantly, the tool should propose solutions for access by members of the community who do not possess a phone or a computer. Indeed, it is likely that the secondary users who are the most at risk of being stripped of their rights (members of minorities, women, etc.) are also the ones with least access to technological devices. Any technology gap must be addressed in order to avoid a potentially adverse outcome. An access point in the village could be the solution but this may not be practical if a large number of community members lack access to either phones or computers. This question is also of importance for hosting nodes of the blockchain and ownership of the data. It is particularly important if only a hash of the data is stored online while some of the computing or storing happens off-chain. In that case, reliable access to the internet is necessary for the community. However, this remains a challenge for many regions. It is likely that some regions are more ready than others for such tools. In particular, Latin America and the Caribbean may have a socio-technical environment that is more suited to implementation in the short term.

Other important issues are gender, inequalities, and exclusion. We have mentioned above that women have very important social roles but most of Ghana (and SSA in general) is patrilineal and women often depend on their fathers, brothers or husband for property rights. On top of the agricultural work they do—they are often in charge of "sowing, weeding, harvesting, storing, processing, and marketing" (Federici, 2011 citing Snyder and Tadesse, 1995)—they often collect wood and fetch water which at least entails the need for access and withdrawal rights. It is thus important to ensure that the process of formalization of rights over the DAO does not enshrine this exclusion. The equilibrium between respecting traditional governance processes and fostering women's empowerment might be delicate but there are various examples in which the introduction of new technologies and formalization helped record and visibilize the work and cognitive workload borne by women and increased gender equality. The introduction of our tool should make sure all users' rights are adequately encoded in the DAO in order for everyone to have a chance to defend their right and their relationship with land.

5.5 Conclusion

Throughout the paper, we have demonstrated that there are theoretical arguments in favor of using blockchains for the governance of Commons, including natural-based Common-Pool Resources. We build on the work of the Bloomington School by applying the Institutional Analysis and Development Framework to governance processes using blockchain-based tools. We unify different strands of research on blockchains and governance of the Commons into a single framework. It allows us to understand how the affordances described by Rozas, Tenorio-Fornés, and Hassan (2021) fit into the paradigm described by Poux et al. (2020), while incorporating hindsight from Cila et al. (2020). In particular, it focuses on disentangling the interaction between the different governance levels and the blockchains layers. We show that the aforementioned papers do not explicitly state which levels they are addressing and that the wider context has often been overlooked. For instance, while significant attention has been devoted to the operational level, the constitutional levels have often received much less consideration although blockchain-based tools are likely to substantially alter them.

This framework could be used by practitioners to either design or describe a sustainable governance process relying on automation and transparency in situations where traditional tools have failed. To illustrate how this could be done, we apply our framework to the case of land Commons in rural Ghana. Building on the work of local experts, we propose a Proof of Concept (PoC) for a blockchain-based tool to address the enclosures threatening customary tenure. We show how the successful adoption of a blockchain-based tool requires careful co-development with *the commoners*, suitability to the local context, and widespread adoption. Bearing this in mind, we propose a DAO prototype to record and mirror the customary continuum of rights over different plots of land. Harnessing the flexibility, the transparency, and the resilience of distributed ledgers, we show that it is possible to record the rights of all users including those most at risk of being stripped of their rights in a context of legal pluralism. Serving as a transparent ledger, such a DAO could help communities resolve disputes over land and back legitimacy claims. We are aware that this PoC remains theoretical and may face certain limitations in developing countries but we believe it could spark further research and applications in that direction in the medium term.

Our paper explores a path for the future application of blockchain-based governance tools. The contribution to the literature is two-fold: first, it offers an actionable framework to analyze recourse to blockchains for the governance of Commons actualizing a time-proven framework. Second, it illustrates how to use this framework by proposing a novel PoC for the governance of threatened land Commons. The literature at the intersection of governance processes, natural CPR and blockchains remains new and our research highlights some of the directions it may take.

Conclusion

Conclusion

This dissertation is a contribution to the understanding of how blockchains can be channeled by communities to invent new institutional arrangements. It particularly focuses on the changes brought about by blockchains in terms of constitutional arrangements. The core of the thesis discusses how the economic theory of the Commons can inform the establishment of a set of rules, both hard-coded into the blockchain and for human interactions, to govern a resource and oversee the provision of a public or common good. After a general introduction situating the context of this research and motivating my PhD, the manuscript starts with an extensive Literature Review. Because my research interrogates how blockchains can be used by groups who may not be tech savvy, it begins with an introduction on the functioning of blockchains that aims to clear enough to familiarize even the less informed reader with the basics. For the sake of clarity, it does not wish to be exhaustive and concentrates on the features that are most important in my work. The presentation of the blockchain environment, and in particular of the Decentralized Autonomous Organizations (DAOs), softwares that run decentrally on the network and are used by a community of users to coordinate and govern a resource, naturally leads to describe the different types of blockchain users and the challenges associated with the management of the network. This is an active research question and subsection 1.1.4 reviews the state of the art. Notably, it underlines that the governance of blockchains is complex, composed of entrenched on-chain (algorithmic through the code of the blockchain) and off-chain (decision-making taking place outside of the chain) processes. It also highlights that the questions of governance *of a* and *with a* blockchain are closely linked as the challenges and the specificities of both are similar. These include dealing with permanence of the data, the benefits and risks of transparency and how to take into account data from outside of the chain.

Section 1.2 then presented the economic theories and methods that I have used in my research. I have chosen political economy and, more specifically, Public Choice theory and Ostrom's theory of the Commons for two reasons. The first one is that it provides a useful framework, relying micro-economics methods, to describe and analyze the dynamics of decision-making. The second is that the premises underlying the design of blockchains and the theories of political economy (in terms of rational behavior and contractarian approach) are strikingly close, facilitating the analysis. The presentation of political economy theories and how they can be applied to blockchain(-based) communities delineates a fertile research program that has already been initiated. Various scholars have applied findings and methodologies from political economy to characterize the new institutional arrangements of blockchains communities. Notably, they contribute to define the new affordances of blockchain-(based) governance. Analysis of blockchains as Commons has provided insights in terms of best practices and risks in their governance. A more recent strand of research has outlined the potential of blockchain-based applications such as DAOs to govern CPR, in particular Knowledge Commons. This research program is ongoing, and some areas that deserve more attention and have inspired the original research of the manuscript. For instance, the research on "crypto-democracy" could benefit from an extension to various voting method and I discuss the case of Liquid Democracy in chapter 3. From the theory of the Commons, I apply findings to suggest a collective approach to the topical issue of Maximal Extractable Value in Ethereum (chapter 2). Finally, the application of the Institutional Analysis and Development framework to blockchain-enabled exhibits that the classical Institutional Analysis and Development framework must be completed to account for the peculiarities of blockchains. Chapters 4 and 5 attempt to provide a unified evaluative framework extending the work of Ostrom. In doing so, it evidences that specific attention should be devoted not only to the operational level (as most existing papers do) but also to the constitutional ones.

The second chapter, *Maximal Extractable Value and the Blockchains Commons*, co-authored with P. de Filippi and B. Deffains, addresses the problem of Maximal Extractable Value (MEV) in Ethereum. This practice consists in actors (miners and searchers) appropriating the value contained in the blocks of the chain by manipulating the order of the transactions it contains. This practice becomes increasingly frequent and is frequently done at the expense of the bulk of the users. We propose a theoretical conceptualization of this behavior informed by the theory of the Commons. In particular we demonstrate that MEV constitutes a new form of free-riding, different from the one classically discussed in economics. It does not result from a lack of participation in the provision of a public good but rather from unfair appropriation of value. This characterization in terms of free-riding leads us to turn to the theory of the Commons to describe how groups can set up collective rules to prevent it. In order to apply Ostrom's framework, we must first better characterize MEV. By doing so, it appears that there are two types of MEV: the first one furthers the objectives of the systems and increases the overall efficiency of the network while the second reduces it leading to congestion and increased costs. Alongside these technical considerations, we demonstrate that this decreased efficiency also brings reduced confidence in the system which may reduce user's adoption and compromises the stability of the network in the long run. This is corroborated by the assessment of Ostrom's 8 design principles that evidence that MEV undermines the sustainable management of the blockchain as a Commons. Discussing the existing solutions, we show that they rely on competing forms of legitimacy that are rooted more in a private market-based (Flashbots) or an external control akin to public management (Chainlink). We contend that a collective Commons-based approach is worth investigating as it may result in a legitimate solution that reinstate confidence through trust-based mechanisms.

Representation and Intensity of Preferences moves away from the governance *of* the blockchain and introduces the main questions of the manuscript: how can blockchains be used to propose new coordination methods for communities and what should we expect from these methods. I start with a discussion concerning one of the core aspects of coordination: aggregation of preferences. Blockchain-based e-voting (BEV) allows to implement new forms of voting methods that would be impracticable otherwise. Among them, Liquid Democracy has attracted significant attention recently, as its champions claim that it allows to faithfully represent the will of the voters and produces efficient output. The underlying principles of Liquid Democracy is that (i) citizens can vote directly, (ii) they can delegate their votes on one, some, or all areas to a representative, (iii) delegation is transitive, and (iv) delegation can be terminated at any time.. It is believed that by delegating votes transitively to more informed and knowledgeable representatives (called gurus), socially optimal outputs may be reached. My analysis, shows that the reality is more nuanced. In particular, while Liquid Democracy as a voting method allows to reduce the costs of decision-making and can facilitate the adoption of more unanimous decisions, it is unsure whether it achieves superior outcomes. Moreover, Liquid Democracy as a political system is not scalable because it cannot provide a mechanism to trade or bundle votes and engage in formal or informal logrolling. The intensity of preferences is thus not taken into account and this can lead to a form of "tyranny of the majority". What is more, the question of the institutions, in particular those in charge of the legislative work, is still largely unresolved. Finally, I discuss the specific challenges of BEV and recall that the governance problems associated with blockchains also affect blockchain-based voting platforms. I conclude that, in the case of small to medium scale communities with only a limited scope of issues to vote on, the benefits of Liquid Democracy may largely outweigh its limitations. Notably, such communities include DAOs or communities managing a Commons.

The next two chapters participate to the research program dedicated to characterizing the new possibilities brought by blockchains for the governance of CPRs. Chapter 4, *Blockchains for the Governance of Common Goods*, P. de Filippi, S. Ramos and I describe the paradigmatic changes entailed by the use of blockchain-based tools to enhance the governance of a Commons. In particular, we discuss the consequences of having to codify *ex-ante* the different actions possible and the fact that any action executed on the chain will remain there indefinitely. This constitutes an evolution from a *monitor and sanction* where agents can defect and take the risk of being sanctioned to an *automate and verify* paradigm where the set of possible of actions is constrained and defection is technically infeasible. While this modification may reinstate the conditions for collaboration in low-trust environments we argue that it does not suffice to create a Commons, especially for the management of natural resources. In these cases, the need to validate external data and the role of *oracles*, the smart-contracts recording external data on the blockchain, requires numerous off-chain processes and a form of collaboration. This evidences that in these contexts, governance can be complemented or even supplemented but not replaced by blockchain-based tools. Discussing this change of paradigm also leads us to consider the new modalities of rule implementation that blockchain-enabled governance adds to the list identified by Ostrom and her colleagues. In the Institutional Analysis and Development framework, they have developed a formal grammar based on typology of rules. To describe and analyze a governance system, scholars must document the way these rules are implemented. This chapter only touches upon how blockchains increase the number of modalities for these rules and this question is developed in the following chapter.

In *A Unified Framework for the Governance of the Commons with Blockchain-Based Tools*, S. Ramos and I put the previous chapter in relation with two foundational papers of commons-oriented blockchain-based governance (Rozas, Tenorio-Fornés, Díaz-Molina, et al. (2018) and Cila et al. (2020)) and propose to unify them in a single framework. To do so, we outline which aspects of the Institutional Analysis and Development framework they each refer to. This provides us with a time-proven framework to see how their results can be put in perspective and how they relate to each other. What is more, it also outlines the parts of the Institutional Analysis and Development framework that have received less attention in blockchain-based governance research. Notably, this work manifests that most of the work so far has focused on the operational level, the day-to-day operations. Our work discusses the consequences that recourse to DAOs may have on the constitutional levels and the collective choice mechanisms. In particular, we insist that they cannot substitute for the social contract that brings legitimacy to the whole governance process but can complement it. It also shows the parallel between the choice levels of the Institutional Analysis and Development framework and the governance levels of blockchain-based organizations before discussing the new modalities enabled by DAOs. This theoretical work is illustrated by a fictitious case study on customary land commons in Ghana. In this situation, a low-trust environment, increased pressure on land, and legal-pluralism reducing the possibilities of local and accessible dispute resolution mechanisms have seriously undermined the traditional Commons-based management of the land. We propose of blueprint for a DAO that commoners could use to legitimize their claims and reduce dispute resolution costs. We also show that the formalization necessitated by the codification of rights and practices may reinstate confidence and ultimately increase interpersonal trust under some conditions. This case study also allows us to mention the risks and limitations of such a tool. Introducing a digital media as complex a blockchain is likely to create power asymmetries or to exclude tech illiterate users. The codification process should be careful not to record and accentuate existing inequalities and increase the disenfranchisement of at-risk users. However, existing practices have demonstrated that when properly conducted in a bottom-up manner, introduction of digital tool may in turn empower communities. The overview of these risks leads us to conclude that, in this case study, although the governance challenges may be suited for experimentations, the context and the attributes of the community make it unrealistic to consider this application in the short to medium term.

All this work participates in a better understanding the dynamics and challenges of blockchain-enabled collective decision-making. Studying different usages of blockchains allows to delineate and accrue to the comprehension of blockchain-based collective choice. I have shown that the decentralization, transparency and automation enabled by blockchains create the opportunity to conceive and implement new constitutional settings and facilitate repeated coordination in settings where it might not have been possible otherwise for lack of trust. This dissertation builds on existing literature to conclude that blockchains provide confidence that may serve as a ground for new institutional arrangements. However, the very tool that introduces this confidence needs being governed. While blockchains were built to be trustless systems, it is now clear that the challenges its governance faces demand trust.

The main contribution of this manuscript is to extend the research on blockchain-based governance to new domains. In particular, it strengthens the links it has with the theory of the Commons, notably applying it to natural resources while most of the existing research had focused on community-based peer produced Commons. Focusing on the interplay between the specific challenges of DAO governance and those of CPR management allows to also propose directions for governance of future blockchains that may be more collectively governed.

My research takes place in emerging research program that is rich with fascinating questions. The work presented in this manuscript is mainly theoretical and developing a more hands-on and grounded research would be beneficial. While I have identified the conditions under which resources could benefit from the recourse to a DAO to (re)instore a Commons, I have also showed that even in contexts where blockchains could reinstate institutional confidence, implementation often face drawbacks and implies risk for potential communities. I believe a next step would be the identification of suitable case-studies. During a lecture I gave in the spring of 2022, I invited the participants, from dozens of countries, to think of the situations they knew of that may be relevant. In less than ten minutes, there were numerous that were proposed and insightful discussions followed, notably on the question of water management in Mexican cities. This indicates that it is a fertile direction to engage in.

Furthering the exploration of potential applications of blockchain-based governance is also an important project and I am committed to investigating the potential of DAOs for platform-cooperatives. Other open questions are proposed in the conclusions of each of the chapters. They are diverse but I believe that a central issue is the notion of scales and homogeneity of the communities. While confidence in the system and decentralization theoretically make it possible to scale up and apply the conclusions to arbitrarily large groups, the results of recent research, including the one presented here, indicate that groups mediated by blockchain will also face challenges when scaling up. While it may not be insurmountable, I believe dedicated research would be extremely valuable.

My work participates to a field of research that attempts to build new imaginaries and narratives for blockchains and promote non-monetary usages. Considering the growth rate of blockchain adoption, the impact it already has on the financial sector, the legal issues it raises but also the potential for decentralized coordination it brings, I am convinced that it is an important matter not only for blockchain users but for society as whole. Specifically, in face of the environmental crises we are going through, a Commons-based approach may facilitate coordination to preserve natural resources at various scales, from local ground water to the atmosphere. If blockchains can serve as a catalyst for collective governance in some situation (while reducing their current energy consumption), it is paramount that we contribute to understanding how they can do so.

List of Figures

List of Tables

Bibliography

@n4motto (June 2022). *Emre Tweet.*

3Blue1Brown (July 2017). *How Secure Is 256-Bit Security?*

Agbosu, Lennox et al. (2007). "Customary and Statutory Land Tenure and Land Policy in Ghana". In.

Alden Wily, Liz (Jan. 2008). "Custom and Commonage in Africa Rethinking the Orthodoxies". In: *Land Use Policy* 25.1, pp. 43–52. ISSN: 0264-8377. DOI: 10.1016/j.landusepol.2007.02.002.

— (2011). "'The Law Is to Blame': The Vulnerable Status of Common Property Rights in Sub-Saharan Africa". In: *Development and Change* 42.3, pp. 733–757. ISSN: 1467-7660. DOI: 10.1111/j.1467-7660.2011.01712.x.

— (July 2012). "Looking Back to See Forward: The Legal Niceties of Land Theft in Land Rushes". In: *The Journal of Peasant Studies* 39.3-4, pp. 751–775. ISSN: 0306-6150. DOI: 10.1080/03066150.2012.674033.

Alden Wily, Liz and Daniel Hammond (2001). "Land Security and the Poor in Ghana: Is There a Way Forward". In: *A Land Sector Scoping Study, DFID Ghana's Rural Livelihoods Programme.*

Alger, Dan (Jan. 2006). "Voting by Proxy". In: *Public Choice* 126.1, pp. 1–26. ISSN: 1573-7101. DOI: 10.1007/s11127-006-3059-1.

Aligica, Paul D. and Vlad Tarko (2012). "Polycentricity: From Polanyi to Ostrom, and Beyond". In: *Governance* 25.2, pp. 237–262. ISSN: 1468-0491. DOI: 10.1111/j.1468-0491.2011.01550.x.

Allen, Darcy W. E. et al. (May 2017). *The Economics of Crypto-Democracy.* SSRN Scholarly Paper ID 2973050. Rochester, NY: Social Science Research Network. DOI: 10.2139/ssrn.2973050.

— (July 2018). "Cryptodemocracy and Its Institutional Possibilities". In: *The Review of Austrian Economics.* ISSN: 1573-7128. DOI: 10.1007/s11138-018-0423-6.

Allen, Douglas W. (2012). *The Institutional Revolution: Measurement and the Economic Emergence of the Modern World.* Markets and Governments in Economic History. Chicago ; London: University of Chicago Press. ISBN: 978-0-226-01474-6.

Alston, Eric et al. (Jan. 2022). “Blockchain Networks as Constitutional and Competitive Polycentric Orders”. In: *Journal of Institutional Economics*, pp. 1–17. ISSN: 1744-1374, 1744-1382. DOI: 10.1017/S174413742100093X.

Arrow, Kenneth J. (1951). *Social Choice and Individual Values: Third Edition*. Yale University Press. ISBN: 978-0-300-18698-7.

Atzori, Marcella (2017). “Blockchain Technology and Decentralized Governance: Is The State Still Necessary?” In: *Journal of Governance and Regulation* 6.1. ISSN: 22209352, 23066784. DOI: 10.22495/jgr_v6_i1_p5.

Aubert, Sigrid et al. (Oct. 2019). *L'approche Par Les Communs de La Terre et Des Ressources Qu'elle Porte Illustration Par Six Études de Cas.*

Bano, Shehar et al. (Nov. 2017). *Consensus in the Age of Blockchains*. arXiv: 1711.03936 [cs].

Barry, Michael and Ephraim Kwame Danso (July 2014). “Tenure Security, Land Registration and Customary Tenure in a Peri-Urban Accra Community”. In: *Land Use Policy* 39, pp. 358–365. ISSN: 0264-8377. DOI: 10.1016/j.landusepol.2014.01.017.

Batubara, F. Rizal, Jolien Ubacht, and Marijn Janssen (May 2018). “Challenges of Blockchain Technology Adoption for E-Government: A Systematic Literature Review”. In: *Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age*. Dg.o '18. New York, NY, USA: Association for Computing Machinery, pp. 1–9. ISBN: 978-1-4503-6526-0. DOI: 10.1145/3209281.3209317.

Bauwens, Michel and Alekos Pantazis (Mar. 2018). “The Ecosystem of Commons-Based Peer Production and Its Transformative Dynamics”. In: *The Sociological Review* 66.2, pp. 302–319. ISSN: 0038-0261. DOI: 10.1177/0038026118758532.

Benkler, Yochai (2006). *The Wealth of Networks: How Social Production Transforms Markets and Freedom*. New Haven, Conn.: Yale Univ. Press. ISBN: 978-0-300-12577-1 978-0-300-11056-2.

Benkler, Yochai and Helen Nissenbaum (Dec. 2006). “Commons-Based Peer Production and Virtue”. In: *Journal of Political Philosophy* 14.4, pp. 394–419. ISSN: 0963-8016, 1467-9760. DOI: 10.1111/j.1467-9760.2006.00235.x.

Berg, Alastair, Chris Berg, and Mikayla Novak (2018). “Crypto Public Choice”. In: *SSRN Electronic Journal*. ISSN: 1556-5068. DOI: 10.2139/ssrn.3236025.

Berg, Chris (July 2017). *Delegation and Unbundling in a Crypto-Democracy*. SSRN Scholarly Paper ID 3001585. Rochester, NY: Social Science Research Network. DOI: 10.2139/ssrn.3001585.

Berg, Chris, Sinclair Davidson, and Jason Potts (2019). “Blockchains as Constitutional Orders”. In: *James M. Buchanan: A Theorist of Political Economy and Social Philosophy*. Ed. by Richard E. Wagner. 1st edition 2019. Remaking Economics: Eminent Post-War Economists. Palgrave Macmillan. ISBN: 978-3-030-03080-3 978-3-030-03079-7.

Bernholz, Peter (1973). “Logrolling, Arrow Paradox and Cyclical Majorities”. In: *Public Choice* 15, pp. 87–95. ISSN: 0048-5829.

Black, Duncan (1958). *The Theory of Committees and Elections*. Dordrecht: Springer Netherlands. ISBN: 978-94-010-8375-1 978-94-009-4225-7. DOI: 10.1007/978-94-009-4225-7.

Black, Julia (2008). "Constructing and Contesting Legitimacy and Accountability in Polycentric Regulatory Regimes". In: *Regulation & Governance* 2.2, pp. 137–164. ISSN: 1748-5991. DOI: 10.1111/j.1748-5991.2008.00034.x.

Bloembergen, Daan, Davide Grossi, and Martin Lackner (Nov. 2018). "On Rational Delegations in Liquid Democracy". In: *arXiv:1802.08020 [cs]*. arXiv: 1802.08020 [cs].

Blum, Christian and Christina Isabel Zuber (2016). "Liquid Democracy: Potentials, Problems, and Perspectives". In: *Journal of Political Philosophy* 24.2, pp. 162–182. ISSN: 1467-9760. DOI: 10.1111/jopp.12065.

Boamah, Emmanuel Frimpong and Margath Walker (2016). "Legal Pluralism, Land Tenure and the Production of "Nomotropic Urban Spaces" in Post-colonial Accra, Ghana". In: *Geography Research Forum* 36, pp. 86–109.

Bodó, Balázs and Heleen Janssen (June 2021). *Here Be Dragons - Maintaining Trust in the Public Sector in Face of Emerging Tech*. SSRN Scholarly Paper ID 3868208. Rochester, NY: Social Science Research Network.

Bodon, Herminio et al. (June 2019). *Ostrom Amongst the Machines: Blockchain as a Knowledge Commons*. SSRN Scholarly Paper ID 3462648. Rochester, NY: Social Science Research Network.

Bollier, David (2002). "Commons Sense - Community Ownership and the Displacement of Corporate Control". In: *Multinational monitor* 23.7 & 8. ISSN: 0197-4637.

— (2007). "The Growth of the Commons Paradigm". In: ed. by Elinor Ostrom and Charlotte Hess. Understanding Knowledge as a Commons: From Theory to Practice. Cambridge, MA: MIT Press, pp. 27–40.

— (2014). *Think Like a Commoner: A Short Introduction to the Life of the Commons*. Gabriola Island: New Society Publishers. ISBN: 978-0-86571-768-8 978-1-55092-559-3.

— (Mar. 2015). *The Blockchain: A Promising New Infrastructure for Online Commons*.

Borda, J.-C. de (1781). "Mémoire Sur Les Élections Au Scrutin: Histoire de l'Académie Royale Des Sciences". In: *Paris, France* 12.

Boyle, James (Apr. 2003). "The Second Enclosure Movement and the Construction of the Public Domain". In: *Law and Contemporary Problems* 66.1, pp. 33–74. ISSN: 0023-9186.

Brasselle, Anne-Sophie, Frédéric Gaspart, and Jean-Philippe Platteau (Apr. 2002). "Land Tenure Security and Investment Incentives: Puzzling Evidence from Burkina Faso". In: *Journal of Development Economics* 67.2, pp. 373–418. ISSN: 0304-3878. DOI: 10.1016/S0304-3878(01)00190-0.

Breidenbach, Lorenz et al. (Apr. 2021). "Chainlink 2.0: Next Steps in the Evolution of Decentralized Oracle Networks". In: *Chainlink Whitepaper*.

Brody, Ann and Stéphane Couture (Sept. 2021). "Ideologies and Imaginaries in Blockchain Communities: The Case of Ethereum". In: *Canadian Journal of Communication* 46.3, pp. 543–561. ISSN: 0705-3657, 1499-6642. DOI: 10.22230/cjc.2021v46n3a3701.

Bromley, Daniel W. (1986). “Closing Comments. National Research Council”. In: *Proceedings of the Conference on Common Property Resource Management, National Academy Press, W~ Ishington, DC*, pp. 593–598.

Bruce, John W. (1993). “Do Indigenous Tenure Systems Constrain Agricultural Development?” In: *Land in African agrarian systems*, pp. 35–56.

Buchanan, James M. (Dec. 1962). “The Relevance of Pareto Optimality”. In: *Journal of Conflict Resolution* 6.4, pp. 341–354. ISSN: 0022-0027. DOI: 10.1177/002200276200600405.

— (1965). “An Economic Theory of Clubs”. In: *Economica* 32.125, pp. 1–14. ISSN: 0013-0427. DOI: 10.2307/2552442.

Buchanan, James M. and Gordon Tullock (1962). *The Calculus of Consent: Logical Foundations of Constitutional Democracy*. The Selected Works of Gordon Tullock v. 2. Indianapolis: Liberty Fund. ISBN: 978-0-86597-521-7 978-0-86597-532-3.

Buterin, Vitalik (May 2014). *DAOs, DACs, DAs and More: An Incomplete Terminology Guide*.

— (Apr. 2021). *Why Sharding Is Great: Demystifying the Technical Properties*.

Caplan, Bryan (May 2003). “The Logic of Collective Belief”. In: *Rationality and Society* 15.2, pp. 218–242. ISSN: 1043-4631. DOI: 10.1177/1043463103015002003.

Caragiannis, Ioannis and Evi Micha (Aug. 2019). “A Contribution to the Critique of Liquid Democracy”. In: *Proceedings of the Twenty-Eighth International Joint Conference on Artificial Intelligence*. Macao, China: International Joint Conferences on Artificial Intelligence Organization, pp. 116–122. ISBN: 978-0-9992411-4-1. DOI: 10.24963/ijcai.2019/17.

Carroll, Lewis (1884). *The Principles of Parliamentary Representation*. Harrison and Sons.

Carrubba, Clifford J. and Craig Volden (2000). “Coalitional Politics and Logrolling in Legislative Institutions”. In: *American Journal of Political Science* 44.2, pp. 261–277. ISSN: 0092-5853. DOI: 10.2307/2669309.

Casella, Alessandra, Aniol Llorente-Saguer, and Thomas R. Palfrey (Aug. 2012). “Competitive Equilibrium in Markets for Votes”. In: *Journal of Political Economy* 120.4, pp. 593–658. ISSN: 0022-3808. DOI: 10.1086/667988.

CBECI (2022). *Bitcoin Electricity Consumtion Comparison*. Tech. rep. The Cambridge Bitcoin Electricity Consumption Index.

Chaum, David (1983). “Blind Signatures for Untraceable Payments”. In: *Advances in Cryptology*. Ed. by David Chaum, Ronald L. Rivest, and Alan T. Sherman. Boston, MA: Springer US, pp. 199–203. ISBN: 978-1-4757-0604-8 978-1-4757-0602-4. DOI: 10.1007/978-1-4757-0602-4_18.

Cila, Nazli et al. (Apr. 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*. Honolulu HI USA: ACM, pp. 1–14. ISBN: 978-1-4503-6708-0. DOI: 10.1145/3313831.3376660.

COALA (2021). *Model Law for Decentralized Autonomous Organizations*. Tech. rep. Coalition of Automated Legal Applications, p. 57.

Coase, R. H. (1937). "The Nature of the Firm". In: *Economica* 4.16, pp. 386–405. ISSN: 1468-0335. DOI: 10.1111/j.1468-0335.1937.tb00002.x.

— (Oct. 1960). "The Problem of Social Cost". In: *The Journal of Law and Economics* 3, pp. 1–44. ISSN: 0022-2186. DOI: 10.1086/466560.

Cole, Daniel H. (2014). "Formal Institutions and the IAD Framework: Bringing the Law Back In". In: *SSRN Electronic Journal*. ISSN: 1556-5068. DOI: 10.2139/ssrn.2471040.

Condorcet, Nicolas de (1785). *Essai sur l'application de l'analyse à la probabilité des décisions rendues à la pluralité des voix*. Cambridge University Press. ISBN: 978-1-108-07799-6.

Corbett, Jon, Logan Cochrane, and Mark Gill (Oct. 2016). "Powering Up: Revisiting Participatory GIS and Empowerment". In: *The Cartographic Journal* 53.4, pp. 335–340. ISSN: 0008-7041, 1743-2774. DOI: 10.1080/00087041.2016.1209624.

Corbett, Jon M. and C. Peter Keller (Dec. 2005). "An Analytical Framework to Examine Empowerment Associated with Participatory Geographic Information Systems (PGIS)". In: *Cartographica: The International Journal for Geographic Information and Geovisualization* 40.4, pp. 91–102. ISSN: 0317-7173, 1911-9925. DOI: 10.3138/J590-6354-P38V-4269.

Coriat, Benjamin (May 2015). *Le retour des communs: & la crise de l'idéologie propriétaire*. les liens qui libèrent. ISBN: 979-10-209-0293-1.

Cossar, Sofía and Paula Berman (2020). *Democracy Earth Foundation Digital Decision-Making Pilots Report*. Tech. rep. Democracy Earth, p. 23.

Cotula, Lorenzo (July 2012). "The International Political Economy of the Global Land Rush: A Critical Appraisal of Trends, Scale, Geography and Drivers". In: *The Journal of Peasant Studies* 39.3-4, pp. 649–680. ISSN: 0306-6150. DOI: 10.1080/03066150.2012.674940.

Cox, Michael, Gwen Arnold, and Sergio Villamayor Tomás (2010). "A Review of Design Principles for Community-based Natural Resource Management". In: *Ecology and Society* 15.4. ISSN: 1708-3087. DOI: 10.5751/ES-03704-150438.

Crawford, Sue E. S. and Elinor Ostrom (Sept. 1995). "A Grammar of Institutions". In: *American Political Science Review* 89.3, pp. 582–600. ISSN: 1537-5943, 0003-0554. DOI: 10.2307/2082975.

Dahl, Robert Alan and Edward R. Tufte (1973). *Size and Democracy*. Vol. 2. Stanford University Press. ISBN: 0-8047-0834-7.

Daian, Phil (Apr. 2021). *Phil Does Security | MEV... Wat Do?*

Daian, Philip et al. (May 2020). "Flash Boys 2.0: Frontrunning in Decentralized Exchanges, Miner Extractable Value, and Consensus Instability". In: *2020 IEEE Symposium on Security and Privacy (SP)*, pp. 910–927. DOI: 10.1109/SP40000.2020.00040.

Danaher, John (Sept. 2016). "The Threat of Algocracy: Reality, Resistance and Accommodation". In: *Philosophy & Technology* 29.3, pp. 245–268. ISSN: 2210-5433, 2210-5441. DOI: 10.1007/s13347-015-0211-1.

Dardot, Pierre and Christian Laval (2015). *Commun: essai sur la révolution au XXIe siècle*. La Découverte-poche. Paris: la Découverte. ISBN: 978-2-7071-8673-7.

Davidson, Sinclair, Primavera De Filippi, and Jason Potts (July 2016a). *Disrupting Governance: The New Institutional Economics of Distributed Ledger Technology*. SSRN Scholarly Paper ID 2811995. Rochester, NY: Social Science Research Network.

— (2016b). "Economics of Blockchain". In: *SSRN Electronic Journal*. ISSN: 1556-5068. DOI: 10.2139/ssrn.2744751.

— (Aug. 2018). "Blockchains and the Economic Institutions of Capitalism". In: *Journal of Institutional Economics* 14.4, pp. 639–658. ISSN: 1744-1374, 1744-1382. DOI: 10.1017/S1744137417000200.

De Filippi, Primavera (Jan. 2015). "Translating Commons-Based Peer Production Values into Metrics: Toward Commons-Based Cryptocurrencies". In: *Handbook of Digital Currency*. Ed. by David Lee Kuo Chuen. San Diego: Academic Press, pp. 463–483. ISBN: 978-0-12-802117-0. DOI: 10.1016/B978-0-12-802117-0.00023-0.

De Filippi, Primavera, Morshed Mannan, and Wessel Reijers (Aug. 2020). "Blockchain as a Confidence Machine: The Problem of Trust & Challenges of Governance". In: *Technology in Society* 62, p. 101284. ISSN: 0160-791X. DOI: 10.1016/j.techsoc.2020.101284.

De Filippi, Primavera and Greg McMullen (June 2018). "Governance of Blockchain Systems: Governance of and by Distributed Infrastructure". In: *COALA*, p. 40.

De Filippi, Primavera and Aaron Wright (2018). *Blockchain and the Law: The Rule of Code*. Cambridge, Massachusetts: Harvard University Press. ISBN: 978-0-674-97642-9.

De Soto, Hernando (2000). *The Mystery of Capital: Why Capitalism Triumphs in the West and Fails Everywhere Else*. First paperback edition. New York, NY: Basic Books. ISBN: 978-0-465-01615-0.

Deininger, Klaus W. (2003). *Land Policies for Growth and Poverty Reduction*. World Bank Publications. ISBN: 978-0-8213-5071-3.

Democracy Earth (2021). https://medium.com/@DemocracyEarth.

Dhillon, Amrita et al. (2019). *Introduction to Voting and the Blockchain: Some Open Questions for Economists*. Tech. rep. 416. Competitive Advantage in the Global Economy (CAGE).

Downs, Anthony (1957). "An Economic Theory of Political Action in a Democracy". In: *The Journal of Political Economy* 65.2, pp. 135–150.

Duhnea, Emil (May 2021). "Public Choice Theory: Reuniting Virginia and Bloomington". In: *Elinor Ostrom and the Bloomington School: Building a New Approach to Policy and the Social Sciences*. Ed. by Adam G. Martin, Jayme Lemke, and Vlad Tarko. Agenda Publishing. ISBN: 978-1-78821-125-3 978-1-78821-123-9. DOI: 10.2307/j.ctv1mvw8wq.

DuPont, Quinn (Nov. 2017). “Experiments in Algorithmic Governance : A History and Ethnography of “The DAO,” a Failed Decentralized Autonomous Organization”. In: *Bitcoin and Beyond*. Routledge, pp. 157–177. ISBN: 978-1-315-21190-9. DOI: 10.4324/9781315211909-8.

DuPont, Quinn and Bill Maurer (June 2015). “Ledgers and Law in the Blockchain”. In: *King’s Review*.

El Faqir, Youssef, Javier Arroyo, and Samer Hassan (Aug. 2020). “An Overview of Decentralized Autonomous Organizations on the Blockchain”. In: *Proceedings of the 16th International Symposium on Open Collaboration*. Virtual conference Spain: ACM, pp. 1–8. ISBN: 978-1-4503-8779-8. DOI: 10.1145/3412569.3412579.

Elliott, Francis and Gary Duncan (Jan. 2009). “Chancellor Alistair Darling on Brink of Second Bailout for Banks”. In: *The Times*. ISSN: 0140-0460.

Elwood, Sarah and Rina Ghose (Mar. 2011). “PPGIS in Community Development Planning: Framing the Organizational Context”. In: *Cartographica: The International Journal for Geographic Information and Geovisualization*. Vol. 38, pp. 83–105. ISBN: 978-0-470-66948-8. DOI: 10.1002/9780470669488.ch8.

Endersby, James W. and Michael J. Towle (Mar. 2014). “Making Wasted Votes Count: Turnout, Transfers, and Preferential Voting in Practice”. In: *Electoral Studies* 33, pp. 144–152. ISSN: 0261-3794. DOI: 10.1016/j.electstud.2013.07.001.

Escoffier, Bruno, Hugo Gilbert, and Adèle Pass-Lanneau (2018). “The Convergence of Iterative Delegations in Liquid Democracy”. In: *CoRR abs/1809.04362*. arXiv: 1809.04362.

— (Dec. 2019). “The Convergence of Iterative Delegations in Liquid Democracy in a Social Network”. In: *arXiv:1904.05775 [cs]*. arXiv: 1904.05775 [cs].

— (Apr. 2020). “Iterative Delegations in Liquid Democracy with Restricted Preferences”. In: *Proceedings of the AAAI Conference on Artificial Intelligence* 34.02, pp. 1926–1933. ISSN: 2374-3468, 2159-5399. DOI: 10.1609/aaai.v34i02.5562.

Eyal, Ittay (May 2015). “The Miner’s Dilemma”. In: *2015 IEEE Symposium on Security and Privacy*, pp. 89–103. DOI: 10.1109/SP.2015.13.

Fan, Xuepeng et al. (May 2020). “Implement Liquid Democracy on Ethereum: A Fast Algorithm for Realtime Self-tally Voting System”. In: *arXiv:1911.08774 [cs]*. arXiv: 1911.08774 [cs].

Farnaghi, Mahdi and Ali Mansourian (Oct. 2020). “Blockchain, an Enabling Technology for Transparent and Accountable Decentralized Public Participatory GIS”. In: *Cities* 105, p. 102850. ISSN: 0264-2751. DOI: 10.1016/j.cities.2020.102850.

Federici, Silvia (2011). “Women, Land Struggles, and the Reconstruction of the Commons”. In: *WorkingUSA* 14.1, pp. 41–56. ISSN: 1743-4580. DOI: 10.1111/j.1743-4580.2010.00319.x.

Fonseca, Felipe et al. (June 2018). “Beyond the Dichotomy between Natural and Knowledge Commons: Reflections on the IAD Framework from the Ubatuba Open Science Project”.

In: *ELectronic PUBlishing* Connecting the Knowledge Commons: From Projects to Sustainable Infrastructure.
Ford, Bryan (Nov. 2014). *Delegative Democracy Revisited*.
— (Mar. 2020). "A Liquid Perspective on Democratic Choice". In: *arXiv:2003.12393 [cs]*. arXiv: 2003.12393 [cs].
Ford, Bryan Alexander (May 2002). "Delegative Democracy".
Frandsen, Annie Gaardsted (Dec. 2002). "Size and Electoral Participation in Local Elections". In: *Environment and Planning C: Government and Policy* 20.6, pp. 853–869. ISSN: 0263-774X. DOI: 10.1068/c0228.
Frey, BrunoS. and Reiner Eichenberger (Jan. 1991). "Anomalies in Political Economy". In: *Public Choice* 68.1-3. ISSN: 0048-5829, 1573-7101. DOI: 10.1007/BF00173820.
Friedman, James W. (Jan. 1971). "A Non-cooperative Equilibrium for Supergames". In: *The Review of Economic Studies* 38.1, pp. 1–12. ISSN: 0034-6527. DOI: 10.2307/2296617.
Frischmann, Brett M., Michael J. Madison, and Katherine J. Strandburg, eds. (Sept. 2014). *Governing Knowledge Commons*. Oxford, New York: Oxford University Press. ISBN: 978-0-19-997203-6.
Frolov, Daniil (Feb. 2021). "Blockchain and Institutional Complexity: An Extended Institutional Approach". In: *Journal of Institutional Economics* 17.1, pp. 21–36. ISSN: 1744-1374, 1744-1382. DOI: 10.1017/S1744137420000272.
Fuchs, Christian and Eva Horak (May 2008). "Africa and the Digital Divide". In: *Telematics and Informatics* 25.2, pp. 99–116. ISSN: 0736-5853. DOI: 10.1016/j.tele.2006.06.004.
Fuster Morell, Mayo (2014). *Governance of Online Creation Communities for the Building of Digital Commons: Viewed Through the Framework of the Institutional Analysis and Development*. SSRN Scholarly Paper ID 2842586. Rochester, NY: Social Science Research Network.
Garmann, Sebastian (Mar. 2017). "Election Frequency, Choice Fatigue, and Voter Turnout". In: *European Journal of Political Economy* 47, pp. 19–35. ISSN: 0176-2680. DOI: 10.1016/j.ejpoleco.2016.12.003.
Gibson, J. Paul et al. (Aug. 2016). "A Review of E-voting: The Past, Present and Future". In: *Annals of Telecommunications* 71.7, pp. 279–286. ISSN: 1958-9395. DOI: 10.1007/s12243-016-0525-8.
Golumbia, David (2015). "Bitcoin as Politics: Distributed Right-Wing Extremism". In: *Moneylab Reader: An Intervention in Digital Economy*. Ed. by Geert Lovink et al. INC Reader 10. Amsterdam: Institute of Network Cultures, pp. 117–131. ISBN: 978-90-822345-5-8.
Green-Armytage, James (2005). *Direct Democracy by Delegable Proxy*.
— (June 2015). "Direct Voting and Proxy Voting". In: *Constitutional Political Economy* 26.2, pp. 190–220. ISSN: 1572-9966. DOI: 10.1007/s10602-014-9176-9.

Gutwirth, Serge and Isabelle Stengers (2016). "Le Droit à l'épreuve de La Résurgence Des Commons". In: *Revue Juridique de l'Environnement* 2016/2, pp. 306–343.

Haefele, Edwin T. (1971). "A Utility Theory of Representative Government". In: *The American Economic Review* 61.3, pp. 350–367. ISSN: 0002-8282.

Hajnal, Zoltan, Nazita Lajevardi, and Lindsay Nielson (Jan. 2017). "Voter Identification Laws and the Suppression of Minority Votes". In: *The Journal of Politics* 79.2, pp. 363–379. ISSN: 0022-3816. DOI: 10.1086/688343.

Hanifatunnisa, R. and B. Rahardjo (Oct. 2017). "Blockchain Based E-Voting Recording System Design". In: *2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA)*, pp. 1–6. DOI: 10.1109/TSSA.2017.8272896.

Hardin, Garrett (Dec. 1968). "The Tragedy of the Commons". In: *Science* 162.3859, pp. 1243–1248. ISSN: 0036-8075, 1095-9203. DOI: 10.1126/science.162.3859.1243.

Hardwick, F. Sheer et al. (July 2018). "E-Voting With Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy". In: *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pp. 1561–1567. DOI: 10.1109/Cybermatics_2018.2018.00262.

Hassan, Samer and Primavera De Filippi (Dec. 2017). "The Expansion of Algorithmic Governance: From Code Is Law to Law Is Code". In: *Field Actions Science Reports. The journal of field actions* Special Issue 17, pp. 88–90. ISSN: 1867-139X.

— (2021). "Decentralized Autonomous Organization". In: *Internet Policy Review* 10.2, pp. 1–10. ISSN: 2197-6775. DOI: 10.14763/2021.2.1556.

Hess, Charlotte (July 2008). *Mapping the New Commons*. SSRN Scholarly Paper 1356835. Rochester, NY: Social Science Research Network. DOI: 10.2139/ssrn.1356835.

Hess, Charlotte and Elinor Ostrom, eds. (2007). *Understanding Knowledge as a Commons: From Theory to Practice*. 1st MIT Press pbk. ed. Cambridge, Mass: MIT Press. ISBN: 978-0-262-51603-7.

Hjálmarsson, F. Þ et al. (July 2018). "Blockchain-Based E-Voting System". In: *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, pp. 983–986. DOI: 10.1109/CLOUD.2018.00151.

Howell, Bronwyn E and Petrus H. Potgieter (2019a). "Governance of Blockchain and Distributed Ledger Technology Projects: A Common-Pool Resource View". In: p. 25.

— (2019b). "Governance of Smart Contracts in Blockchain Institutions". In: *SSRN Electronic Journal*. ISSN: 1556-5068. DOI: 10.2139/ssrn.3423190.

Hughes, Eric (1993). *A Cypherpunk's Manifesto*.

Hutchby, Ian (May 2001). "Technologies, Texts and Affordances". In: *Sociology* 35.2, pp. 441–456. ISSN: 0038-0385. DOI: 10.1177/S0038038501000219.

IIED (1999). *Land Tenure and Resource Access in West Africa: Issues and Opportunities for the next Twenty Five Years*. Tech. rep.

Inoguchi, Takashi (2017). "Theoretical Underpinnings of a Global Social Contract". In: *Oxford Research Encyclopedia of Politics*.

International Business Publications, IBP (Sept. 2018). *Ghana Land Ownership and Agricultural Laws Handbook Volume 1 Strategic Information, Policies, Regulations*. Lulu.com. ISBN: 978-1-4387-5907-4.

Judmayer, Aljosha et al. (2021). "Estimating (Miner) Extractable Value Is Hard, Let's Go Shopping!" In: *Cryptology ePrint Archive* Paper 2021/1231, p. 29.

Kaal, Wulf A. (2018). "Initial Coin Offerings: The Top 25 Jurisdictions and Their Comparative Regulatory Responses". In: *SSRN Electronic Journal*. ISSN: 1556-5068. DOI: 10.2139/ssrn.3117224.

Kahng, Anson, S. Mackenzie, and A. Procaccia (2018). "Liquid Democracy: An Algorithmic Perspective". In: *AAAI*.

Kansanga, Moses et al. (June 2018). "Contested Commons: Agricultural Modernization, Tenure Ambiguities and Intra-Familial Land Grabbing in Ghana". In: *Land Use Policy* 75, pp. 215–224. ISSN: 0264-8377. DOI: 10.1016/j.landusepol.2018.03.047.

Kashyap, Samika and A Jeyasekar (Sept. 2020). "A Competent and Accurate BlockChain Based E-Voting System on Liquid Democracy". In: *2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*. Paris, France: IEEE, pp. 202–203. ISBN: 978-1-72817-091-6. DOI: 10.1109/BRAINS49436.2020.9223308.

Kelkar, Mahimna et al. (2020). "Order-Fairness for Byzantine Consensus". In: *Advances in Cryptology – CRYPTO 2020*. Ed. by Daniele Micciancio and Thomas Ristenpart. Vol. 12172. Cham: Springer International Publishing, pp. 451–480. ISBN: 978-3-030-56876-4 978-3-030-56877-1. DOI: 10.1007/978-3-030-56877-1_16.

Khaqqi, Khamila Nurul et al. (Jan. 2018). "Incorporating Seller/Buyer Reputation-Based System in Blockchain-Enabled Emission Trading Application". In: *Applied Energy* 209, pp. 8–19. ISSN: 0306-2619. DOI: 10.1016/j.apenergy.2017.10.070.

Koblitz, Neal and Alfred J. Menezes (Jan. 2016). "Cryptocash, Cryptocurrencies, and Cryptocontracts". In: *Designs, Codes and Cryptography* 78.1, pp. 87–102. ISSN: 0925-1022, 1573-7586. DOI: 10.1007/s10623-015-0148-5.

Koch, Markus Buhatem (Aug. 2018). *Exploring CryptoKitties — Part 2: The CryptoMidwives*.

Koford, Kenneth J. (1982). "Centralized Vote-Trading". In: *Public Choice* 39.2, pp. 245–268. ISSN: 0048-5829.

Konashevych, Oleksii (June 2017). *The Concept of the Blockchain-Based Governing: Current Issues and General Vision*.

Kroeber, A. L. (1939). *Cultural and Natural Areas of Native North America*. University of California Publications in American Archaeology and Ethnology ;v. 38 xi, 242 p. Berkeley, Calif.: University of California Press.

Kshetri, N. and J. Voas (July 2018). "Blockchain-Enabled E-Voting". In: *IEEE Software* 35.4, pp. 95–99. ISSN: 1937-4194. DOI: 10.1109/MS.2018.2801546.

Lamberty, Ricky, Danny de Waard, and Alexander Poddey (Aug. 2020). *Leading Digital Socio-Economy to Efficiency – A Primer on Tokenomics*. DOI: 10.48550/arXiv.2008.02538. arXiv: 2008.02538 [cs].

Lamport, Leslie, Robert Shostak, and Marshall Pease (July 1982). "The Byzantine Generals Problem". In: *ACM Transactions on Programming Languages and Systems* 4.3, pp. 382–401. ISSN: 0164-0925, 1558-4593. DOI: 10.1145/357172.357176.

Le Roy, Étienne (Dec. 2016). "Des Communs « à double révolution »". In: *Droit et societe* N° 94.3, pp. 603–624. ISSN: 0769-3362.

Lee, Barton E., Daniel J. Moroz, and David C. Parkes (Feb. 2020). *The Political Economy of Blockchain Governance*. SSRN Scholarly Paper ID 3537314. Rochester, NY: Social Science Research Network. DOI: 10.2139/ssrn.3537314.

Lessig, Lawrence (2006). *Code*. Version 2.0. New York: Basic Books. ISBN: 978-0-465-03914-2.

Li, Xiaoqi et al. (June 2020). "A Survey on the Security of Blockchain Systems". In: *Future Generation Computer Systems* 107, pp. 841–853. ISSN: 0167-739X. DOI: 10.1016/j.future.2017.08.020.

Linebaugh, Peter (June 2009). *The Magna Carta Manifesto: Liberties and Commons for All*. ISBN: 978-0-520-26000-9.

Lobo, Hazel J P (2004). "The Risk of E-Voting". In: p. 11.

Luhmann, Niklas (2000). "Familiarity, Confidence, Trust: Problems and Alternatives". In: *Trust: Making and breaking cooperative relations* 6.1, pp. 94–107.

Lumineau, Fabrice, Wenqian Wang, and Oliver Schilke (Mar. 2021). "Blockchain Governance—A New Way of Organizing Collaborations?" In: *Organization Science* 32.2, pp. 500–521. ISSN: 1047-7039, 1526-5455. DOI: 10.1287/orsc.2020.1379.

Lustig, Caitlin et al. (May 2016). "Algorithmic Authority: The Ethics, Politics, and Economics of Algorithms That Interpret, Decide, and Manage". In: *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems*. CHI EA '16. New York, NY, USA: Association for Computing Machinery, pp. 1057–1062. ISBN: 978-1-4503-4082-3. DOI: 10.1145/2851581.2886426.

Madison, Michael, Brett Frischmann, and Katherine Strandburg (Jan. 2010). "Constructing Commons in the Cultural Environment". In: *Cornell Law Review* 95.4, p. 657. ISSN: 0010-8847.

Manski, Sarah (Sept. 2017). "Building the Blockchain World: Technological Commonwealth or Just More of the Same?" In: *Strategic Change* 26.5, pp. 511–522. ISSN: 10861718. DOI: 10.1002/jsc.2151.

Mark, Dino, Vlad Zamfir, and Emin Gün Sirer (May 2016). *A Call for a Temporary Moratorium on The DAO*.

Mayhew, David R. (Dec. 1966). *Party Loyalty Among Congressmen: The Difference Between Democrats and Republicans, 1947–1962*. Harvard University Press. ISBN: 978-0-674-42981-9. DOI: 10.4159/harvard.9780674429826.

McGinnis, Michael and Elinor Ostrom (May 2014). "Social-Ecological System Framework: Initial Changes and Continuing Challenges". In: *Ecology and Society* 19.2. ISSN: 1708-3087. DOI: 10.5751/ES-06387-190230.

McGinnis, Michael D. (Feb. 2011). "An Introduction to IAD and the Language of the Ostrom Workshop: A Simple Guide to a Complex Framework: McGinnis: IAD Guide". In: *Policy Studies Journal* 39.1, pp. 169–183. ISSN: 0190292X. DOI: 10.1111/j.1541-0072.2010.00401.x.

McGinnis, Michael Dean (1999). *Polycentricity and Local Public Economies: Readings from the Workshop in Political Theory and Policy Analysis*. Indiana University, Bloomington Workshop in Political Theory and Policy Analysis: University of Michigan Press. ISBN: 978-0-472-08622-1.

Meijer, David and Jolien Ubacht (2018). "The Governance of Blockchain Systems from an Institutional Perspective, a Matter of Trust or Control?" In: *Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age*. Dg.o '18. New York, NY, USA: ACM, 90:1–90:9. ISBN: 978-1-4503-6526-0. DOI: 10.1145/3209281.3209321.

Migot-Adholla, Shem et al. (Jan. 1991). "Indigenous Land Rights Systems in Sub-Saharan Africa: A Constraint on Productivity?" In: *The World Bank Economic Review* 5.1, pp. 155–175. ISSN: 0258-6770. DOI: 10.1093/wber/5.1.155.

Miller, James C. (Sept. 1969). "A Program for Direct and Proxy Voting in the Legislative Process". In: *Public Choice* 7.1, pp. 107–113. ISSN: 1573-7101. DOI: 10.1007/BF01718736.

Mitchell, Timothy (2002). *Rule of Experts: Egypt, Techno-Politics, Modernity*. Berkeley: University of California Press. ISBN: 978-0-520-23261-7 978-0-520-23262-4.

Morell, Mayo Fuster, J.L Salcedo, et al. (2015). *Value in Commons-Based Peer Production*. Tech. rep. Barcelona.

Morell, Mayo Fuster, Jorge L. Salcedo, and Marco Berlinguer (2016). "Debate About the Concept of Value in Commons-Based Peer Production". In: *Internet Science*. Ed. by Franco Bagnoli et al. Lecture Notes in Computer Science. Cham: Springer International Publishing, pp. 27–41. ISBN: 978-3-319-45982-0. DOI: 10.1007/978-3-319-45982-0_3.

Mueller, Dennis C. (1967). "The Possibility of a Social Welfare Function: Comment". In: *The American Economic Review* 57.5, pp. 1304–1311. ISSN: 0002-8282.

— ed. (1996). *Perspectives on Public Choice: A Handbook*. Transferred to digital print. Cambridge: Cambridge Univ. Press. ISBN: 978-0-521-55377-3 978-0-521-55654-5.

Munger, Michael C. (Oct. 2019). "Tullock and the Welfare Costs of Corruption: There Is a "Political Coase Theorem"". In: *Public Choice* 181.1, pp. 83–100. ISSN: 1573-7101. DOI: 10.1007/s11127-018-0610-9.

Murtazashvili, Ilia et al. (June 2022). "Blockchain Networks as Knowledge Commons". In: *International Journal of the Commons* 16.1, pp. 108–119. ISSN: 1875-0281. DOI: 10.5334/ijc.1146.

Nakamoto, Satoshi (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System". In.

Narayanan, Arvind and Jeremy Clark (Aug. 2017). "Bitcoin's Academic Pedigree: The Concept of Cryptocurrencies Is Built From Forgotten Ideas in Research Literature." In: *Queue* 15.4, pp. 20–49. ISSN: 1542-7730, 1542-7749. DOI: 10.1145/3134434.3136559.

Neumann, John von and Oskar Morgenstern (1947). *Theory of Games and Economic Behavior (Commemorative Edition)*. Princeton University Press. ISBN: 978-0-691-13061-3.

Niskanen, William A. (1971). *Bureaucracy and Representative Government*. Transaction Publishers. ISBN: 978-0-202-36445-2.

Norden, Lawrence and Christopher Famighetti (2015). *America's Voting Machines at Risk*. Tech. rep. Brennan Center for Justive, p. 68.

North, Douglass C. (1990). *Institutions, Institutional Change, and Economic Performance*. The Political Economy of Institutions and Decisions. Cambridge ; New York: Cambridge University Press. ISBN: 978-0-521-39416-1 978-0-521-39734-6.

Nyman, Linus and Juho Lindman (Jan. 2013). "Code Forking, Governance, and Sustainability in Open Source Software". In: *Technology Innovation Management Review* 3.1, pp. 7–12. ISSN: 1927-0321. DOI: 10.22215/timreview/644.

O'Dwyer, Rachel (2015). *The Revolution Will (Not) Be Decentralised*.

Olson, Mancur (1965). *The Logic of Collective Action: Public Goods and the Theory of Groups*. 21. printing. Harvard Economic Studies 124. Cambridge, Mass.: Harvard Univ. Press. ISBN: 978-0-674-53751-4.

Osgood, Ryan (2016). *The Future of Democracy: Blockchain Voting*.

Ostrom, Elinor (1965). *Public Entrepreneurship: A Case Study in Ground Water Basin Management*.

— (1990). *Governing the Commons: The Evolution of Institutions for Collective Action*. The Political Economy of Institutions and Decisions. Cambridge ; New York: Cambridge University Press. ISBN: 978-0-521-37101-8 978-0-521-40599-7.

— (June 1999). "Coping WIth Tragedies of the Commons". In: *Annual Review of Political Science* 2.1, pp. 493–535. ISSN: 1094-2939, 1545-1577. DOI: 10.1146/annurev.polisci.2.1.493.

— (Sept. 2000). "Collective Action and the Evolution of Social Norms". In: *Journal of Economic Perspectives* 14.3, pp. 137–158. ISSN: 0895-3309. DOI: 10.1257/jep.14.3.137.

— (2005). *Understanding Institutional Diversity*. Princeton, NJ: Princeton Univ. Press. ISBN: 978-0-691-12207-6 978-0-691-12238-0.

— (2010). "Beyond Markets and States: Polycentric Governance of Complex Economic Systems". In: *The American Economic Review* 100.3, pp. 641–672. ISSN: 0002-8282.

— (2011a). "Background on the Institutional Analysis and Development Framework". In: *Policy Studies Journal* 39.1, pp. 7–27. ISSN: 1541-0072. DOI: 10.1111/j.1541-0072.2010.00394.x.

— (Oct. 2011b). "Honoring James Buchanan". In: *Journal of Economic Behavior & Organization*. Special Issue on the Work of James Buchanan 80.2, pp. 370–373. ISSN: 0167-2681. DOI: 10.1016/j.jebo.2011.04.002.

Ostrom, Elinor, Arun Agrawal, et al. (1989). *CPR Coding Manual*. Tech. rep. Bloomington: Indiana University.

Ostrom, Elinor, Roy Gardner, and James Walker (Mar. 1994). *Rules, Games, and Common-Pool Resources*. Ann Arbor: The University of Michigan Press. ISBN: 978-0-472-06546-2.

Ostrom, Elinor and Charlotte Hess (2007). "A Framework for Analyzing the Knowledge Commons". In: ed. by Elinor Ostrom and Charlotte Hess. Understanding Knowledge as a Commons: From Theory to Practice. Cambridge, MA: MIT Press, pp. 41–81.

Ostrom, Elinor and James Walker (1996). "Neither Markets nor States: Linking Transormation Processes in Collective Action Arenas". In: *Perspectives on Public Choice: A Handbook*. Ed. by Dennis C. Mueller. Transferred to digital print. Cambridge: Cambridge Univ. Press, pp. 163–180. ISBN: 978-0-521-55377-3 978-0-521-55654-5.

Ostrom, Vincent (1972). *Polycentricity*. Working Paper.

Ostrom, Vincent and Elinor Ostrom (1977). "Public Goods and Public Choices". In: *Alternatives for Delivering Public Services*. Routledge. ISBN: 978-0-429-04797-8.

Ostrom, Vincent, Charles M. Tiebout, and Robert Warren (1961). "The Organization of Government in Metropolitan Areas: A Theoretical Inquiry". In: *The American Political Science Review* 55.4, pp. 831–842. ISSN: 0003-0554. DOI: 10.2307/1952530.

Papadimitropoulos, Vangelis (Oct. 2018). "Commons-Based Peer Production in the Work of Yochai Benkler". In: *tripleC: Communication, Capitalism & Critique. Open Access Journal for a Global Sustainable Information Society* 16.2, pp. 835–856. ISSN: 1726-670X, 1726-670X. DOI: 10.31269/triplec.v16i2.1009.

Parisi, Francesco (Apr. 2003). "Political Coase Theorem". In: *Public Choice* 115.1, pp. 1–36. ISSN: 1573-7101. DOI: 10.1023/A:1022877303100.

Paulin, Alois (July 2020). "Ten Years of Liquid Democracy Research: An Overview". In: *Central and Eastern European eDem and eGov Days* 338, pp. 455–466. ISSN: 2663-9394, 2520-3401. DOI: 10.24989/ocg.338.36.

Pazaitis, Alex, Primavera De Filippi, and Vasilis Kostakis (Dec. 2017). "Blockchain and Value Systems in the Sharing Economy: The Illustrative Case of Backfeed". In: *Technological Forecasting and Social Change* 125, pp. 105–115. ISSN: 0040-1625. DOI: 10.1016/j.techfore.2017.05.025.

Piet, Julien, Jaiden Fairoze, and Nicholas Weaver (Mar. 2022). "Extracting Godl [Sic] from the Salt Mines: Ethereum Miners Extracting Value". In: *arXiv:2203.15930 [cs]*. arXiv: 2203.15930 [cs].

Pilkington, Marc (2016). "Blockchain Technology: Principles and Applications". In: *Research Handbook on Digital Transformations*. Edward Elgar Publishing, pp. 225–253. ISBN: 978-1-78471-776-6. DOI: 10.4337/9781784717766.00019.

Platteau, Jean-Philippe (1995). *Reforming Land Rights in Sub-Saharan Africa: Issues of Efficiency and Equity / Publications / UNRISD*. Tech. rep. Discussion Paper N°60.

— (1996). “The Evolutionary Theory of Land Rights as Applied to Sub-Saharan Africa: A Critical Assessment”. In: *Development and Change* 27.1, pp. 29–86. ISSN: 1467-7660. DOI: 10.1111/j.1467-7660.1996.tb00578.x.

pmcgoohan (Aug. 2014). *Miners Frontrunning.* Reddit Post.

Polanyi, Karl (1944). *The Great Transformation.* New York: Rihehart and Co.

Polanyi, Michael (Dec. 1951). *Logic of Liberty.* Routledge & Kegan Paul PLC. ISBN: 978-0-7100-1962-2.

Posner, Eric A. and E. Glen Weyl (2015). “Voting Squared: Quadratic Voting in Democratic Politics”. In: *Vand. L. Rev.* 68, p. 441.

Potop-Butucaru, Maria (2021). “Blockchains and the Commons”. In: *Networked Systems.* Ed. by Chryssis Georgiou and Rupak Majumdar. Lecture Notes in Computer Science. Cham: Springer International Publishing, pp. 28–44. ISBN: 978-3-030-67087-0. DOI: 10.1007/978-3-030-67087-0_3.

Potts, Jason (Dec. 2018). “Governing the Innovation Commons”. In: *Journal of Institutional Economics* 14.6, pp. 1025–1047. ISSN: 1744-1374, 1744-1382. DOI: 10.1017/S1744137417000479.

Potts, Jason et al. (2021). “An Economic Theory of Blockchain Foundations”. In: *SSRN Electronic Journal.* ISSN: 1556-5068. DOI: 10.2139/ssrn.3842281.

Poux, Philémon, Primavera de Filippi, and Simona Ramos (Dec. 2020). “Blockchains for the Governance of Common Goods”. In: *Proceedings of the 1st International Workshop on Distributed Infrastructure for Common Good.* DICG’20. New York, NY, USA: Association for Computing Machinery, pp. 7–12. ISBN: 978-1-4503-8197-0. DOI: 10.1145/3428662.3428793.

Provenance (Nov. 2015). *Blockchain: The Solution for Transparency in Product Supply Chains.*

Qin, Kaihua, Liyi Zhou, Pablo Gamito, et al. (Oct. 2021). *An Empirical Study of DeFi Liquidations: Incentives, Risks, and Instabilities.* DOI: 10.1145/3487552.3487811. arXiv: 2106.06389 [cs, q-fin].

Qin, Kaihua, Liyi Zhou, Benjamin Livshits, et al. (2021). “Attacking the DeFi Ecosystem with Flash Loans for Fun and Profit”. In: *Financial Cryptography and Data Security.* Ed. by Nikita Borisov and Claudia Diaz. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, pp. 3–32. ISBN: 978-3-662-64322-8. DOI: 10.1007/978-3-662-64322-8_1.

Quan-Haase, Anabel (Aug. 2020). *Technology and Society: Social Networks, Power, and Inequality.* 3rd edition. Don Mills, Ontario,Canada: Oxford University Press. ISBN: 978-0-19-903225-9.

Rae, Douglas W. and Eric Schickler (1996). “Majority Rule”. In: *Perspectives on Public Choice: A Handbook.* Ed. by Dennis C. Mueller. Transferred to digital print. Cambridge: Cambridge Univ. Press, pp. 163–180. ISBN: 978-0-521-55377-3 978-0-521-55654-5.

Rahman, H. M. et al. (2017). "A framework for analyzing institutional gaps in natural resource governance". In: *International Journal of the Commons* 11.2, pp. 823–853. ISSN: 1875-0281. DOI: 10.18352/ijc.758.

Rajagopalan, shruti (2019). "Blockchain and Buchanan: Code as Constitution". In: *James M. Buchanan: A Theorist of Political Economy and Social Philosophy*. Ed. by Richard E. Wagner. 1st edition 2019. Remaking Economics: Eminent Post-War Economists. Cham, Switzerland: Palgrave Macmillan. ISBN: 978-3-030-03080-3 978-3-030-03079-7.

Rawls, John (1971). *A Theory of Justice*. 22. print. Cambridge, Mass: The Belknap Press of Harvard Univ. Press. ISBN: 978-0-674-88014-6.

Reijers, Wessel, Fiachra O'Brolcháin, and Paul Haynes (Dec. 2016). "Governance in Blockchain Technologies & Social Contract Theories". In: *Ledger* 1.0, pp. 134–151. ISSN: 2379-5980. DOI: 10.5195/ledger.2016.62.

Reijers, Wessel, Iris Wuisman, et al. (Sept. 2021). "Now the Code Runs Itself: On-Chain and Off-Chain Governance of Blockchain Technologies". In: *Topoi* 40.4, pp. 821–831. ISSN: 1572-8749. DOI: 10.1007/s11245-018-9626-5.

Richman, Barak D. (2006). "How Community Institutions Create Economic Advantage: Jewish Diamond Merchants in New York". In: *Law & Social Inquiry* 31.2, pp. 383–420. ISSN: 0897-6546.

Rogers, Everett M. (Dec. 2001). "The Digital Divide". In: *Convergence* 7.4, pp. 96–111. ISSN: 1354-8565. DOI: 10.1177/135485650100700406.

Rozas, David, Antonio Tenorio-Fornés, Silvia Díaz-Molina, et al. (2018). "When Ostrom Meets Blockchain: Exploring the Potentials of Blockchain for Commons Governance". In: *SSRN Electronic Journal*. ISSN: 1556-5068. DOI: 10.2139/ssrn.3272329.

— (Jan. 2021). "When Ostrom Meets Blockchain: Exploring the Potentials of Blockchain for Commons Governance". In: *SAGE Open* 11.1, p. 21582440211002526. ISSN: 2158-2440. DOI: 10.1177/21582440211002526.

Rozas, David, Antonio Tenorio-Fornés, and Samer Hassan (Apr. 2021). "Analysis of the Potentials of Blockchain for the Governance of Global Digital Commons". In: *Frontiers in Blockchain* 4, p. 577680. ISSN: 2624-7852. DOI: 10.3389/fbloc.2021.577680.

Sai, Ashish Rajendra, Jim Buckley, and Andrew Le Gear (2021). "Characterizing Wealth Inequality in Cryptocurrencies". In: *Frontiers in Blockchain* 0. ISSN: 2624-7852. DOI: 10.3389/fbloc.2021.730122.

Salame, Richard (Mar. 2020). "Texas Closes Hundreds of Polling Sites, Making It Harder for Minorities to Vote". In: *The Guardian*. ISSN: 0261-3077.

Samuelson, Paul A. (Nov. 1954). "The Pure Theory of Public Expenditure". In: *The Review of Economics and Statistics* 36.4, p. 387. ISSN: 00346535. DOI: 10.2307/1925895.

Schlager, Edella and Elinor Ostrom (1992). "Property-Rights Regimes and Natural Resources: A Conceptual Analysis". In: *Land Economics* 68.3, pp. 249–262. ISSN: 0023-7639. DOI: 10.2307/3146375.

Scopus (2020). *Search Results 'Voting' & 'Blockchain'*. shorturl.at/fmuv6.

Shackelford, Scott and Steven Myers (Nov. 2016). *Block-by-Block: Leveraging the Power of Blockchain Technology to Build Trust and Promote Cyber Peace*. SSRN Scholarly Paper ID 2874090. Rochester, NY: Social Science Research Network.

Shubik, Martin (1970). "On Homo Politicus and the Instant Referendum". In: *Public Choice* 9, pp. 79–84. ISSN: 0048-5829.

Siddarth, Divya et al. (2020). "Who Watches the Watchmen? A Review of Subjective Approaches for Sybil-Resistance in Proof of Personhood Protocols". In: *Frontiers in Blockchain* 3, p. 46. ISSN: 2624-7852. DOI: 10.3389/fbloc.2020.590171.

Siefkes, Christian (Nov. 2013). "The Boom of Commons-Based Peer Production". In: *The Wealth of the Commons: A World Beyond Market and State*. Levellers Press, pp. 289–294.

Snyder, Margaret C. and Mary Tadesse (1995). *African Women and Development: A History*. Johannesburg : London ; Atlantic Highlands, N.J: Witwatersrand University Press ; Zed Books. ISBN: 978-1-85649-299-7 978-1-85649-300-0.

Stratmann, Thomas (1996). "Logrolling". In: *Perspectives on Public Choice: A Handbook*. Ed. by Dennis C. Mueller. Transferred to digital print. Cambridge: Cambridge Univ. Press, pp. 322–341. ISBN: 978-0-521-55377-3 978-0-521-55654-5.

Sullivan, Clare and Eric Burger (2019). "Blockchain, Digital Identity, E-government". In: *Business Transformation through Blockchain: Volume II*. Ed. by Horst Treiblmaier and Roman Beck. Cham: Springer International Publishing, pp. 233–258. ISBN: 978-3-319-99058-3. DOI: 10.1007/978-3-319-99058-3_9.

Swan, Melanie (Jan. 2015). *Blockchain: Blueprint for a New Economy*. "O'Reilly Media, Inc." ISBN: 978-1-4919-2047-3.

Swartz, Lana (2017). "Blokchain Dreams: Imagining Techno-Economic Alternatives After Bitcoin". In: *Another Economy Is Possible: Culture and Economy in a Time of Crisis*. Ed. by Manuel Castells. Malden, MA: Polity, pp. 65–81. ISBN: 978-1-5095-1724-4 978-1-5095-1723-7.

— (July 2018). "What Was Bitcoin, What Will It Be? The Techno-Economic Imaginaries of a New Money Technology". In: *Cultural Studies* 32.4, pp. 623–650. ISSN: 0950-2386, 1466-4348. DOI: 10.1080/09502386.2017.1416420.

Szabo, Nick (Sept. 1997). "Formalizing and Securing Relationships on Public Networks". In: *First Monday* 2.9. ISSN: 13960466. DOI: 10.5210/fm.v2i9.548.

Takabatake, Yu, Daisuke Kotani, and Yasuo Okabe (2016). "An Anonymous Distributed Electronic Voting System Using Zerocoin". In: p. 6.

Tang, Weizhao et al. (May 2022). *Strategic Latency Reduction in Blockchain Peer-to-Peer Networks*. DOI: 10.48550/arXiv.2205.06837. arXiv: 2205.06837 [cs].

Taş, Ruhi and Ömer Özgür Tanrıöver (Aug. 2020). "A Systematic Review of Challenges and Opportunities of Blockchain for E-Voting". In: *Symmetry* 12.8, p. 1328. DOI: 10.3390/sym12081328.

Tideman, Nicolaus (Mar. 1995). "The Single Transferable Vote". In: *Journal of Economic Perspectives* 9.1, pp. 27–38. ISSN: 0895-3309. DOI: 10.1257/jep.9.1.27.

Tiebout, Charles M. (Oct. 1956). “A Pure Theory of Local Expenditures”. In: *Journal of Political Economy* 64.5, pp. 416–424. ISSN: 0022-3808, 1537-534X. DOI: 10.1086/257839.

Toulmin, Camilla et al., eds. (2000). *Evolving Land Rights, Policy, and Tenure in Africa*. Issues / Department for International Development. London: IIED : Natural Resources Institute. ISBN: 978-1-899825-51-6.

Troncoso, Stacco and Ann-Marie Ultratel (2020). *DisCO Elements: Groove Is in the Heart.*

Tullock, Gordon (Dec. 1959). “Problems of Majority Voting”. In: *Journal of Political Economy* 67.6, pp. 571–579. ISSN: 0022-3808. DOI: 10.1086/258244.

— (1972). *Toward a Mathematics of Politics*. 1. ed. Ann Arbor Paperback 187. Ann Arbor, Mich: Univ. of Michigan Press. ISBN: 978-0-472-06187-7 978-0-472-92600-8.

— (1992). “Computerizing Politics”. In: *Mathematical and Computer Modelling* 16.8-9, pp. 59–65.

Tullock, Gordon and Geoffrey Brennan (1981). “Why so Much Stability”. In: *Public Choice* 37.2, pp. 189–204. ISSN: 0048-5829.

Ubink, Janine M. and Julian F. Quan (Apr. 2008). “How to Combine Tradition and Modernity? Regulating Customary Land Management in Ghana”. In: *Land Use Policy* 25.2, pp. 198–213. ISSN: 0264-8377. DOI: 10.1016/j.landusepol.2007.06.002.

Vujičić, D., D. Jagodić, and S. Ranđić (Mar. 2018). “Blockchain Technology, Bitcoin, and Ethereum: A Brief Overview”. In: *2018 17th International Symposium INFOTEH-JAHORINA (INFOTEH)*, pp. 1–6. DOI: 10.1109/INFOTEH.2018.8345547.

Wagner, Richard E., ed. (2019). *James M. Buchanan: A Theorist of Political Economy and Social Philosophy*. 1st edition 2019. Remaking Economics: Eminent Post-War Economists. Cham, Switzerland: Palgrave Macmillan. ISBN: 978-3-030-03080-3 978-3-030-03079-7.

Wan, Shaohua et al. (Nov. 2020). “Recent Advances in Consensus Protocols for Blockchain: A Survey”. In: *Wireless Networks* 26.8, pp. 5579–5593. ISSN: 1022-0038, 1572-8196. DOI: 10.1007/s11276-019-02195-0.

Werbach, Kevin (Aug. 2017). *Trust, But Verify: Why the Blockchain Needs the Law*. SSRN Scholarly Paper ID 2844409. Rochester, NY: Social Science Research Network.

— (2018). *The Blockchain and the New Architecture of Trust*. Information Policy Series. Cambridge, MA: MIT Press. ISBN: 978-0-262-03893-5.

Williams, Robin and David Edge (Sept. 1996). “The Social Shaping of Technology”. In: *Research Policy* 25.6, pp. 865–899. ISSN: 00487333. DOI: 10.1016/0048-7333(96)00885-2.

Williamson, Oliver E. (1985). *The Economic Institutions of Capitalism: Firms, Markets, Relational Contracting*. New York : London: Free Press ; Collier Macmillan. ISBN: 978-0-02-934820-8.

— (1993). “Opportunism and Its Critics”. In: *Managerial and Decision Economics* 14.2, pp. 97–107. ISSN: 0143-6570.

Wood, Gavin (2014a). *ÐApps: What Web 3.0 Looks Like*. http://gavwood.com/dappsweb3.html.

— (2014b). *Ethereum Yellow Paper.*

Xiao, Yang et al. (2020). "A Survey of Distributed Consensus Protocols for Blockchain Networks". In: *IEEE Communications Surveys & Tutorials* 22.2, pp. 1432–1465. ISSN: 1553-877X, 2373-745X. DOI: 10.1109/COMST.2020.2969706. arXiv: 1904.04098 [cs].

Yaga, Dylan et al. (Oct. 2018). "Blockchain Technology Overview". In: *arXiv:1906.11078 [cs]*, NIST IR 8202. DOI: 10.6028/NIST.IR.8202. arXiv: 1906.11078 [cs].

Yavuz, Emre et al. (Mar. 2018). "Towards Secure E-Voting Using Ethereum Blockchain". In: *2018 6th International Symposium on Digital Forensic and Security (ISDFS)*. Antalya: IEEE, pp. 1–7. ISBN: 978-1-5386-3449-3. DOI: 10.1109/ISDFS.2018.8355340.

Yeboah, Eric and Mark Kakraba-Ampeh (2016). *Land Investments, Accountability and the Law: Lessons from Ghana.* IIED Land, Investment and Rights Series. London, UK: International Institute for Environmental and Development. ISBN: 978-1-78431-323-4.

Zufferey, Freddie AS (1986). *A Study of Local Institutions and Resource Management Inquiry in Eastern Central District.* Tech. rep. Land Tenure Center.

Résumé :

Dans cette thèse, j'utilise le cadre conceptuel de l'économie politique et institutionnelle pour analyser le choix collectif et l'établissement de constitutions, c'est-à-dire l'ensemble des règles pour décider des règles, dans les communautés blockchain. J'adopte une double approche avec, d'une part, l'utilisation de la théorie économique classique pour évaluer le processus de gouvernance dans les communautés rassemblées autour d'une blockchain (gouverner la blockchain) et, d'autre part, l'identification de la façon dont les innovations permises par les blockchains peuvent être utilisées pour améliorer la coopération dans les groupes (gouverner avec une blockchain). Ces directions se nourrissent mutuellement : à mesure que nous comprenons mieux les spécificités de la gouvernance des blockchains, nous découvrons dans quelle mesure elles peuvent à leur tour être utilisées pour la gouvernance de ressources partagées dans différents contextes. La principale question abordée dans ce manuscrit est de savoir comment les blockchains peuvent être utilisées pour gouverner des biens Communs.

Le manuscrit est composé de cinq chapitres. Il commence par une revue de littérature discutant les notions mobilisées dans l'ensemble de ma recherche et présente ensuite les quatre articles écrits durant ma thèse. Le premier propose une réponse basée sur les communs au problème actuel de la MEV (Maximal Extractable Value) dans les blockchains telles qu'Ethereum. Il conceptualise la MEV comme une nouvelle forme de *free-riding* et explore comment la théorie des biens Communs éclaire les solutions futures pour faire face à ce problmè. Le deuxième propose une analyse économique (de type Public Choice) de la démocratie liquide et des enjeux associés à une mise en œuvre basée sur la blockchain. Il se concentre en particulier sur les questions d'échelle et conclut que la démocratie liquide peut être pertinente pour de petites communautés homogènes, mais qu'elle ne peut représenter l'intensité des préférences et n'est donc pas adaptée aux grandes communautés. Le troisième article s'interroge sur les changements paradigmatiques qu'implique une gouvernance des Communs basée sur la blockchain, notamment en raison de l'automatisation et de la transparence. Le quatrième article complète ce travail en s'appuyant sur deux articles de recherche fondamentale sur la gouvernance des biens communs basée sur la blockchain et propose un cadre unifié, reposant sur le cadre d'analyse institutionnelle et de développement (Institutional Analysis and Development Framework, IAD) d'Ostrom dans un nouveau contexte technologique. Une étude de cas fictive des biens communs fonciers au Ghana est proposé pour illustrer comment cette IAD améliorée par la blockchain pourrait être utilisée.

Ces quatre articles forment un corpus qui montre que si les blockchains sont un outil puissant pour garantir une certaine confiance dans les opérations quotidiennes de gouvernance d'une ressource, il ne faut pas ignorer les dynamiques en œuvre lorsque ces règles doivent être modifiées. Cela alimente une relation à double sens : les blockchains peuvent introduire la confiance dans des environnement qui en sont dépourvus mais, dans le même temps, elles ont besoin de l'implication de la communauté, de sa confiance et de ses normes pour faire face à aux évolutions du système.

Descripteurs :

Communs, Blockchain, Choix Collectif, DAO, Economie Politique