Can Permissionless Blockchains Avoid Governance?

By: Eric Alston (University of Colorado), Wilson Law (Baylor University), Ilia Murtazashvili (University of Pittsburgh) and Martin Weiss (University of Pittsburgh)

Abstract. Permissionless (or public) blockchain networks provide a new form of decentralized private governance in the digital sphere. The unique nature of permissionless blockchain networks – especially that anyone can participate in them – means the polycentric balance of governance forces to which they are subject merits more granular analysis. We provide a comprehensive typology of the predominant forms of cryptocurrency blockchain governance and discuss their implications for the ongoing development of these novel organizational forms. In our typology, blockchain is governed by a protocol, along with a set of subsidiary, competitive, and superior governance forces. Governance by code includes the constitution of blockchain defined by its consensus mechanism and the possibility for forking. Governance forces subsidiary to the blockchain protocol include distinctions between discrete constituent groups like miners and users, and how protocol choices themselves lead to specific concentrations of power in practice. Moreover, cryptocurrency users have choice in terms of their digital tokens of value, as well as currencies and other liquid stores of value writ large, which means competitive forces also shape governance choices on a given cryptocurrency blockchain. Finally, blockchain is a polycentric enterprise: cryptocurrency users, participants, and exchanges are subject to a variety of governance forces that are superior to a given cryptocurrency network itself; any given individual playing one of those roles is subject to a variety of legal restrictions surrounding property, contract, tax and securities law in whatever jurisdiction they reside, at a minimum. In sum, permissionless blockchains are themselves a discrete form of governance but will nonetheless inevitably be subject to other processes of governance, both subsidiary and superior to the organization whose information is contained on the distributed ledger controlled by a given blockchain protocol.

1. Introduction

Rule-based governance is ubiquitous in groups above a certain size bcause an organization's members tend to reach its decisions through a collective decision-making process.[1] Governance at scale often entails considerably centralized decision-making, perhaps nowhere more so than in the canonical case of the private firm (Alchian and Demsetz 1972). Public governance is also inevitably centralized to a certain extent, though institutions such as democracy and federalism considerably decentralize public authority compared to other forms of government, thereby addressing to some extent the knowledge or information problem confronting government (Aligica, Boettke, and Tarko 2019; Pennington 2011).[2] Regardless of the level of centralization of an organization's authority in the future, the reality is of a world whose interactions are continually increasing in scale and complexity.[3] Governance outcomes in practice are typically characterized by numerous overlapping layers of jurisdictional authority as a result of the inevitable increases in the magnitude and complexity of social processes.

Enter permissionless blockchains and their protocol-based decentralized governance.[4] Permissionless blockchains are what Nakamoto (2008) envisioned when creating Bitcoin: publicly accessible ledgers available to anyone to join. Bitcoin is the best known permissionless blockchain. It is a virtual currency where the processes of issuance and transfer are public and transparent. Simultaneously to maintaining the underlying ledger, miners create bitcoins, which are then used in transactions reflected on the distributed ledger. Unlike all fiat currencies in the modern era, the government has at best a limited role in its value, which is determined primarily by perceptions of the users. The novelty of these cryptocurrencies' organizational structure meant existing law and regulation were, in many instances, ill-equipped to deal with them. Indeed, Bitcoin and Ethereum, two of the largest cryptocurrencies, could not be regulated by the SEC as securities because there is no third-party residual claimant to either of those networks' activities. Because of the structure of permissionless blockchain protocols, all payments from network actions flow to the miners without any residual benefits flowing to the network as a whole. It presents a novel form of private governance that may facilitate impersonal online exchange in ways that have previously been stymied precisely because the blockchain network's performance and changes in the rules occur via a decentralized process that is transparent and open to anyone with the software, internet access, and electricity access.

[1] Though *governance* is necessary under such circumstances, *government* (i.e., formal political decision-making) is not inevitable (Leeson 2011).

[2] Decentralization has costs, such as increasing decision-making costs, at least mechanically (Buchanan and Tullock 1962)m as well as benefits: reducing oppression and corruption and unleashing a host of economic, technological, and institutional innovation (North, Wallis, and Weingast 2009; Acemoglu et al. 2019)

[3] Whether greater centralization is "efficient" depends on comparing the expected gains from deeper integration with a centralized source of authority to the costs of imposing larger-scale government (Leeson 2006; 2014).

[4] Permissioned blockchains, because they can exclude people, are closer to the traditional notion of a firm, and in our view the governance aspects, which still exist, are less interesting than with permissionless blockchains.

Despite the claim to be decentralized and self-governing, we argue that permissionless cryptocurrency blockchains cannot avoid the forces of governance, both external to and within the blockchain networks. The requirement of governance within blockchain arises because the code and rules predictably need to be changed periodically in ways that cannot be anticipated ex-ante. One user might see a system behavior as a bug, but another might see it as a feature because they have different objectives or desire different outcomes. How do protocol changes take place? Who adjudicates disputes related to network processes and rule changes? These conflicts are not too different from a political process with all its pitfalls. Blockchains also promise a complete contract because users must agree on all rules ex-ante (Davidson, De Filippi, and Potts 2018). But rules inherently need to be changed from time to time. Thus, our analysis hinges on the analogy that using a blockchain system is not unlike being a citizen of a country in the sense that each subjects a given individual to a specific polycentric balance of overlapping governance authorities. These layers of institutions resultant from overlapping governance units define a number of distinct, and at times competing, interest groups subsidiary to each blockchain network, as well creates pressure for change within the blockchain. The distinct roles associated with shaping governance outcomes on a given cryptocurrency network create distinct incentives surrounding the outcomes of network processes.

Given that all institutional remedies resultant from collective decision-making are incomplete, governance in complex organizations necessarily involves mechanisms for change over time. And the change is unavoidably nested within, among, and above other governance units. As a system of governance themselves, permissionless blockchains provide a means of decentralized execution and validation of network processes that are defined by the resultant effects on network participants and users' incentives.[5] While the core protocol governance is the consensus mechanism, other direct governance outcomes include the possibility for forking and better user interfaces to broaden blockchain access. Within a given cryptocurrency blockchain network, governance forces subsidiary to the network include the communities involved in drafting protocol updates and how specific protocol design choices create concentrations of political power. Competitive governance also influences outcomes because cryptocurrency networks are constrained by the possibility of exit of participants and users to other alternatives. Finally, in terms of superior jurisdictional authorities, permissionless cryptocurrency participants and users are subject to a variety of laws and regulations due to how cryptocurrencies implicate property, contracts, tax, and securities law. In our analysis here, we detail these predominant forms of cryptocurrency blockchain governance; protocol, subsidiary, competitive, and superior; and discuss their implications for the ongoing development of these novel organizational forms.

2. Incomplete governance as dynamic, costly and polycentric

Public governance often organizes around geospatially delimited jurisdictions to which individuals belong (e.g., counties, cities, states, nations). Private governance tends to involve the

[5] As a payment mechanism, Bitcoin is a distributed payment technology in that it relies not ony on the parties to a transaction, but the network of users, to validate transactions (Luther and Stein Smith 2020); as a decision-making structure, it is decentralized in that the parties participate directly in governance (Craig and Kachovec 2019)

associations that one voluntarily joins (e.g., soccer leagues, churches, employers, etc.).[6] Public governance tends to be centralized and a monopoly of power with a very high cost of joining and leaving the community. In a democracy, especially decentralized democracy (such as federalism), constituents are permitted greater input into the decisions governing future outcomes than in more centralized systems. These systems that facilitate decentralized group input into ongoing decision-making processes and dispute resolution necessarily involve secondary rules (Hart, 1967), and may in part explain the ubiquity of formal constitutions, notwithstanding the wide variety of forms of governments that create these constitutions (Elkins, Ginsburg, and Melton 2009; Law and Versteeg 2013, 2011). Blockchains can themselves be understood as a form of secondary rules shaping and constraining the incentives of network participants and users (Cowen 2019; Rajagopalan 2018; Alston 2020; Berg, Berg, and Novak 2020).

Secondary rules are “the rules about making rules.” Secondary rules define the means by which group decisions will occur, who has the authority to weigh in on those decisions (legislators), who has the authority to implement/enforce those decisions (executives), who has the authority to interpret and apply those rules (judges), and as importantly, how secondary rules get changed (amendment processes). An organization of sufficient complexity that undertakes the costly process of articulating ongoing rules for the process of governance is countenancing that it can neither ex-ante anticipate all the decisions that group governance will entail, but also anticipates a sufficient set of ongoing governance questions to warrant the ongoing costs of organized “government.” This deliberative aspect of an organization is what gives rise to law: if an institution cannot change through a deliberative process, then it cannot be a “law” (Hadfield 2016; Hadfield and Weingast 2014). Thus, for an organization’s rules to be effective, there must be a means in the organization to change them.[7]

Many contracts are implausibly sparse on detail, especially when one considers that they often signify economic relationships worth millions to billions of dollars. This concept of relational contracting emphasizes how our institutions are always imperfect - we live in a highly dynamic, uncertain, and complex world, such that we cannot possibly ex-ante specify all downstream contingencies of relevance to a given commercial relationship.[8] Contracting in the face of complexity means we contract away the unknown tails and dimensions of the probability distribution by simply removing those outcomes from the terms of the contract, rather than believing we can specifically identify them ex-ante. Public governance deals with problems of incompleteness as well because the articulation of rules for future conduct faces the same uncertainty associated with dynamic and complex nature of the world.[9] In the context of interest to us here, the ongoing need for adjustment to blockchain network protocols shows how the

[6] Private governance also enforce and coerce such that they are not fully “voluntary,” such as in criminal organizations or gangs (Skarbek 2014; Leeson 2007).

[7] Ostrom’s (1990) analysis of governance recognized the importance of collective decision-making as one of the criteria for long-standing self-governance of organizations.

[8] For this reason, trust and reciprocity are essential to business relations (Macaulay 1963).

[9] This uncertainty gives rise to the fundamental political dilemma, which is thay any government that can establish the rule of law can violate it (Weingast 1995).

notion of ex-ante defining all possible governance outcomes flies in the face of how governance actually proceeds in practice.[10]

Because of the fact that the need for adjustment is certain, even if the nature of that adjustment is uncertain, organizations and governments tend to have clearly specified rules for how the system itself can be changed. In terms of public governance, a major tradeoff identified in the literature on comparative constitutional design (and practical constitutional drafting procedure) is that associated with how easy or hard a constitution is to amend - rigidity v. flexibility, which indicates the importance of amendment processes for sustainable governance, including in cryptocurrency communities (Alston 2020). The tradeoff between rigidity and flexibility in secondary rules provides comparative certainty of the rules in play at the end of rigidity, but this comes at the cost of being able to change rules to either improve them or adjust to unforeseen circumstances. Practical evidence suggests constitutional flexibility is closely tied to the endurance of a given governance regime; if the regime cannot be adapted by its constituents when there is sufficient need to do so, than better it be discarded due to its rigidity (Elkins, Ginsburg, and Melton 2009). In the context of permissionless blockchains, the need for significant protocol updates, including an upcoming transition of consensus mechanism for the Ethereum protocol, directly indicates that protocol flexibility is a desirable institutional feature.

Huge swaths of governance issues surround the unanticipated harms that result from individuals with diverse preferences pursuing their own objectives in a highly complex and dynamic world. Because it is intrinsically costly, people do not tend to want to dispute, let alone harm, one another. Disputes emerge unexpectedly to one or more parties much of the time - while the law of large numbers can imply that types of disputes emerge at a predictable rate in a population of a sufficient size, the ongoing need for judicial clarification and application of the law to new circumstances emphasizes how necessarily dynamic governance needs to be. It needs to suit the community, which means juries still play a large role in legal outcomes in the U.S. Therefore, the questions that emerge in the process of governance are by definition controversial – universally beneficial actions are almost self-executing by definition, as compared to questions that surround the appropriate limits of individuals' and organizations' actions. This means the resolution of policy issues is costly both mechanically and distributionally. Distributional consequences resultant from collective choice means that the mechanical resolution of this choice is more costly due to strategic behavior within and between groups whose interests oppose one another on one or more issues (De Filippi and Loveluck 2016). In sum, issues that require action on the part of governance authorities, including changing rules or articulating new ones, are intrinsically costly in that they pose gains and losses to members and may be a decision that only a subset of the community views as correct in light of an unforeseen event.

What do disputes look like in permissionless network communities? Advocates of the irreversible nature of permissionless cryptocurrency transactions claim that this feature prevents an important class of ex-post payment disputes that are unavoidable when transactions are facilitated by a third party authority (Nakamoto 2008). Nonetheless, while payments are largely

[10] This issue comes up in research which considers technology as a commons, which in many cases requires the participants to develop rules and institutions on their own (Bustamante et al. 2020; Harris 2018; Potts 2018).

irreversible,[11] a wide variety of governance disputes nonetheless occur, resulting in changes within the networks, as well as provide an ongoing role for legal adjudication in these networks (Werbach 2018b). In this regard, blockchain is a polycentric enterprise, which refers to multiple levels of governance sharing autonomy. Polycentric enterprises are characterized by limited and autonomous prerogatives operating under an overarching set of rules (Aligica and Tarko 2012). Central to this notion of polycentrism is autonomy, as an organization may be decentralized but lack meaningful autonomy (V. Ostrom 1994). This focus on functional autonomy necessarily implicates the distinction between de jure and de facto authority, for as we have noted, formally decentralized regimes are often far from being so in practice (Alston 2020).

Since blockchain is a distributed ledger technology, it meets the autonomy criteria of polycentricity in that outcomes on the blockchain network are greatly influenced by the governance choices of network participants. DAOs, for example, have substantial autonomy. Currencies on platforms such as Ethereum are also autonomous, as well as volatile as a result of that autonomy – there is not much ability of a centralized entity to intervene to provide for such stability, and so the ebb and flow of values is a result on the decisions of countless individuals making decisions deliberately, but without a third party with a formal role in coordinating them. Blockchain also operates under a set of superior governance institutions. In this regard, they are not like the anarcho-capitalist view of institutions arising in the absence of institutions, but operate within a legal framework to handle disputes about blockchain, as well as a regulatory environment that asserts influence over the ability of business to use this technology.

Blockchains are like all other ubiquitous units of social governance in that they articulate clear rules for changing governance processes in the face of future demand to do so. But dynamic governance creates mechanical and strategic costs because the process of change present different costs to different group members, in great part because the right governance choice in the face of new events or information is often unclear, and hence, subject to dispute among group members. Moreover, like most governance units in practice, blockchains are polycentric. Permissionless blockchains' autonomy makes them merit analysis as a governance unit in their own right, but network users and participants compose discrete subsidiary governance units themselves, and are also subject to a variety of forms of governance superior to the blockchain network itself. Before discussing the wide range of governance forces to which cryptocurrency network participants and users are subject, we discuss the aspects of blockchain governance.

3. Decentralized governance by code: permissionless blockchains

Bitcoin, which emerged without lawyers or regulators, offers a system that is more flexible, more private, and less amenable to regulatory oversight, and hence has the potential to disrupt existing payment and perhaps monetary systems (Böhme et al. 2015). Because of the way in which permissionless blockchains provide network governance according to a transparent ruleset, some advocates claim they can replace governments altogether, or that it is itself a novel

[11] Our discussion of the emergence of Ethereum Classic below represents a case where dispute over a set of dishonestly transferred units of Ether led to the primary Ethereum blockchain dialing back its ledger state to just before the DAO hack.

institutional technology alongside governments and firms (Davidson, De Filippi, and Potts 2018; Allen, Berg, and Lane 2019; De Filippi and Wright 2018). Such a perspective tends to conflate the distinction between a given technology revolutionizing certain aspects of public governance as opposed to transforming it writ large (Werbach 2018a). Despite these potential cost-saving benefits in terms of governance, we argue that permissionless cryptocurrency blockchains cannot avoid the forces of governance, both external to and within blockchain networks themselves.

Cryptocurrency networks are private organizations - people can willingly join and depart from them (and currently face quite low exit costs to do so). Nonetheless, these networks' governance structure is decentralized and transparent in a way that the vast majority of private organizations in society do not share. This means anyone with the access to electricity, internet connection, and processing power can become a decision-maker for the given cryptocurrency network, voting on rule changes, and performing costly actions on behalf of the network. Any cryptocurrency miner has the equivalent of legislative, executive, and judicial authority for the permissionless blockchain on which they are operating (Alston 2020). In the realm of currencies, this level of decentralization and (technically) egalitarian access to control to the processes of currency issuance and transactions is unparalleled. Compared to politically controlled processes of currency maintenance and issuance, this makes these structural features of network governance particularly appealing.

Cryptocurrency networks need to provide a system that is tamper-proof on the part of users (payment transfer requests) and participants (resilient processing of these transfer requests). Asymmetric cryptography underlies the ability for users to reliably send (using transfer requests signed by their private key) and receive (by embedding a public wallet key in another user's transfer request) units of value enumerated on the distributed ledger maintained by network participants. As long as a given user maintains the security of their private key, no one else can send units of currency from that user's wallet. In contrast to a centralized process, where a single actor or organization maintains the fidelity of transactions on a given network, permissionless blockchains decentralize this authority, which makes doing so reliably more complex than the processes of network oversight provided by payment systems like banks' demand deposits or Visa's network .[12] On permissionless blockchains, network participants police one another's proposed blocks of new transactions updating the ledger entries surrounding balances in a given cryptocurrency. The means by which different network participants "police" one another's successfully proposed blocks is known as the consensus mechanism – how does the network reach consensus about whether a new set of changes to the ledger should be accepted or rejected? This stands as one of the most important aspects of governance by protocol on permissionless cryptocurrency blockchains, which we discuss in the following section.

4. Governance by Blockchain Protocol

[12] Technically, this challenge is referred to as byzantine fault tolerance, which surrounds how independent network nodes that do not have oversight of one another can be structured to collectively validate one another's messages to the network as reliable or not. A validly proposed block is one containing transaction requests signed with private keys that correspond to wallets containing sufficient balances of network units of value.

A blockchain is a distributed ledger with subsequent entries that update as opposed to overwrite one another. The distributed nature of the ledger coupled with the need to provide sequential updates to prior states requires updates occur in discrete “blocks.” A blockchain is thus a chain of blocks of data that refer back to initial and previously changed ledger states. The means by which a given blockchain network updates ledger states can vary, though. Just as highly centralized political systems permit very little input from their constituents, some blockchain networks are centrally controlled, which means a central authority defines the permissions associated with all network participants and users. In such a context, the means by which the ledger is updated is relatively simple, and is akin to traditional centralized firm governance.

What makes permissionless blockchains unique is that they provide a decentralized process of network governance, both in terms of execution and validation of network processes, but also in terms of governance of the underlying protocol layer. As we have already argued, this protocol layer can be understood to have a constitutional nature vis-à-vis the incentives of network participants and users. However, just as not all constitutional systems contemplate identical political systems in practice, permissionless cryptocurrency blockchains can vary as to the structure of their governance. In the foundational case of bitcoin, the network relies on the use of asymmetric cryptography to secure payment requests, and an algorithm known generally as a consensus mechanism to validate and transmit ledger updates across the network. A payment sender broadcasts a public wallet address to the network in a message signed by their private key permitting release of the transfer amount from their wallet – a valid payment request has been verifiably signed by the user’s private key but does not reveal the private key to the rest of the network. In the blockchain ledger, each unit of bitcoin (and fraction thereof) is like a vector of arrows pointing from block to block to block in the blockchain, going from one wallet to another from its point of origination, creating a quantifiable balance of Bitcoin user’s wallet that always sums to the total Bitcoins in circulation.

If the network is reliably and successfully processing transactions, then why are economies of scale in processing power a bad thing? The first is due to the structural link between processing power and ability to override network rules with sufficient singular or coordinated control of processing power on the network. Nonetheless, those controlling some of the most powerful mining pools have argued that their incentives are well-aligned with the long-term viability of Bitcoin as a store of value and/or payment network.[13] But this requires that atomistic users and smaller network participants effectively trust that the larger mining pools’ incentives are indeed well-aligned, because there is no formal block to their ability to wield their concentrated power for good. If this power were limited to the successful proposal and validation of payment transfers, it would be more squarely tied to the incentives we have described here. But as we have mentioned, network participants also accept or reject proposed updates to the protocol layer itself, which makes concentrations of power also have necessary political

[13] If their costly investments in buildings full of interlinked graphics processor units are to continue yielding returns, the network needs to maintain its integrity as a hyper-reliable ledger. Indeed, the units of value that network participants receive are only valuable to the extent that the network is resilient to double-spending and is sufficiently widely used to generate transaction fees in excess of processing costs once mining rewards have been exhausted.

implications vis-à-vis the form and substance of changes that do occur on the network. In particular, consensus mechanisms and forking shape network participants and users' incentives in discrete and identifiable ways. As network processes become more complex in terms of the scope and form of transactions they facilitate, such as with DAOs or subsidiary transactive networks, the interaction between these different layers of protocol-based governance will become increasingly salient.

a. Consensus mechanisms/Amendment rules paragraph

The technical answer to how the network reach consensus across the numerous distributed copies of the ledger when it comes to a proposed block of potential transfers is called the consensus mechanism, which needs to prevent two types of fraud: (i) original sender tries to send bitcoins they do not have, or have simultaneously spent; (ii) other member of the network alters message when transmitting to rest of network. The way in which a given network confronts these challenges varies in practice, though, a distinction in governance by protocol that will continue to shape observed governance outcomes for permissionless cryptocurrency blockchains.

Currently, the predominant means by which permissionless blockchains reach agreement over proposed changes to the underlying ledger is known as the Proof-of-Work (PoW) consensus algorithm, which is a specific way to delimit and validate the rate and means by which information is added to the network. In the case of Bitcoin, each network participant (miner) races to find a specific type of solution to a cryptographic hash function – plugging in random sets of characters to get a solution that has enough zeros in front. Importantly, due to the nature of the cryptographic hash function, no one can predict ex-ante which characters will generate a result below desired threshold. The conformity of proposed transactions with network rules is the result of Nash equilibrium; each miner has an incentive to update with valid proposed blocks because otherwise they will be working on a network that no one else values – their future attempts to facilitate bitcoin transactions will be fruitless because their ledger does not conform to that of the rest of the network (Nakamoto 2008). It is the value of bitcoin units that provides the incentive to update blockchain with proposed blocks as opposed to double-spending – the moment a network participant proposes a block containing fraudulent transactions, they cannot process transactions for bitcoin users on the blockchain subsequently due to the non-conformity of their ledger. If anyone can successfully control (or coordinate) more than half the computing power on the Bitcoin network at a given time, they can force the acceptance of invalid transactions and potentially result in de facto concentrations of processing power (Craig and Kachovec 2019).

Beyond the de facto concentrations of mining power subsidiary to permissionless blockchain networks, the PoW consensus algorithm suffers from another structural problem – it is electricity intensive by designEach participant is expending electricity as they race to find a solution to the cryptographic hash puzzle, but only one participant successfully adds a proposed block in a given period, which makes the electricity expended by other miners problematic. Advocates of this design argue that this cost is a deterrent to fraudulent network activity, for to even be able to propose a fraudulent block would require the expenditure of a large amount of electricity, and would then be subject to the game theoretic problems detailed previously in terms of acceptance by the rest of the network. But for a payment network that consumes more electricity per single transaction than an average US household consumes in 18 days, this energy intensity is itself seen as a problem by some network participants. This has led to changes to the Ethereum protocol that culminated in a transition away from a PoW system to a new structure called Proof-of-Stake, where network validators will effectively pledge a sufficient amount of Ether in order to process and validate transactions on the network. This stands as a major change to network processes, and is tantamount to changing the entire system of government altogether. Such proposed changes are not without their controversies, though, and in order to understand the dynamics of permissionless blockchain network governance by protocol, the choice set of participants as to whether accept or reject a given network update also plays an important role.

b. Forking

Protocol updates are presented to permissionless cryptocurrency networks with some regularity, and in the case of larger changes to the protocol, network participants are presented with a choice of whether to accept the new protocol update, or continue working on the blockchain governed by the previous set of rules, provided a sufficient number of network participants continue under the old standard. This means of changing the blockchain protocol is called forking. If the changes proposed in the update are sufficiently controversial, enough participants might reject such that there is a viable “fork” to the blockchain, in which case two (smaller) blockchain networks exist where there once was one. This has occurred most famously in the cases of Bitcoin and Ethereum, with forks due to disputes over the right governance choice resulting in Bitcoin Cash and Ethereum Classic, respectively, the origins of which we discuss subsequently.

A number of scholarly and industry commentators have identified forking in permissionless blockchains as a governance innovation, but the notion of forking is not new in information technology. Disputes over the protocol design that will best achieve a network’s objectives in an ongoing sense fundamentally becomes a governance question because of the well-understood phenomena of dynamic uncertainty and the contractual incompleteness it begets. While a given computer (or blockchain) network executes a given protocol with certainty, this does not mean the fit between the network’s protocol as designed and the world in which its applied uses are occurring is not subject to the same problems of uncertainty and incompleteness. Because of this, networks inevitably need protocol adjustments because of defects that have been revealed, or because of changes in the user base or intended outputs of the network. This naturally results in disputes as network participants vary in terms of both their beliefs as to what change is needed, as well as the intended network objectives they preference. A cryptocurrency participant that believes more in the purpose of their chosen network as being a long term store of digital value is likely less concerned about transaction processing time and fees than a participant who thinks the long term purpose of the blockchain should be a payment network. These disputes about the appropriate protocol to achieve network objectives can and do result in distinct schisms to a given blockchain, where one set of cryptocurrency participants support the updated protocol, and another continue to support the original protocol. Ultimately, though, disputes as to the protocol that will best achieve a given network’s objectives are as old as computer networks themselves, as the history of standards setting in the information technology industry clearly indicates.

The economic aspects of standardization are summarized by David and Greenstein (1990), but it is worth considering the development of the local area network (LAN) standards in Committee 802 of the Institute of Electrical and Electronic Engineers (IEEE) in particular. The history of LAN standards has been recorded and analyzed in some detail.[14] In summary, Committee 802 attempted to standardize a single technology. In the early 1980s, the leading candidate was a technology called Ethernet that was developed as a joint project by Xerox, Intel and Digital Equipment Corporation (it was called DIX Ethernet). As the deliberations in the standards committee proceeded, the members of the DIX coalition continued developing and building products and systems based on the DIX parameters. Being an open process, the standards committee considered several approaches, each of which had different sponsors and different technical characteristics. To avoid the building deadlock, the leadership of the committee decided to split the standards efforts into several subcommittees (802.3 for Ethernet-like technologies, 802.5 for token ring technologies, and, eventually, 802.11 for wireless technologies). This is essentially a fork of the standards development process, which resulted in a wide array of products and systems that were offered to consumers. Many of these (e.g., token bus, token ring, FDDI, etc.) are historical footnotes while some (Ethernet and wireless LAN) have persisted in the marketplace. Although beyond the scope of our analysis here, it is likely that network standards were governed by a similar process to that we describe here of competition between networks resulting in differential levels of adoption that eventually led to certain standards carrying the day.

Each of these technologies had different technical features intended to prioritize certain tradeoffs in network processes over other ones.[15] Ethernet uses a medium access control protocol that mimics human conversation: stations have equal rights to transmit anytime the channel is idle, and stop transmitting when two stations end up transmitting at the same time. For these systems, the transmission delay is low when the communications channel is lightly used but grows exponentially as the channel utilization increases. In token passing protocols, stations take turns transmitting; if a station does not have the “token”, they cannot transmit. In these systems, transmission delay is higher than Ethernet when the medium is lightly loaded but increases much more gradually as the network load increases. Furthermore, token passing systems allow for the implementation of priority transmission, something that is not possible in Ethernet.

These distinctions were not random variation on the part of coders – they instead reflected deliberate protocol design choices associated with intended user bases and the tradeoffs that different solutions to communications problems posed. Ethernet was developed with office automation functions in mind, where loads are variable and priority communications is usually not important. It was quickly adopted by the minicomputer (and later, microcomputer community). Token ring was developed by IBM for a more server intensive environment that could see much higher loads, as well as for time critical applications such as factory automation.

[14] For analyses of the development of LAN technologies see Sirbu and Hughes (1986), Weiss and Sirbu (1990), and von Burg and Kenney (2000).

[15] Each network standard also tended to have different sponsors. Each sponsor had different target markets and different applications. Some sponsors also used the standards process to defend their dominant position.

Thus, the ideal of having a single LAN standard was incompatible with the diversity of uses to which this technology would be applied.[16]

As in the case of network standards development, cryptocurrency forking tends to surround heterogeneity, much like secessionist pressure tends to arise within governments as a result from heterogeneity of inhabitants (Alesina and Spolaore 1997; Alesina, Easterly, and Matuszeski 2011). Heterogeneity of constituents is linked to increased benefits of subsidiarity, but given sufficient heterogeneity, entirely discrete governance units might indeed be optimal. Accordingly, heterogeneity is a potential challenge within a permissionless blockchain, and the initial constitutional framework may act like "artificial state" that constrains choice. Given sufficiently distinct visions for how a network should (or should not) be changed, this led to a number of cases where distinct sets of network participants had sufficiently divergent visions for the future of the network that they parted ways and governed transactions for entirely separate networks.

Thus, these governance mechanisms are not limited to realm of theory, although there has been considerable scholarly interest in the process of forking itself (Lee, Moroz, and Parkes 2020). Given the nature by which a fork operates as a form of secession on the part of network participants who choose to follow a separate blockchain from that accepted by the majority of the network, the disagreements surrounding protocol changes are necessarily significant. These disagreements have surrounded functional changes to the permissionless blockchain, such as in the case of Bitcoin and Bitcoin Cash. The slow transaction times associated with the known rate at which blocks are added to the Bitcoin blockchain led some network participants (and users) to believe that Bitcoin would be better off with a larger block size, allowing for a greater number of transactions to be processed simultaneously (Kwon et al. 2019). A predominant number of network participants, however, supported the original Bitcoin protocol, in part due to an existing protocol change (Segwit) designed to deal with scalability issues (Song 2017). Despite being a more technical change, the extent to which the Bitcoin community debated scaling solutions suggests that even technical changes implicate fundamental beliefs on the part of network participants and community.

In the case of Ethereum and Ethereum Classic, these beliefs were implicated even more strongly, because the choice for network participants came down to prioritizing the immutability of network code, or punishing bad actors who had taken advantage of an error in the code for an autonomous organization (DAO) subsidiary to the Ethereum blockchain (Mehar et al. 2019). When malicious actors were able to steal tens of millions in Ether[17] some community members wanted to punish those responsible by dialing back the Ethereum blockchain to the state immediately prior to the attack, while others wanted the lost Ether to serve as a costly lesson and future reminder to network participants and users about the immutability of code (Alston 2020).

[16] To enable devices on different networks to interconnect, the committee adopted the layering approach, which allowed systems on diverse networks to communicate with each other through the use of bridges and routers. This was a part of the IEEE committee's "fork" as well: the IEEE 802.2 standard describes the interconnection of LANs. Even within the dominant Ethernet standard, evolution occurred through the use of different transmission media (so-called physical layers). Interoperability among networks with different standards is also a challenge facing permissionless blockchains, which has consistently been identified since as early 2016 by thinkers such as Vitalik Buterin (2016) and Belchior et.al. (2020).

[17] Estimates of the value vary due to fluctuations in market value.

These forks have been chosen as examples because they surround some of the most prominent (and market-capitalized) cryptocurrencies, but as importantly, the forks resultant in viable cryptocurrency networks in their own rights, for both Bitcoin Cash and Ethereum Classic command market capitalizations in hundreds of millions of dollars respectively (Coinmarketcap.com 2020). This signals that for a sufficient proportion of network participants (and ongoing users), the governance changes that resulted from the forking of the original blockchain were ones worth supporting. More generally, these changes display the unique nature of blockchain forking as a means of resolving competing governance visions among network participants and users.

c. Complex smart contracts and DAOs

Beyond the realm of processing transfers of units of value accounted for on the blockchain's distributed ledger, some permissionless cryptocurrency blockchains also permit more complex arrangements. Ethereum in particular is envisioned as a protocol backbone for a wide variety of applications, with units of Ether being used to "power" the processing of subsidiary networks. Among these subsidiary processes are "smart" contracts, self-enforcing contracts that exist on a blockchain. Decentralized autonomous organizations, once created, exist on a blockchain and are self-sufficient: they can make contracts, create their own assets (digital property) and currency (De Filippi and Wright 2018). DAOs promise to realize digitally the view of firms as a nexus of contracts (Jensen and Meckling 1976), though with potentially very different oversight than the contracts that define economic activity to date. This is because the DAO is governed by the code and trust that users place in it. As envisioned by its designers, the DAO operates via self-executing agreements that remove the need for traditional corporate governance or a centralized, trusted third party. DAO can enter contracts with other individual and machines, with rules that are determined beforehand and not subject to manipulation. As we've already discussed though, the first operationalization of a DAO led to major schism within the Ethereum blockchain due to the theft of a large amount of Ether that resulted. For our purposes, though, it is worth noting that as contractual and organizational process complexity increases on a given blockchain, the need for governance is also likely to increase due to the inability to predict all possible contingencies ex-ante. Governance is necessarily dynamic, such that while certain transactional processes can be made autonomous, the nexus between permissionless blockchain processes and the incentives of their users will inevitably need governance, as our analysis here argues throughout. Ultimately, a given cryptocurrency blockchain's governance dynamic are greatly defined by its protocol design choices, which include its consensus mechanism and the possibility of forking to better accommodate heterogeneity of network participants.

5. Governance Subsidiary to a Cryptocurrency Blockchain

For permissionless cryptocurrency blockchains (like most governance systems), the fit is imperfect between organization objectives and the rules and roles articulated to achieve those objectives. Thus, the specific protocol choices on the bitcoin network, for example, have resulted in considerable centralization of network control, as well as different groups with competing visions as to the extent and way in which the bitcoin network should adjust in medium term. These updates, when they occur, need to be coded and tested long before they are deployed on a given cryptocurrency network, which means the communities that develop and test protocol updates themselves play an important role in governance outcomes. Despite the variance in the process by which protocol updates are created, it is apparent that governance subsidiary to a given cryptocurrency blockchain – the effectiveness of the process by which a community generates protocol improvement proposals – is itself a margin by which various cryptocurrencies compete.

Institutional scholars have long recognized the distinction between the de jure rules, which are articulated by a given authority, and de facto rules, which are rules in use in a given context subject to the institution in question (E. Ostrom 2005). This means the extent to which a potentially highly decentralized system is decentralized in practice can vary quite widely (Hooghe et al. 2016). Unsurprisingly, this outcome has also occurred in the context of permissionless cryptocurrencies. The means by which the bitcoin network achieves decentralized agreement as to proposed changes to the currency ledger (and proposed changes to the protocol layer as well) gives a significant advantage to network participants (miners) with huge levels of processing speed (and cheap electricity to power the graphics processors that can most efficiently solve the cryptographic hash function). This has resulted in a few major mining pools exerting a significant amount of control over network governance, although importantly some of these pools have made public statements intended to bolster confidence in the level of power they hold over network outcomes (De Filippi and Loveluck 2016).

This outcome can be thought of as akin to the two-party system (resultant from first-past-the-post single-member geographic districts per Duverger's Law) and the extent to which it is representative of all constituents' preferences. Specific political institutions in the United States' otherwise decentralized political system have centralized power, dominance of two political parties. The consensus algorithm on a technically decentralized blockchain network can also result in considerable centralization of authority. Protocol design can only foresee so many downstream outcomes relevant to the intended objectives of network designers originally and participants in an ongoing sense.

In contrast to the centralization of authority and opposing interests that a given blockchain creates, another major form of off-chain governance is the coding of protocol updates. This process responds to network participants' input as to changes that are needed, and is like constitutional amendment drafting in the context of public governance. But in the case of Ethereum at least, major protocol updates are tested before they're ever released to the network, something which has delayed the network's long-forecast change in consensus algorithm. Both the coding of the protocol update, but also the testing in a firewalled test blockchain are forms of governance external to the blockchain itself, but which greatly shape outcomes on-chain. The most significant structural change to the Ethereum blockchain (and one of considerable interest to cryptoinstitutional scholars) is that of moving away from a proof-of-work to a proof-of-stake consensus algorithm. Given the importance of such a change, and likelihood that the implementation of the consensus mechanism will require ongoing adjustment, has led the Ethereum community to develop a separate blockchain called the "beaconchain," a blockchain whose genesis will occur when a sufficient number of network validators have pledged the Ether required to be a validator on the new network. These significant changes, and the roles that core developers and network figureheads play in their development and advertisement to the broader network, are governed by a specific process on cryptocurrency networks. This is prior to the stage at which protocol updates are "voted" on by network miners as to whether they will govern the blockchain going forward.

The means by which protocol updates are drafted vary considerably from cryptocurrency to cryptocurrency. Nonetheless, in most cases there is a publicly defined process by which updates to network protocols are proposed, coded, discussed, and formally subjected to a "vote" by network miners. Where more variance results surrounds the extent to which anyone can draft, comment upon, or authorize protocol updates that then appear on a given network to be subject to "voting" via the consensus algorithm (or forking in the event there is sufficient disagreement as to the desirability of the update). Ethereum has a public process by which proposals can be submitted, and anyone can submit an EIP to the specific location hosted by the Ethereum Foundation. The procedure by which an EIP will proceed is defined quite granularly, including a number of distinct proposal types corresponding to the scope and magnitude of the change to the Ethereum protocol, as well as a specific structure that each proposal must take. In contrast, Bitcoin improvement proposals are submitted to an email listserv and then posted by Bitcoin developers on a public Github page. While the Ethereum protocol structure results in a more uniform format of protocol proposal, the two fora maintain proposals (and stages of proposal acceptance within the core development community) that present similar information for the larger development community considering the need for a given change and the extent to which a specific protocol update will achieve it.

As in other aspects of permissionless blockchain governance, the creation of protocol updates displays concentrations of authority along a variety of lines. In some communities, such as Ethereum or Litecoin, founders play a special role in advocating for major network changes or as gatekeepers to the development community itself. Each case we survey here also displays the extent to which technical skill is a requisite for participation, for the ability to code a viable protocol update is a minimum requirement for successful proposal. This technical bar has led to some measure of ex-ante filtering of proposals, a process which intrinsically concentrates some measure of governance authority.[18] As is evident from the proposed and accepted proposals in the case of Bitcoin[19] and Ethereum,[20] a small group of individuals plays a large role in proposing updates to the blockchain protocol for each cryptocurrency.

There are interesting structural parallels between the process of protocol improvement proposals and those allowing public input to fundamental governance processes more generally. The notice and comment period for regulation, the ability of third parties to submit amicus briefs, and public consultation processes more broadly all provide a variety of governance benefits.[21] Similarly, in permissionless cryptocurrency communities, there is considerable discussion surrounding the intended benefits a given proposal will provide, which tends to track the

[18] Need to verify if any community makes public proposals that are not provided for public comment.

[19]

[20]

[21]

magnitude of change the proposal entails for the network itself.[22] Nonetheless, where cryptocurrency governance varies from governance more broadly is in the concentration of community debate ex-ante. In contrast to public comments on regulatory or judicial processes, which surround the administration or application of a law that has already been enacted, “enactment” is necessarily final for a given blockchain.

6. Competitive governance of cryptocurrency blockchains

One distinguishing feature of the blockchain governance from public governance is that it is subject to the constraints of market structure and competition. When citizens do not like policies, they can participate in the formal process of changing the rules, or move elsewhere – each costly options. Similarly, it is costly as well for typical cryptocurrency users to make a change in the system. However, a cryptocurrency is only one among numerous digital currencies, not to mention competing stores of value and other mediums of exchange such as fiat currencies, gold, and highly liquid financial instruments. Blockchain networks that serve the same market are effectively competitors. Users can move to a better-governed network with relative ease. The platform developers, miners, and some members in the network communities have concentrated power in governing the systems. However, their fortune is tied to the values of the cryptocurrencies, and its value is a function of the size of the user base. Therefore, the threat of exit from the users constrains and incentivizes the network’s governance to compete for and retain users. This exit strategy has long been recognized as a critical margin of governance (Hirschman 1970), and is also deemed the ability to vote with one’s feet (Somin 2020). The nature of this competition creates another channel of influence in governance, but it does not necessarily produce, in a broadly defined term, better governance.

In the terminologies of industrial organization in economics, competition can present itself in the vertical (quality) dimension or the horizontal (product differentiation) dimension (Hotelling 1929). When products are highly substitutable for each other, they compete in the quality dimension. In the context of cryptocurrency, quality can include the ease of exchange with others, the stability of values, fees, and other concerns. In particular, the ease of exchange increases with the network size (or user base). This attribute can lead to market consolidation. The cryptocurrency market is currently dominated by Bitcoin (65%) and Ethereum (10%), who jointly comprise about 75% of the market capitalization, according to CoinMarketCap.[23] It is a piece of suggestive evidence that market power potentially dominates other features in this market. However, many cryptocurrencies are differentiating themselves as different products. For example, anti-inflationary protocol design choices are central to the design of Bitcoin. The choice of a firm upper limit on the number of bitcoins in circulation can be understood as a response to fiat currencies in which unelected central bankers control the monetary rules. In response to the volatility of coin prices, Tether offers a digital currency that is pegged to the U.S.

[22] In the case of EIPs, a change that only affects a subsidiary is obviously orders of magnitude less important than a change to the consensus mechanism itself, and such changes are accordingly treated quite differently. Indeed, in the latter case, a test chain is intended to be deployed to allow for transparent implementation of the changes before they go live on the Ethereum network in its entirety.

[23] Market capitalization as of Tue, 16 Jun 2020 19:00:00 UTC on CoinMarketCap.com.

dollar and backed by traditional currency reserves. Ethereum provides a rich programming environment to support smart contracts and DAOs. Whether these competing features are in the quality dimension or product differentiation dimension is a separate future research topic, but the evolution of these markets has critical implications for their governance.

Generally speaking, in pursuing more users, networks might pursue shorter-term goals or easily observed features, rather than longer-term and more beneficial policies that are harder to measure. More specifically, in markets where digital currencies are highly substitutable, market forces tend to consolidate the networks into a natural monopoly as much as the technology allows. Even if current technology might not allow a single provider to dominate the market, the market forces may speed up the development of new technology or new rules. As the number of dominant players decreases, the constraints in governance from the competition will relax over time. The systems might not be as sensitive to the users' priorities as before. Alternatively, the market may develop products that are only weakly substitutable because a diversity of governance approaches satisfies users of different needs. Their governance may be constantly constrained by competition. If the networks provide a competing service to the public system, their adoption and experience might even serve as feedback to the governance of the public system.

This cost of exit is quite low currently for cryptocurrency network participants, but a concern associated with low exit costs is that it gives community members a lower stake in participating in the costly processes of collective decision-making. Having skin in the game actually improves incentives when it comes to participating in the costly processes of governance. This incentive to free-ride on the political contributions of others ("rational ignorance" or "rational inaction") is certainly present in blockchain communities - early DAO designers were dismayed by the actual levels of participation in investment decisions, investment decisions that directly implicated valuable funds of members who did not vote on their allocation.

Low exit and entry costs facilitate development of new communities and new institutions for collective decision-making, but the viability of a network requires a sufficient number of actively contributing members. Too many blockchains governing too many cryptocurrencies, while generating potential competitive benefits due to the institutional diversity it foments, may ultimately destroy the usefulness of the networks, or present a serious risk in the collapse of the ecosystem back to a core set of tokens. All of this depends on community members being informed about and participating in the governance processes to which they are subject.

All this being said, easy exit may not be as costly as it seems in theory. An interesting strand of research in finance shows how the threat of exit of shareholders actually operates as a constraint on firm governance, even when that threat is purely passive. Increases in market liquidity (which correspond to an easier ability to "exit" a publicly traded firm by selling shares) have been linked increased participation in governance by activist and passive large shareholders. This allows for a form of specialization, in which certain funds engage actively in the processes of governance in the firms in which they acquire a stake, while others arguably use the passive threat of a large shareholder's exit to induce better governance (Edmans, Fang, and Zur 2013). This split between two classes of stakeholders with the ability to exit a given cryptocurrency network is interesting, because it corresponds directly to the difference in influence that cryptocurrency network participants have as against users. While participants actively vote on updates to the governance structure of the network, and facilitate ongoing network processes, users only have the ability to exit the cryptocurrency network when it comes to influencing governance processes.

7. Superior governance of cryptocurrency blockchains

Blockchain is also subject to superior governance forces. While permissionless cryptocurrencies may not be structured like typical private organizations, their network participants and users are nonetheless subject to a variety of law and regulation due to the ways in which cryptocurrencies implicate property, contracts, tax, and securities law. Blockchain reduces contracting costs, thereby reducing the demand for lawyers – hence, increasing access – though the costs are shifted to up front contracting, such as the extent interfaces are easily accessible. Yet even if contracts are self-enforcing, there will inevitably be disputes. Such considerations have led to calls for *lex cryptographia* – a flattening of law to adapt to a changing environment (Hadfield 2016; Hadfield and Bozovic 2016; Werbach 2018b).

There are several aspects that suggest law is indeed evolving to a polycentric relationship with blockchain. Some of the central ones include property law, contract law, securities and taxation regulation, as well as private governance; exchanges, funds, securities, and interoperability protocols. Although it is outside the scope of our analysis here to treat the wide range of ways in which stores of economic value (even when possessing the relatively novel structure of a cryptocurrency vehicle) are governed by existing law, a few examples suffice to motivate our overarching point that these network processes are nonetheless subject to superior forms of public institutional governance. Although obviously dependent upon the jurisdiction in which a given cryptocurrency user, participant, or exchange is domiciled, cryptocurrencies obviously invoke questions of property law. One salient concern surrounds the ownership of a digital store of value – what serves as the valid proof of "title" over a given unit of cryptocurrency? Courts have tended to identify control of private wallet keys as equivalent to ownership in a traditional property sense, which has important implications for the extent to which users of major exchanges like Coinbase actually own their investments held by the exchanges. Obviously, the automated execution of contractual terms has important implications for contract law (Werbach and Cornell 2017; Governatori et al. 2018), and only more so as increasingly complex transactions are implicated by the workings of DAOs and other applications subsidiary to a given blockchain network. Of course, stores of economic value used as investments and a backbone for ongoing economic activity by an identifiable organization are not without their implications for tax and securities law. Any gains resultant from a holding of a cryptocurrency are subject to tax law in the vast majority of jurisdictions (Prewett, Dorsey, and Kumar 2019), although the tax status of the rewards for mining cryptocurrencies remains less settled (Yalaman and Yıldırım 2019). The cryptocurrency networks we discuss at length here have generally not been deemed securities by relevant authorities, due to the absence of a controlling third party residual beneficiary from network activities. However, where many cryptocurrencies intended to ultimately be permissionless have run afoul of securities law in the United States surrounds their initial status before the blockchain has begun processing transactions in a decentralized fashion. If an organization issues tokens in exchange for startup capital, these tokens will be viewed as securities, regardless of the long-run intent to make the blockchain using those tokens permissionless (Mendelson 2019).

Just as we do not take a position on the extent to which any given permissionless cryptocurrency network's governance outcomes reflect "good" governance, we are similarly agnostic as to the extent to which the patchwork of private and public institutions superior to any given blockchain are a normatively preferable polycentric equilibria. Instead, we define the current (as of this writing) extent to which permissionless blockchains are nonetheless subject to a wide variety of governance forces that shape the incentives, and therefore, choice set, of network participants and users.

8. Conclusion

Rule-based governance is ubiquitous in organizations above a certain size, which leads to varying degrees of centralization of authority. Relatively decentralized forms of governance harness the benefits of subsidiarity, and the need for local administration of authority is ubiquitous in private and public organizations above a certain scale. Permissionless blockchains are a uniquely decentralized system for recording information of central relevance to a given unit of governance. As a unit of governance themselves, cryptocurrency blockchains shape users' and participants' incentives through protocol choices, which creates units of governance subsidiary to each protocol. But because no governance unit exists in a vacuum, there are governance jurisdictions both competitive and superior to each permissionless cryptocurrency blockchain that shape outcomes as well. In this regard, permissionless blockchains are at their core polycentric, nested enterprises.

Our analysis here emphasizes that permissionless blockchains will inevitably involve governance because they are a specific associational form (which betokens a discrete jurisdictional layer of governance). This means that as a set of rules constraining uniquely empowered organization members (cryptocurrency miners) to act on behalf of the larger set of organization members (cryptocurrency users), permissionless blockchains are a form of governance in and of themselves. But like all other governance systems, blockchain networks are polycentric, meaning their governance outcomes are also shaped by the larger and smaller associations that are part of the same governance network, as well as other similarly sized governance units with which a given network competes. The permissionless blockchain itself defines a constituency of network participants who engage in a variety of forms of on-chain governance like exit, voice/loyalty, and use of other cryptocurrencies. But as an associational form that implicates stores of economic value and payments transacted thereto, permissionless blockchains are subject to a variety of forms of non-digital governance, both public and private. Securities and fiduciary regulation have greatly shaped outcomes for different cryptocurrencies, and protocol coders develop protocol updates in communities with their own informal governance mechanisms. A given permissionless blockchain's success also depends to an extent on supportive governments and legal institutions to address challenges arising from multiple legal jurisdictions, breach of contract, and disputes over intellectual property, although low network exit and entry costs facilitate users' ability to choose among legal jurisdictions in interesting ways. Our analysis of the different governance forces to which cryptocurrency blockchains are subject illustrates the challenges of blockchain governance and its entanglement within broader political and legal frameworks.

This survey of permissionless blockchain governance is necessarily agnostic as to the intended purpose of cryptocurrency networks and their consequences, and instead identifies predominant governance forces that network protocol designers, participants, and users should be aware of. The study of how we choose to collectively decide rules for our voluntary and public associational forms is not a new one - indeed, it has motivated human societies as long as we have records for them. We can therefore learn much from the study of institutions that has immense applicability in the governance of online communities (and vice-versa) like those defined by cryptocurrency blockchain networks.

The concept of polycentricity is an unkind one for scholars or practitioners who want to derive clean prescriptions for the "right" set of governance choices. This is precisely because no institutional choice exists in a vacuum; the choice set for any potential institutional change is greatly shaped by the governance forces subsidiary, competitive, and superior to given social unit. Understanding observed outcomes requires a comprehensive understanding of the different governance forces that shape actual governance choices. Through our survey of the predominant governance forces shaping outcomes on permissionless blockchain networks, we provide a starting point for cryptocurrency network participants, users, and scholars to begin the challenging process of understanding, let alone predicting, governance outcomes in practice. Which set of network participants support a specific objective of network processes, and for what reasons tied to their incentives and the larger institutional context in which they operate? The choice set within any given governance unit is shaped by the governance forces polycentric to it, an insight that has guided our exposition throughout.

References

Acemoglu, Daron, Suresh Naidu, Pascual Restrepo, and James A. Robinson. 2019. "Democracy Does Cause Growth." *Journal of Political Economy* 127 (1): 47–100.

Alchian, Armen A., and Harold Demsetz. 1972. "Production, Information Costs, and Economic Organization." *American Economic Review* 62 (5): 777–95.

Alesina, Alberto, William Easterly, and Janina Matuszeski. 2011. "Artificial States." *Journal of the European Economic Association* 9 (2): 246–77.

Alesina, Alberto, and Enrico Spolaore. 1997. "On the Number and Size of Nations." *The Quarterly Journal of Economics* 112 (4): 1027–56.

Aligica, Paul Dragos, Peter J. Boettke, and Vlad Tarko. 2019. *Public Governance and the Classical-Liberal Perspective: Political Economy Foundations*. New York: Oxford University Press.

Aligica, Paul Dragos, and Vlad Tarko. 2012. "Polycentricity: From Polanyi to Ostrom, and Beyond." *Governance* 25 (2): 237–62.

Allen, Darcy WE, Chris Berg, and Aaron M. Lane. 2019. *Cryptodemocracy: How Blockchain Can Radically Expand Democratic Choice*. Rowman & Littlefield.

Alston, Eric. 2020. "Constitutions and Blockchains: Competitive Governance of Fundamental Rule Sets."

Belchior, Rafael, André Vasconcelos, Sérgio Guerreiro, and Miguel Correia. 2020. "A Survey on Blockchain Interoperability: Past, Present, and Future Trends." *ArXiv Preprint ArXiv:2005.14282*.

Berg, Alastair, Chris Berg, and Mikayla Novak. 2020. "Blockchains and Constitutional Catallaxy." *Constitutional Political Economy*, 1–17.

Böhme, Rainer, Nicolas Christin, Benjamin Edelman, and Tyler Moore. 2015. "Bitcoin: Economics, Technology, and Governance." *Journal of Economic Perspectives* 29 (2): 213–38.

Buchanan, James M., and Gordon Tullock. 1962. *The Calculus of Consent*. Ann Arbor: University of Michigan Press.

Bustamante, Pedro, Marcela M. Gomez, Ilia Murtazashvili, and Martin BH Weiss. 2020. "Spectrum Anarchy: Why Self-Governance of the Radio Spectrum Works Better than We Think." *Journal of Institutional Economics*.

Buterin, Vitalik. 2016. "Chain Interoperability." *R3 Research Paper*.

Cowen, Nick. 2019. "Markets for Rules: The Promise and Peril of Blockchain Distributed Governance." *Journal of Entrepreneurship and Public Policy*.

Craig, Ben R., and Joseph Kachovec. 2019. "Bitcoin's Decentralized Decision Structure." *Economic Commentary*, no. 2019–12.

David, Paul A., and Shane Greenstein. 1990. "The Economics of Compatibility Standards: An Introduction to Recent Research." *Economics of Innovation and New Technology* 1 (1–2): 3–41.

Davidson, Sinclair, Primavera De Filippi, and Jason Potts. 2018. "Blockchains and the Economic Institutions of Capitalism." *Journal of Institutional Economics* 14 (4): 639–58.

De Filippi, Primavera, and Benjamin Loveluck. 2016. "The Invisible Politics of Bitcoin: Governance Crisis of a Decentralized Infrastructure." *Internet Policy Review* 5 (4).

De Filippi, Primavera, and Aaron Wright. 2018. *Blockchain and the Law: The Rule of Code*. Harvard University Press.

Edmans, Alex, Vivian W. Fang, and Emanuel Zur. 2013. "The Effect of Liquidity on Governance." *The Review of Financial Studies* 26 (6): 1443–82.

Elkins, Zachary, Tom Ginsburg, and James Melton. 2009. *The Endurance of National Constitutions*. Cambridge University Press.

Governatori, Guido, Florian Idelberger, Zoran Milosevic, Regis Riveret, Giovanni Sartor, and Xiwei Xu. 2018. "On Legal Contracts, Imperative and Declarative Smart Contracts, and Blockchain Systems." *Artificial Intelligence and Law* 26 (4): 377–409.

Hadfield, Gillian K. 2016. *Rules for a Flat World: Why Humans Invented Law and How to Reinvent It for a Complex Global Economy*. New York: Oxford University Press.

Hadfield, Gillian K., and Iva Bozovic. 2016. "Scaffolding: Using Formal Contracts to Support Informal Relations in Support of Innovation." *Wisconsin Law Review*, 981–1032.

Hadfield, Gillian K., and Barry R. Weingast. 2014. "Microfoundations of the Rule of Law." *Annual Review of Political Science* 17: 21–42.

Harris, Colin. 2018. "Institutional Solutions to Free-Riding in Peer-to-Peer Networks: A Case Study of Online Pirate Communities." *Journal of Institutional Economics* 14 (5): 901–24.

Hart, H.L.A. 1967. "Social Solidarity and the Enforcement of Morality." *The University of Chicago Law Review* 35 (1): 1–13.

Hirschman, Albert O. 1970. *Exit, Voice, and Loyalty: Responses to Decline in Firms, Organizations, and States*. Cambridge: Harvard University Press.

Hooghe, Liesbet, Gary Marks, Arjan H. Schakel, Sandra Chapman Osterkatz, Sara Niedzwiecki, and Sarah Shair-Rosenfield. 2016. *Measuring Regional Authority: A Postfunctionalist Theory of Governance*. Vol. 1. Oxford University Press.

Hotelling, Harold. 1929. "Stability in Competition." *Economic Journal* 39 (4): 57.

Jensen, Michael C., and William H. Meckling. 1976. "Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure." *Journal of Financial Economics* 3 (4): 305–60.

Kwon, Yujin, Hyoungshick Kim, Jinwoo Shin, and Yongdae Kim. 2019. "Bitcoin vs. Bitcoin Cash: Coexistence or Downfall of Bitcoin Cash?" In *2019 IEEE Symposium on Security and Privacy (SP)*, 935–51. IEEE.

Law, David S., and Mila Versteeg. 2011. "The Evolution and Ideology of Global Constitutionalism." *California Law Review* 99: 1163–1258.

———. 2013. "Sham Constitutions." *California Law Review* 101: 863–952.

Lee, Barton E., Daniel J. Moroz, and David C. Parkes. 2020. "The Political Economy of Blockchain Governance." *Available at SSRN 3537314*.

Leeson, Peter T. 2006. "Efficient Anarchy." *Public Choice* 130 (1–2): 41–53.

———. 2007. "An-arrgh-chy: The Law and Economics of Pirate Organization." *Journal of Political Economy* 115 (6): 1049–94.

———. 2011. "Government, Clubs, and Constitutions." *Journal of Economic Behavior & Organization* 80 (2): 301–8.

———. 2014. *Anarchy Unbound: Why Self-Governance Works Better than You Think*. New York: Cambridge University Press.

Luther, William J., and Sean Stein Smith. 2020. "Is Bitcoin a Decentralized Payment Mechanism?" *Journal of Institutional Economics*.

Macaulay, Stewart. 1963. "Non-Contractual Relations in Business: A Preliminary Study." *American Sociological Review* 28 (1): 55–67.

Mehar, Muhammad Izhar, Charles Louis Shier, Alana Giambattista, Elgar Gong, Gabrielle Fletcher, Ryan Sanayhie, Henry M. Kim, and Marek Laskowski. 2019. "Understanding a Revolutionary and Flawed Grand Experiment in Blockchain: The DAO Attack." *Journal of Cases on Information Technology (JCIT)* 21 (1): 19–32.

Mendelson, Michael. 2019. "From Initial Coin Offerings to Security Tokens: A US Federal Securities Law Analysis." *Stanford Technology Law Review* 22: 52.

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

North, Douglass C., John Joseph Wallis, and Barry R. Weingast. 2009. *Violence and Social Orders: A Conceptual Framework for Interpreting Recorded Human History*. New York: Cambridge University Press.

Ostrom, Elinor. 1990. *Governing the Commons: The Evolution of Institutions for Collective Action*. New York: Cambridge University Press.

———. 2005. *Understanding Institutional Diversity*. Princeton: Princeton University Press.

Ostrom, Vincent. 1994. *The Meaning of American Federalism: Constituting a Self-Governing Society*. San Francisco: Institute for Contemporary Studies.

Pennington, Mark. 2011. *Robust Political Economy: Classic Liberalism and the Future of Public Policy*. Cheltenham: Edward Elgar Publishing.

Potts, Jason. 2018. "Governing the Innovation Commons." *Journal of Institutional Economics* 14 (6): 1025–47.

Prewett, Kyleen, Roger W. Dorsey, and Gaurav Kumar. 2019. "A Primer on Taxation of Investment in Cryptocurrencies." *Journal of Taxation of Investments* 36 (4).

Rajagopalan, Shruti. 2018. "Blockchain and Buchanan: Code as Constitution." In *James M. Buchanan*, edited by Richard E. Wagner, 359–81. Springer.

Sirbu, Marvin, and Kent Hughes. 1986. "Standardization of Local Area Networks." In *14th Annual Telecommunications Policy Research Conference, Virginia*.

Skarbek, David. 2014. *The Social Order of the Underworld: How Prison Gangs Govern the American Penal System*. New York: Oxford University Press.

Somin, Ilya. 2020. *Free to Move: Foot Voting, Migration, and Political Freedom*. Oxford University Press, USA.

Song, Jimmy. 2017. "Bitcoin Cash: What You Need to Know. Medium.Com." *Medium* (blog). 2017. https://medium.com/@jimmysong/bitcoin-cash-what-you-need-to-know-c25df28995cf.

Von Burg, Urs, and Martin Kenney. 2000. "Venture Capital and the Birth of the Local Area Networking Industry." *Research Policy* 29 (9): 1135–55.

Weingast, Barry R. 1995. "The Economic Role of Political Institutions: Market-Preserving Federalism and Economic Development." *Journal of Law, Economics, and Organization* 11 (1): 1–31.

Weiss, Martin BH, and Marvin Sirbu. 1990. "Technological Choice in Voluntary Standards Committees: An Empirical Analysis." *Economics of Innovation and New Technology* 1 (1–2): 111–33.

Werbach, Kevin. 2018a. *The Blockchain and the New Architecture of Trust*. MIT Press.

———. 2018b. "Trust, but Verify: Why the Blockchain Needs the Law." *Berkeley Technology Law Journal* 33: 487.

Werbach, Kevin, and Nicolas Cornell. 2017. "Contracts Ex Machina." *Duke Law Journal* 67: 313.

Yalaman, Gamze Öz, and Hakan Yıldırım. 2019. "Cryptocurrency and Tax Regulation: Global Challenges for Tax Administration." In *Blockchain Economics and Financial Market Innovation*, edited by Umit Hacioglu, 407–22. Springer.