2019

Ostrom Amongst the Machines: Blockchain as a Knowledge Commons

Herminio Bodon
University of Pittsburgh, hbd52@pitt.edu

Pedro Bustamante
University of Pittsburgh - School of Information Sciences, Students, pjb63@pitt.edu

Marcela Gomez
University of Pittsburgh - School of Information Sciences, mmg62@pitt.edu

Prashabnt Krishnamurthy
University of Pittsburgh, prashk@pitt.edu

Michael J. Madison
University of Pittsburgh - School of Law, madison@pitt.edu

Recommended Citation

Herminio Bodon, Pedro Bustamante, Marcela Gomez, Prashabnt Krishnamurthy, Michael J. Madison, Ilia Murtazashvili, Jennifer B. Murtazashvili, Tymofiy Mylovanov & Martin B. Weiss, *Ostrom Amongst the Machines: Blockchain as a Knowledge Commons*, Working Paper (2019).
Available at: https://scholarship.law.pitt.edu/fac_articles/402

Authors

Herminio Bodon, Pedro Bustamante, Marcela Gomez, Prashabnt Krishnamurthy, Michael J. Madison, Ilia Murtazashvili, Jennifer Brick Murtazashvili, Tymofiy Mylovanov, and Martin B. H. Weiss

Ostrom amongst the Machines: Blockchain as a Knowledge Commons

Herminio Bodon, Pedro Bustamante, Marcela Gomez, Prashant Krishnamurthy, Michael Madison, Ilia Murtazashvili, Jennifer Murtazashvili, Tymofiy Mylovanov, Martin Weiss[1]

Abstract

Blockchains are distributed ledger technologies that allow the recording of any data structure, including money, property titles, and contracts. In this paper, we suggest that Hayekian political economy is especially well suited to explain how blockchain emerged, but that Elinor Ostrom's approach to commons governance is particularly useful to understand why blockchain anarchy is successful. Our central conclusions are that the blockchain can be thought of as a spontaneous order, as Hayek anticipated, as well as a knowledge commons, as Ostrom's studies of self-governance anticipated.

Introduction

Blockchains sprang into existence in 2008 with the introduction of Bitcoin. One of the most innovative features of Bitcoin is its core technology, the blockchain (Nakamoto, 2008). A blockchain is a distributed and shared ledger, where all transactions (i.e., committed entries in a database) in the ledger are stored in a chain of blocks. This chain is ever-growing as new transactions occur, in a network of connected nodes, and are appended to it through the creation of blocks containing multiple transactions. Several broad themes emerged as people engaged more deeply with Bitcoin, including that the underlying technology (blockchains) had utility beyond digital currency, that blockchain was a philosophy as much as a technology and that there were many distinct forms of blockchains, each of which have a unique set of technical, economic, and social characteristics.

[1] Herminio Bodon, Pedro Bustamante, Marcela Gomez, Prashant Krishnamurthy, and Martin Weiss are with the School of Computing and Information of the University of Pittsburgh
Ilia Murtazashvili and Jennifer Murtazashvili are with the Graduate School of Public and International Affairs of the University of Pittsburgh
Michael Madison is with the School of Law of the University of Pittsburgh, and is the Academic Director of the University of Pittsburgh Institute for Cyber Law, Policy, and Security
Tymofiy Mylovanov is with the Department of Economics of the University of Pittsburgh and is Honorary President, Kyiv School of Economics

Corresponding Author: Marcela Gomez <mmg62@pitt.edu>

The concept of “alternative” forms of currencies such as cryptocurrencies has gained a lot of attention not only in academia but also in the government and business domain. Bitcoin is without a doubt one of the main reasons for its popularity. The Bitcoin platform for the exchange of monetary units is often referred to as the first cryptocurrency with commercial success, reaching a maximum market capitalization of over $300 billion dollars in December of 2018 (Coinmarket, 2018). As of this writing, one Bitcoin is worth around $7000.

It is true that cryptocurrencies are the most popular application for the blockchain with an estimated number of users between 2.9 and 5.9 million in 2017 (Hileman 2017). Nonetheless, with the appearance of new blockchains, private and public, platforms such as Ethereum, Hyperledger Fabric, Corda, Ripple, etc., are allowing for other applications to be developed on top of the blockchain. This includes financial applications, notary services, smart contracts, and decentralized autonomous organizations (Peters, 2015). The new developments especially include “smart contracts” in the Ethereum blockchain (Werbach, 2019).

In this paper, we consider governance of blockchain. In the context of blockchains, the term “governance” often refers to the management of technical implementation factors, such as improvements to system software, or changes in the consensus mechanism. But other governance aspects have been addressed as well; for example, Werbach (2019) describes an attack on the Ethereum blockchain known as The DAO in which the governance process involved rolling back transactions (essentially setting the ledger back to an earlier state). In all cases, these governance processes involve interactions between human stakeholders. These contracts respond to changing information in the environment by executing and enforcing (in computer software) the terms of the contract that was defined algorithmically in advance. Thus, blockchains and smart contracts can be seen as a Hayekian “institutional framework” in which market mechanisms can work (Boettke, 2018). Because of the proliferation of blockchains with different characteristics, potential market participants can “shop” across blockchains to find the one(s) that have characteristics most suitable for the transaction(s) they hope to execute (Alston, 2019). In essence, we see this as a realization of competitive development of frameworks of rules, or institutions, that allow exchange (Hadfield, 2017).

We extend the analysis of blockchain governance by suggesting that a Hayekian perspective is especially well suited to explain the spontaneous order of the blockchain but that an Ostromian perspective on the knowledge commons is especially well suited to understand the taxis aspect of the blockchain: the reason why blockchain anarchy is generally successful, as well as its nested relationship to higher-level governance organizations. Together, these perspectives can explain the limits of human ability to design institutions for innovation but also open up the black box of institutional design within the blockchain.

Hayek amongst the Machines

Hayek (1978) contrasted organizational orders with spontaneous orders. Spontaneous orders must be recognizable as an order and a result of purposeful human action, but are not the result of deliberate design. Made orders (taxis) are artificial, deliberately constructed by an individual or group of individuals. Spontaneous orders do not have an author and are not the result of a unified plan devised and enforced by a third party, such as the state (Boettke and Coyne 2005; Pennington 2011). Emergent orders are often challenging to control, and while behavior is governed by rules, the participants may not even be aware of them. These orders in some instances contribute to wealth creation, but in others may be destructive (Martin and Storr, 2008).

The Blockchain, from this perspective, is a spontaneous order. It resulted from purposeful action. There was even a single set of authors of the rules governing the blockchain (in fact, four people who were the “authors” of Ethereum). But the blockchain itself did not have a plan, and it has evolved in ways that reflect a market that changes as a cumulative consequence of many independent activities. It also appears to be one that generates substantial wealth, unlike destructive spontaneous orders, such as a mob or a riot, and may even provide a foundation for improving governance functions of the state, such as providing public goods and services (Munger, 2019).

Blockchain also provides insight into the foundations of exchange in the Great Society, which has as its defining feature anonymity of interactions (Hayek 1988). Blockchain represents a shift from trust in centralized to decentralized entities as a result of technology (Werbach 2019). Indeed, this type of trust, together with incentives stemming from gains in the consensus algorithms, is what prompts participants to engage in peer-to-peer interactions. Nevertheless, the question arising is whether blockchain-enabled trust is sufficient for engaging in complex social interactions that involve the sharing of resources and assets (Pazaitis, DeFilippi, & Kostakis, 2017).

Informal orders have the potential to behave abusively, thus markets for choice are important. One corrective to such challenges is through Hayekian competition, or opportunities for people to choose venues of collective decision-making or exchange (Stringham and Zywicki 2011). One of the features of blockchain is that it allows some choice of forums.

Even though there are aspects of spontaneous order for the Blockchain as an institution, there is some role for design (Bert, Markey-Towler, Novak, and Potts 2018). The Blockchain has within it, islands of conscious power, much like Coasean firms. But unlike the traditional firm, which is now highly regulated and relies on the legal system, much of the blockchain is self-governing. It is therefore useful to consider explicitly the insights of Elinor Ostrom, whose work focused explicitly on the analysis of institutions that lead to successful self-governance in anarchic environments, of which blockchain certainly qualifies, as well as the challenge of separating Blockchain neatly from the state. Ostrom (2010) viewed the concepts of “market” and “state” as too blunt and binary, which is also the idea of “entangled” political economy approaches to blockchain, which considers the blurring of boundaries among the economic, social, and political realms with phenomena such as “crypto-secession” and decentralization over record-keeping functions normally provided by the government (Allen, Berg, and Novak, 2018).

Ostrom Amongst the Machines: The Knowledge Commons

Self-governance is especially important to the blockchain and it has features of a commons. It is also governed by institutions that provide the basis for interaction in political, socio-economic systems, while establishing the social positions that different individuals may occupy according to their rights, obligations and empowerments to act in specific situations (Markey-Towler, 2018). Thus, it is a potentially important application of Elinor Ostrom's (2005, 1990) early work on the commons, which resulted in design principles for effective self-governance of common-pool resources (CPRs). These design principles focused on boundaries, the link between rules and needs, opportunities for participation, and the design of enforcement mechanisms, as well as the nested nature of governance.

Knowledge is not a natural resource and is not necessarily depletable, which is a key feature of a CPR. Yet knowledge in its broadest and most general form, suggests social dilemmas that can be addressed by commons governance, including issues of underproduction, free riding, overconsumption and withdrawal of information, enclosure, inequitable access and distribution, coordination among information producers and users, conflict, deception, congestion (insufficient bandwidth at times of peak demand), pollution (Ostrom and Hess, 2007). Early adaptations of Ostrom's work to knowledge and information resources characterized them as "new" commons (Hess 2008).

More recently, the knowledge commons concept has been developed and applied as a method of researching "constructed cultural commons," a shorthand for shared resources composed primarily of products of the human mind (Frischmann, Madison, and Strandburg 2014; Strandburg, Frischmann, and Madison 2017). The characteristic that distinguishes the "commons" from the "noncommons" is institutionalized sharing of resources among community members (Madison, Frischmann, and Strandburg 2010). One of the key aspects of the knowledge commons as an institution are self-governance, including how self-governance can be linked to other formal and informal governance mechanisms and the constraints on self-governance imposed by technology and other material constraints.

Like Ostrom's earlier work that questioned privatization as a solution to CPR governance, the knowledge commons literature questions simple solutions to the challenge of governing knowledge (Madison, Frischmann, and Strandburg, 2010). Successful distributed commons governance examples, such as open source production and Wikipedia, illustrate cases where knowledge and information are naturally shareable, and where the absence of clear property rights does not inevitably lead to "tragedy" (Madison, Frischmann, and Strandburg 2009). An implication is that knowledge commons research must be an empirical, rather than conceptual, exercise (Frischmann 2013).

The knowledge commons research framework builds on Osrom's Institutional Analysis and Development (IAD) framework, which considers how formal and informal "rules-in-use" constitute an action arena that influence collective outcomes for a group (Ostrom 2005). The knowledge commons framework differs from the IAD framework in that it places less emphasis on depletable CPRs and allows for greater historical contingency, as well as recognizes that forms of knowledge are shaped by a variety of institutional forces, rather than nature. The knowledge commons framework generally begins, intuitively, with the understanding that intangible information and knowledge resources are nonrival, nondepletable public goods. The analysis of the knowledge commons can be summarized with the following clusters of concerns and questions (Frischmann, Madison, and Strandburg 2014):

1. A detailed story of the origins, history, and operation of the commons

2. A description of formal and informal (norm-based) rules and practices regarding distribution and coordination of commons resources among participants, including rules for appropriation and replenishment of commons resources
3. The institutional setting(s), including the character of the regime's possibly being "nested" in larger scale institutions and being dependent on the other, adjacent institutions
4. Relevant legal regimes, including property regimes, that influence the operation of the primarily self-governing institutions
5. The structure of interactions between commons resources and participants and institutions adjacent to and outside the regime
6. Dispute resolution and other disciplinary mechanisms by which commons rules, norms, and participants are policed

The next section describes key features of blockchain governance. We then show how the framework just introduced helps to understand blockchain governance.

Blockchain Governance

Behind most implementations of blockchain we find a shared, replicated, and distributed ledger. The main characteristic of a peer-to-peer (P2P) system is that it allows network users to transfer (i.e., transact) digitized, valuable, and tokenized assets (e.g., cryptocurrencies) at a distance with no need of a central trusted third party.[2] To achieve this decentralization (i.e., no need of a trusted third-party), every user in the blockchain network has a full copy of the transaction ledger and the networked system makes sure every user's copy reflects the current state of the underlying data (Christidis, 2016). This distributed ledger can be seen as a secure form of a database of records (e.g., transactions) with characteristics such as decentralization (any transaction can be conducted in a P2P manner), persistency (all transactions are broadcast to all users in the network), auditability (all entries are verifiable and traceable), immutability (no registered data point can be changed or deleted), and security (all data are cryptographically secure) (Crosby, 2016).

This secure "database" is constructed as a log of records that are batched into time-stamped blocks identified by their cryptographic hash, which creates a unique identifier for each generated block.[3] The new block also contains a pointer to the hash (i.e., unique identifier) of the previous block, also known as the parent block, creating in this manner a chain of blocks, commonly known as the Blockchain (see Fig. 1). The first element in the chain is the genesis block, which is a block with no parent and common to the whole network (Peters, 2015).

[2] In the past, users could transfer assets *face-to-face*. For long distance transactions, users needed to trust a central entity such as a Bank or the Postal Service.

[3] A hash or hash value is the result of a hash function. A hash function is a mathematical algorithm that takes an alphanumeric input to produce an alphanumeric output of a predefined length. The produced messages have hashes that are entirely different for each different input. It is computationally infeasible to generate two inputs that have the same output - essentially rendering the hash value unique.

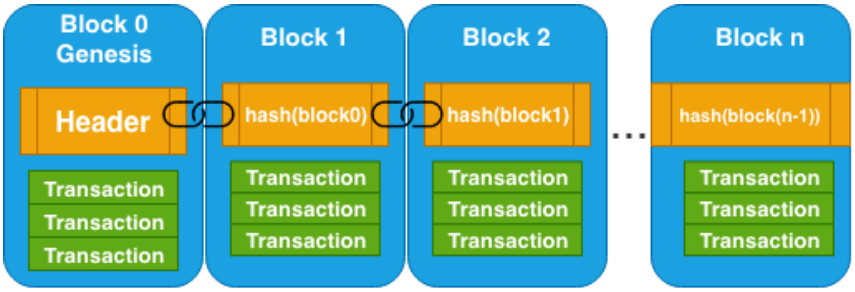

Figure 1: The Blockchain Architecture

In blockchain-based systems we usually find two main components: the transactions and the blocks containing these transactions. The latter is further divided into the block body, and the block header (See Fig. 2). The body of the block contains the transactions and a transaction counter to keep track of the number of transactions to be batched into the block.[4] On the other hand, the header of the block contains additional details regarding the creation of the block. This includes a timestamp (exact date and time of the creation of the block), a *nonce* (arbitrary number to guarantee that transactions are handled only once), the parent block unique identifier (the hash of the previous block), and the Merkle Tree Root (the hash result or fingerprint of the transactions of the block[5]) (Nakamoto, 2017).

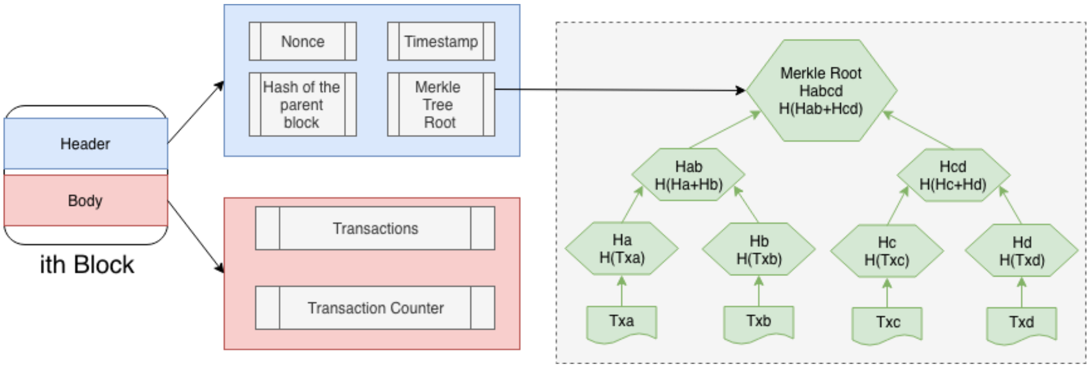

Figure 2: The Blockchain Block

Taxonomy of Blockchain Platforms

The most common way to categorize a blockchain system is according to the access rights to the network. In this manner, blockchain-based platforms are classified into private, consortium, or public. A public or permissionless blockchain, such as Bitcoin or Ethereum, allows any user (usually anonymously or using pseudonyms) to access the network. On the other hand, in a private or permissioned platform, such as Hyperledger Fabric or Corda, only a limited number of

[4] Different blockchain platforms allow different numbers of transactions per block. In the case of Bitcoin, an average of 1,500 transactions are included per block (Decker, 2013).

[5] Single value (i.e., hash) that results from repeatedly digesting (i.e., applying a hashing function to a given input) pairs of transactions until there is one root hash (Gupta, 2017).

users (usually with known identities) can access the network. This allows for identifiable users, where older users exercise access control to the new entrants. Finally, in a consortium or hybrid blockchain platform, instead of allowing any person to participate or allowing a single user/company to have full access control, a few selected nodes perform the most important functions in the network, including access control, as summarized in Table 1.

	Private	Consortium	Public
Access Rights	Permissioned	Permissioned but more flexible	Permissionless
Read Privileges	Restricted	Usually restricted	No restrictions (open)
Immutability Level	Medium	Medium	High
Efficiency	High: Low overhead from the consensus algorithm	High: Low overhead from the consensus algorithm	Low: High overhead from the consensus algorithm
Centralization	Yes	Partial	No
Consensus Algorithm	Pre-approved by nodes	Pre-approved by nodes	PoW, PoS, DPoS,etc.
User's identity	Known identities	Anonymous / Known identities	Anonymous / Pseudonyms
Digital Asset	Any	Any	Platform-native
Platform examples	Hyperledger Fabric, Corda, etc.	Ripple, Multichain, etc.	Bitcoin, Ethereum, etc.

Table 1: Blockchain Taxonomy by Access Rights

Consensus Algorithms in Blockchain

A key characteristic of the Blockchain is that it does not rely on a trusted, centralized entity (e.g., a central bank). Consequently, the network requires a method to ensure nodes agree on the validity of the transactions in each block, and the order in which blocks are appended to the chain. In case of cryptocurrencies, consensus also solves the problem of double spending. Consensus is a critical process in blockchain; otherwise, each user in the network could have a different view of the “state of the world” (Greenspan, 2015). To deal with this problem most Blockchain deployments implement a distributed consensus mechanism (Bach, 2018). Consensus algorithms are a set of rules that ensure a consistent copy of the ledger across the network. Reaching a consensus in the Blockchain is an adaptation of the Byzantine Generals (BG) problem.[6] Nonetheless, it is necessary to point out that the implemented consensus

[6] A group of Generals commanding a part of the Byzantine army have surrounded an enemy camp. However, for an attack to be successful, the majority of the generals need to agree on whether, when, and how to attack. Yet, there may be “traitors” trying to boycott the attack (Lamport 1982).

mechanism in a blockchain platform depends on the type of blockchain (e.g., private vs. public), the network configuration (e.g., known user identities), and the type of digital asset being exchanged (e.g., cryptocurrencies). In fact, the advantages of consensus-based systems (e.g., resistance to censorship, immutable transaction record, etc.) also depend on the characteristics of the blockchain-based platform (Christidis, 2016). Due to the popularity of cryptocurrencies and the considerable amount of applications being developed on top of blockchain-based platforms, a substantial number of consensus algorithms is being developed (Cong, 2019). In what follows, we briefly describe the most popular algorithms in public blockchains and their main characteristics.[7]

Proof of Work (PoW): This is the most widely known consensus algorithm in blockchain due to its utilization in Bitcoin. The goal of the algorithm is to validate transactions so they can be batched into blocks to be appended at the end of the blockchain. In order to append a new block, each node (known as "miners" in Bitcoin) compete to show that it has performed (i.e., mined) some amount of work such as solving a complex mathematical puzzle.[8] The first node to solve the problem appends the block at the end of the chain while being rewarded for the mining process. Other nodes solve the same problem, and consensus is achieved when the nodes that reached the solution vote (by simple majority) to admit the new block to the chain (Nakamoto, 2008). The effectiveness of PoW in the face of dishonest agents was analyzed by Mylovanov and Vohra (2019), who suggest that increasing entry costs or increasing rewards cannot create incentives for these agents to forgo opportunism.

Proof of Stake (PoS): Born as a resource-efficient option for PoW, the main assumption of PoS is that nodes with higher stakes in the network are less likely to harm (i.e., attack) the system. In PoS, users with higher stakes (e.g., ownership of digital assets) have bigger chances to become a validator (i.e., verify the correctness of a block to be attached to the chain) in the "pseudo-random" process used to select a block validator (Pîrlea, 2018).

Many alternative variations of PoS have been proposed in different blockchain-based systems. This includes Delegated Proof of Stake (DPoS), Proof of Weight (PoWeight), Leased Proof of Stake (LPoS), etc. Further, many consensus algorithms have tried to combine the best of two worlds. Thus, new mechanisms are being developed as a hybrid version of PoW and PoS (e.g., Proof of Importance, Proof of Capacity, etc.). All these systems share the core characteristics of PoW and PoS with some variations such as representative democracy, different definitions of stake, single leader selection, among others.

Forks in Blockchain

Forks or branches are a commonly discussed topic in blockchain. From a programming perspective, a fork is an open source modification to the code. In other words, a fork is a new version of the rules that govern the platform. In most cases, the forked code is very similar to the original with important modifications, where the two prongs comfortably co-exist. In the particular case of applications of blockchain such as cryptocurrencies, a fork is usually

[7] Private blockchains also implement versions of consensus algorithms, usually as adaptations of old mechanisms used in other distributed systems (e.g., distributed computing).

[8] In the particular case of Bitcoin, a node has to find a hash value that has to be less than a given target.

implemented to introduce a fundamental change, or to create a new asset with similar characteristics as the original. Nonetheless, it is necessary to point out that not all forks are the result of a change in the version. Due to the distributed and decentralized nature of blockchain, a branch can also happen accidentally. This can happen when not all nodes are replicating the same information, time lags are introduced in the network, two nodes find a block simultaneously, or introduced by malicious nodes (Coindesk, 2018).

In blockchain, we commonly talk about two types of forks: hard and soft (see Fig. 3). Forks however have a shared history. In other words, the log of records on each of the chains is usually identical prior to the split.

Soft Forks: The main characteristic of this type of fork is that newer versions can co-exist with older versions. That is, a change in protocol (e.g., a cosmetic change or adding a new functionality) does not affect the core structure of the platform. New blocks will be accepted by old version nodes (i.e., nodes that are not generating blocks according to the current version of the platform). Nonetheless, the other way around is not true. The newer version would reject blocks created under the old version of the system. This type of amendment generally requires only the majority of miners to upgrade (i.e., majority consensus), which makes it more feasible and less disruptive. Finally, a key characteristic of soft forks is that they do not carry the same potential of double-spending attacks, since both old and new nodes will read both the new and old version blocks (Castor 2017) .

Hard forks: In this type of fork, a change to the protocol of the platform renders the older version invalid[9]. In this light, if nodes continue running an older version, they will end up with a different protocol. Consequently, nodes would have different data than the newer version, which can lead to significant confusion and potential errors. In other words, the software upgrade is not compatible with the older software. Hence, nodes that continue running the old version of the software will see the new transactions as invalid. Consequently, to switch over to the new chain and to continue appending valid blocks to the end of the chain, all of the nodes in the network (i.e., full consensus) need to upgrade to meet the new rules (Liao, 2017).

Hard forks have recently happened in well-known public blockchain platforms such as Ethereum and Bitcoin. It is worth mentioning a couple of examples prior to these well-publicized splits. First, the MintPal hard fork - in 2014, the platform suffered a hack that led to a two million USD tokens being stolen (Higgins, 2014). Due to this problem, developers of the platform reclaimed the funds by introducing a hard fork into the chain. Also in 2014, NXT suffered a hack, which resulted in the theft of $1.75 million dollars. In this case developers also proposed a hard fork to recover the stolen funds, a proposal that was rejected. Instead, most of the funds were recovered through negotiations (Isgur, 2014). These examples show the different approaches taken by blockchain-based platforms dealing with very similar circumstances. Further, it shows that the changes (i.e., forks) introduced in a blockchain platform *are characterized by a relevant governance mechanism*.

Forking includes additional layers of complexity due to the decentralized nature of the system. A change can be initiated by anyone who proposes an upgrade in the protocol. It only

[9] As an example, in Bitcoin, a hard fork would be necessary to change defining parameters such as the block size, the difficulty of the cryptographic puzzle, limits to additional information that can be added, etc.

fully succeeds if the whole network accepts the new upgrade. With every fork, especially hard forks, there is always a risk of a chain split into two halves. Hence, an owner of a cryptocoin, for instance, would receive two new coins. Both currencies then start functioning as separate entities (Arruñada, 2018).

As explained by Arruñada (2018), changes (i.e., splits) in decentralized systems, such as the blockchain, drastically change the incentives with respect to those presented in centralized ones. In blockchain, the platform architect plays a limited role: the nature of the system is that all nodes can unilaterally determine which protocol they run, and whether they update it or not is their decision. Consequently, the challenge for blockchain-based systems lies in developing efficient mechanisms producing “a necessarily ‘soft’ form of governance that takes as given the ultimately decentralized decision-making (via potential splits); but, by promoting the good ‘equilibria,’ ensures efficient nodes’ coordination when adapting to new circumstances.” (Arruñada 2018).

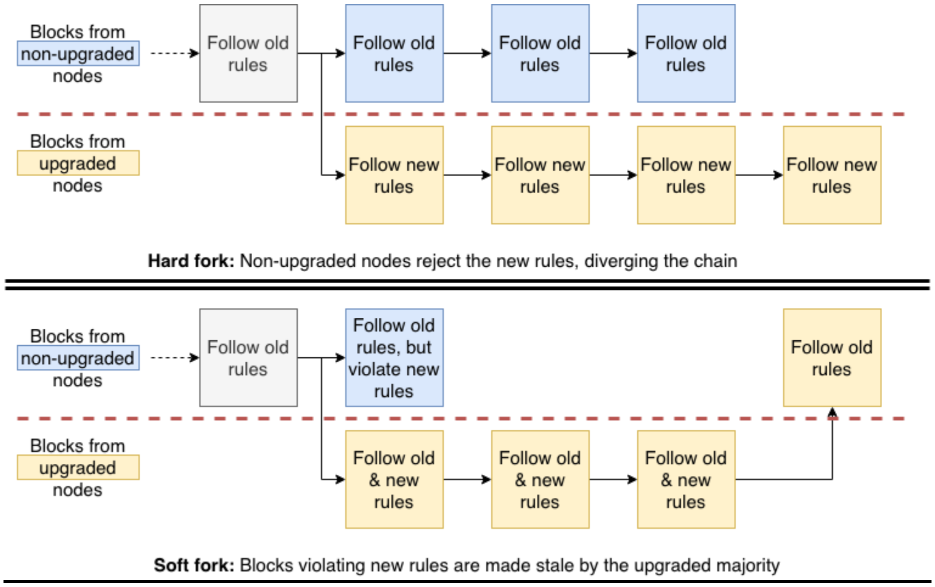
Blocks from non-upgraded nodes
Follow old rules
Follow old rules
Follow old rules
Follow old rules
Blocks from upgraded nodes
Follow new rules
Follow new rules
Follow new rules
Follow new rules
Hard fork: Non-upgraded nodes reject the new rules, diverging the chain
Blocks from non-upgraded nodes
Follow old rules
Follow old rules, but violate new rules
Follow old rules
Blocks from upgraded nodes
Follow old & new rules
Follow old & new rules
Follow old & new rules
Soft fork: Blocks violating new rules are made stale by the upgraded majority

Figure 3: Hard vs. Soft forks in Blockchain

Understanding Blockchain Governance

Based on the discussion above, we concur with Davidson, DiFillippi and Potts 2018 that blockchains are consistent with the institutional context of economic transactions as argued by Mises, Hayek and other Austrian economists (Boettke 2018). Transactions on blockchains are effectively transfers of property rights within that institutional context. As we discussed above, each blockchain may represent a somewhat different institutional context, and may (but need not) represent an evolution (or specialization) of previously existing blockchains; new blockchains may even begin with the same code base (computer software) of a prior blockchain and modify it to implement the new institutional context.

The process of creating a new blockchain is normally the effort of a small team of people who then seek to have their innovation adopted by, and subsequently governed by, the community. In most cases, the "community" consists of transaction validators (miners), software developers, and (typically) transactors with large stakes (coins) on the chain. Governance actions consist of validating transactions and software changes that may result in soft or hard forks. Broadly speaking (but not necessarily), soft forks are upgrades that do not make major changes to the institutional framework created by the blockchain, and hard forks are the result of a change in more fundamental institutional rules.

The Story

The blockchain has features of a commons: congestion, conflict, deception and fraud, efforts to create boundaries, and inequities in who can participate. These inequities are reflected in the intensive demands for understanding mining activities for Bitcoin. There are currently high entry costs and high rewards for mining, but as Mylovanov and Vorhra (2018) explain, this many not be optimal or efficient, as resources are dissipated. Their point is an idea consistent with the knowledge commons, which is that there might be inefficiencies in governance that cannot be solved easily by establishing property rights. In this particular case, this is effectively a race to extract property rights. Blockchains do not have boundaries in the usual sense of institutions and property rights, and there is much freedom for transactors to move from one blockchain to another[10]. Blockchain as an institution is governed by stakeholders (typically miners, or validators) and aligns more closely with the knowledge commons' move away from non-depleting resources. However, there is a clear ability to distinguish blockchains, and some are clearly excludable. For example, permissioned blockchains can alter trust relationships between transacting parties by restricting who may execute transactions on the chain. Thus, it is useful to think of blockchain as a commons, but also one that is not subjected to the challenges of divisibility.

Institutions for Distribution and Coordination

As previously mentioned, the boundaries in blockchain are akin to the knowledge commons' move away from this concept. However, there are important distinctions between blockchains, as Table 1 shows. What is also clear from Table 1 is that rules evolved to satisfy distributional needs. Thus, institutional analysis of blockchains and the institutions of blockchains are highly differentiated. Stil, there is not necessarily as much ability for people to modify rules, as there are no "town halls" in blockchains, especially public ones . In permissioned blockchains, there is more ability to choose, and ability to participate in the blockchain. In addition, for reasons explained above, when there are challenges to the blockchain, the solutions involve working in teams with humans and multiple, overlapping decision-making authority.

[10] Moving from one blockchain to another is not costless. This was discussed in some detail by Alston (Alston, 2019).

Nested-ness

For Ostrom, the terms market and state are restrictive categories that do not include all available forms of governance arrangements. Instead, it is more useful to refer to polycentrism, which involves nesting of markets in higher-level organizations and networks between market and nonmarket participants. Blockchains are nested in higher-level organizations, and there is a blockchain interface with human elements (Werbach, 2019). Governments also regulate blockchain, but they cannot necessarily eliminate self-governance. Blockchain moves to areas where there is less regulatory burden (Berg, Davidson, and Potts, 2018b).

Legal Regimes and Property Rights

There is not a unified system of law governing blockchain. However, there is generalized criminal and common law available. Some blockchains involve permission. For violations, the enforcement would presumably come from a third-party enforcer, including the state. For reasons noted, property rights are also fluid. There is no third party to call on to enforce property rights. This is an additional reason why the commons metaphor is appropriate.

Interactions between Insiders and Outsiders in the Blockchain

One of the features of the blockchain is that it is relatively immune from outside interference. The “cypherpunk” community developed the Bitcoin in part because of this feature and a desire to exist outside of the state (Berg, Davidson & Potts 2018b). It remains challenging for outsiders to come in and destabilize governance, as the blockchain is relatively challenging to control and hard for outsiders to eliminate self-governance. Thus, it is an insider driven system. The freedom from outside interference is why some may view it as a source of constraints on the state, such as by removing challenges with corruption.

Dispute Resolution and Discipline in the Blockchain

Forking is the “dispute” in blockchain. Beyond these issues, it is clear that many disputes can be governed by people. When there are challenges to the blockchain, the solutions involve working in teams with humans and multiple, overlapping decision-making authorities. However, there is not as much discipline beyond choice. However, voting with one’s feet is an important source of discipline. Blockchain allows for local choice, and can be thought of as a crypto-democracy (Allen et al 2018).

Conclusions

In this paper, we sought to demonstrate that the tools offered by scholars such as Hayek, Ostrom and Buchanan provide powerful analytical tools to study blockchains. We have argued that blockchain is best thought of as an institutional context for transactions, and a Hayekian approach provides insight into the unfolding of blockchain and the limits of design. Order, as

Hayek understood, need not come from Leviathan. At the same time, blockchain has rules and features of a commons. It is also nested in a framework of government. Accordingly, it is useful to think of blockchain in the same terms as a knowledge commons.

The Ostroms' work and the public choice literature even suggest a role for blockchain in strengthening the state. Elinor and Vincent Ostrom also eschewed a clear division between "market" and "state" (Aligica 2018). James M. Buchanan (1975) divided the state into protective and productive functions. The blockchain can both constrain and improve the effectiveness of the state, which is a possibility in the Ostroms' framework and even Buchanan's perspective but not as explicit in Hayek's approach. In general terms, we have argued that the blockchain fits Hayek's spontaneous order; however, relying only on such an approach would portray the blockchain as a *mysterious black-box.* Through this analysis, we have leveraged Ostroms' insights to disentangle the different pieces that have turned blockchain into the technology that it is today, with all its applications and potential implications for governance and the state.

References

ALIGICA, PAUL DRAGOS. (2018). *Public Entrepreneurship, Citizenship, and Self-Governance*. Cambridge University Press.

ALLEN, DARCY W., CHRIS BERG, AARON M. LANE, AND JASON POTTS. (2018) "Cryptodemocracy and its institutional possibilities." *The Review of Austrian Economics* : 1-12.

ALLEN, DARCY WE, CHRIS BERG, AND MIKAYLA NOVAK. (2018) "Blockchain: an entangled political economy approach." *Journal of Public Finance and Public Choice* 33, no. 2: 105-125.

ALSTON, E (2019) *CONSTITUTIONS AND BLOCKCHAINS:Competitive Governance of Fundamental Rule Sets* Working paper, Center for Growth and Opportunity, 2019. Retrieved on 22 May 2019 from https://www.growthopportunity.org/research/working-papers/constitutions-and-blockchains

ARRUÑADA, B., & GARICANO, L. (2018). "Blockchain: The birth of decentralized governance".

BACH, L. M., MIHALJEVIC, B., & ZAGAR, M. (2018, May). Comparative analysis of blockchain consensus algorithms. In *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)* (pp. 1545-1550). IEEE.

BARZEL, YORAM. (2002). *A Theory of the State: Economic Rights, Legal Rights, and the Scope of the State*. New York: Cambridge University Press.

BERG, C., DAVIDSON, S, & POTTS, J (2018a) "The Blockchain Economy: A beginner's guide to institutional cryptoeconomics" *Medium* retrieved 22 May 2019 from https://medium.com/@couponone/the-blockchain-economy-a-beginners-guide-to-institutional-cryptoeconomics-9b3581b3e078

BERG, C, DAVIDSON, S & POTTS, J (2018b), Some Public Economics of Blockchain Technology (March 2, 2018). Available at SSRN: https://ssrn.com/abstract=3132857 or http://dx.doi.org/10.2139/ssrn.3132857

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

BERG, CHRIS, MARKEY-TOWLER, BRENDAN, NOVAK, MIKAYLA AND POTTS, JASON. (2018) “Blockchains Evolving: Institutional and Evolutionary Economics Perspectives” Available at SSRN: https://ssrn.com/abstract=3160428

BOETTKE, PETER J. AND CHRISTOPHER J. COYNE. (2005). “Methodological Individualism, Spontaneous Order and the Research Program of the Workshop in Political Theory and Policy Analysis.” *Journal of Economic Behavior & Organization* 57(2):145–58.

BOETTKE, P (2018) *F.A. Hayek* Palgrave Macmillan

BUCHANAN, JAMES M. (1975). *The Limits of Liberty: Between Anarchy and Leviathan*. University of Chicago Press.

CASTOR, AMY. (2017). “A short guide to Bitcoin forks”. *CoinDesk.* Retrieved 06 June 2019 from https://www.coindesk.com/short-guide-bitcoin-forks-explained

COINDESK, (2018), “Hard Fork vs. Soft Fork”. *Coindesk.* Retrieved 06 June 2019 from https://www.coindesk.com/information/hard-fork-vs-soft-fork.

COINMARKET, (2018), “Top 100 cryptocurrencies by market capitalization”

COLE, DANIEL H., GRAHAM EPSTEIN, AND MICHAEL D. MCGINNIS. (2019). Combining the IAD and SES frameworks. *International Journal of the Commons.* 13(1): 244–275.

CONG, L. W., & HE, Z. (2019). Blockchain disruption and smart contracts. *The Review of Financial Studies*, *32*(5), 1754-1797.

CHRISTIDIS, K., & DEVETSIKIOTIS, M. (2016). “Blockchains and smart contracts for the internet of things”. *IEEE Access*, *4*, 2292-2303.

CROSBY, M., PATTANAYAK, P., VERMA, S., & KALYANARAMAN, V. (2016). “Blockchain technology: Beyond bitcoin”. *Applied Innovation*, *2*(6-10), 71.

DAVIDSON, S., DE FILIPPI, P., & POTTS, J. (2018). “Blockchains and the economic institutions of capitalism”. *Journal of Institutional Economics*, 14(4), 639-658. doi:10.1017/S1744137417000200

DECKER, C., & WATTENHOFER, R. (2013, September). Information propagation in the bitcoin network. In *IEEE P2P 2013 Proceedings* (pp. 1-10). IEEE.

ETHEREUM, TEAM, (2017), “Byzantim HF Announcement”. *Ethereum Blog.* Retrieved 05 June 2019 from https://blog.ethereum.org/2017/10/12/byzantium-hf-announcement/

EUSEPI, GIUSEPPE AND RICHARD E. WAGNER. (2010). “Polycentric Polity: Genuine vs. Spurious Federalism.” *Review of Law & Economics* 6(3):329–45.

FRISCHMANN, BRETT M. (2013). “Two Enduring Lessons from Elinor Ostrom.” *Journal of Institutional Economics* 9(4): 387-406.

FRISCHMANN, BRETT M., MICHAEL J. MADISON, AND KATHERINE JO STRANDBURG. 2014. *Governing Knowledge Commons*. Oxford University Press.

HADFIELD, G (2017) *Rules for a Flat World: Why Humans Invented Law and How to Reinvent It for a Complex Global Economy* Oxford University Press

HAYEK, F. A. (1978). *Law, legislation and liberty, volume 1: Rules and order* (Vol. 1). University of Chicago Press.

HAYEK, F.A. (1988) *The Fatal Conceit: The Errors of Socialism*. University of Chicago Press.

HESS, CHARLOTTE. (2008) "Mapping the New Commons" Presented at "Governing Shared Resources: Connecting Local Experience to Global Challenges. *The 12th Biennial Conference of the International Association for the Study of the Commons*. University of Gloucestershire, Cheltenham, England (July 14–18) http://hdl.handle.net/10535/304.

HESS, CHARLOTTE AND ELINOR OSTROM. (2007). *Understanding Knowledge as a Commons: From Theory to Practice*. The MIT Press.

HIGGINS, STAN.(2014). "8 Million Vericoin Hack Prompts Hard Fork to Recover Funds". *CoinDesk.* Retrieved 05 June 2019 from https://www.coindesk.com/bitcoin-protected-vericoin-stolen-mintpal-wallet-breach

HILEMAN, G., & RAUCHS, M. (2017). Global cryptocurrency benchmarking study. *Cambridge Centre for Alternative Finance*, *33*.

ISGUR, BEN. (2014). "The Negotiations Behind the Bter NXT Theft". *CoinReport.* Retrieved 06 June 2019 from https://coinreport.net/negotiations-behind-bter-nxt-theft/

GREENSPAN, G. (2015). Avoiding the pointless blockchain project. *MultiChain, blog*.

GUPTA, S. S. (2017). *Blockchain*. John Wiley & Sons, Inc.

JAVARONE, M. A., & WRIGHT, C. S. (2018). "From Bitcoin to Bitcoin Cash: a network analysis". *arXiv preprint arXiv:1804.02350*.

LAMPORT, L., SHOSTAK, R., & PEASE, M. (1982). The Byzantine generals problem. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, *4*(3), 382-401.

LIAO, K., & KATZ, J. (2017, April). "Incentivizing blockchain forks via whale transactions". In *International Conference on Financial Cryptography and Data Security* (pp. 264-279). Springer, Cham.

MADISON, MICHAEL J., BRETT M. FRISCHMANN, AND KATHERINE J. STRANDBURG (2009) "The University as Constructed Cultural Commons." *Washington University Journal of Law & and Policy* 30(1): 365-403.

MADISON, MICHAEL J., BRETT M. FRISCHMANN, AND KATHERINE J. STRANDBURG. (2010) "Constructing Commons in the Cultural Environment." *Cornell Law Review* 95(4): 657-709.

MARKEY-TOWLER, B. (2018). Anarchy, blockchain and utopia: a Theory of Political - Socioeconomic Systems Organised Using Blockchain. *Available at SSRN 3095343*.

MARTIN, NONA, AND VIRGIL HENRY STORR (2008). "On perverse emergent orders." *Studies in Emergent Order* 1, no. 1 (2008): 73-91.

MUNGER, MICHAEL. (2019). "The Future of Public Goods." https://www.aier.org/article/future-public-goods

MYLOVANOV, TYMOFIY, AND VOHRA, RAKESH (2018). "Corruption is the Path to Security." Working Paper, University of Pittsburgh, Department of Economics.

'NAKAMOTO, P. (2017). *Bitcoin: Ultimate guide to understanding blockchain, bitcoin, cryptocurrencies, smart contracts and the future of money*. CreateSpace Independent Publishing Platform.

NAKAMOTO, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

NORTH, DOUGLASS C. (1990). *Institutions, Institutional Change and Economic Performance*. New York: Cambridge University Press.

OSTROM, ELINOR AND CHARLOTTE HESS. (2007) "A Framework for Analyzing the Knowledge Commons," in Charlotte Hess and Elinor Ostrom eds. *Understanding Knowledge as a Commons: From Theory to Practice.* Cambridge, MA: MIT Press.

OSTROM, ELINOR. (2007) "A Diagnostic Approach for Going Beyond Panaceas." *Proceedings of the National Academy of Sciences* 104(39):15181–15187.

OSTROM, ELINOR (2009). *Understanding institutional diversity*. Princeton University Press.

OSTROM, ELINOR (2010). Beyond markets and states: polycentric governance of complex economic systems. *American economic review*, *100*(3), 641-72.

OSTROM, ELINOR (1990). *Governing the Commons*. Cambridge University Press.

OSTROM, VINCENT. (2008). *The Political Theory of a Compound Republic: Designing the American Experiment*. Lexington Books.

PAZAITIS, A., DE FILIPPI, P., & KOSTAKIS, V. (2017). Blockchain and value systems in the sharing economy: The illustrative case of Backfeed. *Technological Forecasting and Social Change*, *125*, 105-115.

PENNINGTON, MARK. (2011). *Robust Political Economy: Classic Liberalism and the Future of Public Policy*. Cheltenham, UK: Edward Elgar Publishing.

PETERS, G., PANAYI, E., & CHAPELLE, A. (2015). "Trends in cryptocurrencies and blockchain technologies: a monetary theory and regulation perspective". *Journal of Financial Perspectives*, *3*(3).

PÎRLEA, G., & SERGEY, I. (2018, January). Mechanising blockchain consensus. In *Proceedings of the 7th ACM SIGPLAN International Conference on Certified Programs and Proofs* (pp. 78-90). ACM.

STRANDBURG, KATHERINE J., BRETT M. FRISCHMANN, AND MICHAEL J. MADISON eds. (2017). *Governing Medical Knowledge Commons* Cambridge: Cambridge University Press.

STRINGHAM, EDWARD P. AND TODD J. ZYWICKI. (2011). “Hayekian Anarchism.” *Journal of Economic Behavior & Organization* 78(3):290–301.

WERBACH, K (2019) *Blockchains and the New Architecture of Trust* MIT Press.