VOLUME 2 MARCH 2021 ISSUE 1

JOURNAL ON EMERGING TECHNOLOGIES

ARTICLES

CAN PERMISSIONLESS BLOCKCHAINS AVOID GOVERNANCE AND THE LAW?

Eric Alston, Wilson Law, Ilia Murtazashvili & Martin Weiss

CAN PERMISSIONLESS BLOCKCHAINS AVOID GOVERNANCE AND THE LAW?

Eric Alston,[*] Wilson Law,[**] Ilia Murtazashvili[***] & Martin Weiss[****]

Permissionless (or public) blockchain networks are a new form of decentralized private governance in the digital sphere. Though legal scholars recognize the significance of law in the use of blockchain, existing research using legal and institutional perspectives leaves blockchain governance as something of a black box. We provide a more granular analysis, finding that blockchain governance operates on four distinct levels. Governance at the protocol layer involves discrete institutional design choices intended to constrain network members' incentives in an ongoing sense. Subsidiary governance arises from the need for communities to draft protocol updates and from the fact that governance protocol design choices create discrete concentrations of political power within the network. Competitive governance forces arise because cryptocurrency networks are constrained by the possibility of exit of participants and users to other alternatives. Finally, in terms of superior governance, 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. Since the interaction of these governance aspects shapes the operation of any given network, legal and regulatory governance of blockchain ought to consider permissionless blockchains as confronting political and governance dilemmas much like any complex organization. Predicting the effect legal and regulatory treatment of permissionless blockchains requires an accurate understanding of the incentives of their members, all of which are greatly shaped by the governance forces we outline in detail here.

[*] University of Colorado Boulder.
[**] Baylor University.
[***] University of Pittsburgh.
[****] University of Pittsburgh.

INTRODUCTION

In this paper, we provide a more granular analysis of the governance of blockchain with a focus on permissionless (or public) blockchains. Our analysis clarifies that blockchain networks are subject to governance dilemmas not unlike those of any large, complex organization and that any given network resides in a legal and regulatory framework by necessity. A more precise understanding of the networks is useful for understanding the organization of blockchain as well as offering a perspective that policymakers can use to craft laws and regulations that help blockchain fulfill its promise of improving economic performance,[1] financial performance,[2] and the quality of public administration.[3]

The reason a governance perspective on blockchain is appropriate is because any given blockchain network is a large, complex organization. Rule-based governance is ubiquitous in groups above a certain size because an organization's members tend to reach decisions through a collective decision-making process.[4] Governance at scale often entails considerably centralized decision-making, perhaps nowhere more so than in the canonical case of the private firm.[5] 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,[6] thereby addressing to some extent the knowledge or information problem confronting the government.[7] Regardless of the level of centralization of an organization's authority, the reality is of a world whose interactions are continually

---

[1] *See, e.g.*, Melanie SWAN, BLOCKCHAIN: BLUEPRINT FOR A NEW ECONOMY (Tim McGovern, ed., 2015).

[2] Christian Catalini & Joshua S. Gans, *Some Simple Economics of the Blockchain*, COMM. OF THE ACM, July 2020, at 80; Ye Guo & Chen Liang, *Blockchain Application and Outlook in the Banking Industry*, 2 FIN. INNOVATION 24 (2016).

[3] DARCY W.E. ALLEN, CHRIS BERG & AARON M. LANE, CRYPTODEMOCRACY: HOW BLOCKCHAIN CAN RADICALLY EXPAND DEMOCRATIC CHOICE (2019).

[4] Though *governance* is necessary under such circumstances, *government* (i.e., formal political decision-making) is not inevitable. *See* EDWARD PETER STRINGHAM, PRIVATE GOVERNANCE: CREATING ORDER IN ECONOMIC AND SOCIAL LIFE (2015); Peter T. Leeson, *Government, Clubs, and Constitutions*, 80 J. ECON. BEHAV. & ORG. 301 (2011); TERRY L. ANDERSON & PETER J. HILL, THE NOT SO WILD, WILD WEST: PROPERTY RIGHTS ON THE FRONTIER (2004); ROBERT C. ELLICKSON, ORDER WITHOUT LAW: HOW NEIGHBORS SETTLE DISPUTES (1991); Oliver E. Williamson, *The Economics of Governance*, 95 AM. ECON. REV. 1 (2005); Alexander William Salter, *Space Debris: A Law and Economics Analysis of the Orbital Commons*, 19 STAN. TECH. L. REV. 221 (2016).

[5] Armen A. Alchian & Harold Demsetz, *Production, Information Costs, and Economic Organization*, 62 AM. ECON. REV. 777, 793–94 (1972).

[6] PAUL DRAGOS ALIGICA, PETER J. BOETTKE & VLAD TARKO, PUBLIC GOVERNANCE AND THE CLASSICAL-LIBERAL PERSPECTIVE: POLITICAL ECONOMY FOUNDATIONS (2019); MARK PENNINGTON, ROBUST POLITICAL ECONOMY: CLASSIC LIBERALISM AND THE FUTURE OF PUBLIC POLICY (Peter J. Boettke, ed., 2011).

[7] Decentralization has costs, such as increasing decision-making costs, at least mechanically. *See* JAMES M. BUCHANAN & GORDON TULLOCK, THE CALCULUS OF CONSENT (1962). At the same time, it has benefits, including reducing oppression and corruption and unleashing a host of economic, technological, and institutional innovation. *See* DOUGLASS C. NORTH, JOHN JOSEPH WALLIS & BARRY R. WEINGAST, VIOLENCE AND SOCIAL ORDERS: A CONCEPTUAL FRAMEWORK FOR INTERPRETING RECORDED HUMAN HISTORY (2009); Daron Acemoglu et al., *Democracy Does Cause Growth*, 127 J. POL. ECON. 47, 54 n.4 (2019).

increasing in scale and complexity.[8] 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.[9]

Enter permissionless blockchains and their protocol-based decentralized governance.[10] Permissionless blockchains are what Nakamoto[11] envisioned when creating Bitcoin: publicly accessible ledgers available to anyone to join and participate in governance.[12] 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 ongoing processes, which are governed primarily by network participants and users.[13] This is because the novelty of these cryptocurrencies' organizational structure meant existing law and regulation were, in many instances, ill-equipped to deal with them.[14] 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 individual miners without any residual benefits (profits) flowing to the network as a whole.[15] It presents a novel form of private governance that facilitates impersonal online exchange 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 right software, internet access, and electricity access.

Despite the claim to be decentralized and self-governing,[16] we argue that permissionless cryptocurrency blockchains cannot avoid the

---

[8] 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. *See* Peter T. Leeson, *Efficient Anarchy*, 130 PUB. CHOICE 41, 45 (2006); PETER T. LEESON, ANARCHY UNBOUND: WHY SELF-GOVERNANCE WORKS BETTER THAN YOU THINK (2014).

[9] Elinor Ostrom, *Beyond Markets and States: Polycentric Governance of Complex Economic Systems*, 100 AM. ECON. REV. 641, 642 (2010).

[10] 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.

[11] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* (2008), https://bitcoin.org/bitcoin.pdf (last visited Jan. 22, 2021).

[12] Granted, participation in the Bitcoin is not costless. At the onset it requires a computer with sufficient graphics processing power and internet connection to facilitate connecting to the network, and in practice the barriers to entry for successful Bitcoin mining are quite high, due to the way in which the network preferences large concentrations of graphics processing power. We return to the governance implications of this point in the following sections.

[13] Rainer Böhme et al., *Bitcoin: Economics, Technology, and Governance*, 29 J. ECON. PERSP. 213 (2015).

[14] PRIMAVERA DE FILIPPI & AARON WRIGHT, BLOCKCHAIN AND THE LAW: THE RULE OF CODE (2018).

[15] Gerald P. Dwyer, *The Economics of Bitcoin and Similar Private Digital Currencies*, 17 J. FIN. STABILITY 81, 83 (2015).

[16] Nakamoto, *supra* note 11; Vitalik Buterin, *A Next-Generation Smart Contract and Decentralized Application Platform*, ETHEREUM WHITE PAPER (2014), https://ethereum.org/en/whitepaper/#a-next-generation-smart-contract-and-decentralized-application-platform.

forces of governance, both within and external to 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 have also been characterized as promising a complete contract because users must agree on all rules ex-ante.[17] 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 distinct, and at times competing, interest groups subsidiary to each blockchain network, and create pressure for change within the blockchain. The distinct roles associated with shaping governance outcomes on a given cryptocurrency network create specific incentives surrounding the outcomes of network processes. While existing research emphasizes blockchain as a novel system of governance,[18] less attention had been paid to the granular details of how permissionless blockchains are governed. In addition, while a sizable literature considers the legal aspects of blockchain governance (or external governance),[19] we argue that the legal and regulatory aspects cannot be understood without consideration of the numerous polycentric governance forces to which permissionless blockchains are subject.

Drawing on the tradition of polycentric governance specifically,[20] along with the new institutional economics more generally,[21] we argue

---

[17] Sinclair Davidson, Primavera De Filippi & Jason Potts, *Blockchains and the Economic Institutions of Capitalism*, 14 J. INST. ECON. 639, 651 (2018).

[18] *Id.*; DE FILIPPI & WRIGHT, *supra* note 14; Marcella Atzori, *Blockchain Technology and Decentralized Governance: Is the State Still Necessary?* (2015); Daniil Frolov, *Blockchain and Institutional Complexity: An Extended Institutional Approach*, J. INST. ECON. 1 (2020).

[19] DE FILIPPI & WRIGHT, *supra* note 14; Kevin Werbach, *Trust, but Verify: Why the Blockchain Needs the Law*, 33 BERKELEY TECHNOL. L.J. 487 (2018); Kevin Werbach & Nicolas Cornell, *Contracts Ex Machina*, 67 DUKE L.J. 313 (2017).

[20] *See* ELINOR OSTROM, UNDERSTANDING INSTITUTIONAL DIVERSITY (2009); ELINOR OSTROM, GOVERNING THE COMMONS: THE EVOLUTION OF INSTITUTIONS FOR COLLECTIVE ACTION (1990); VINCENT OSTROM, THE POLITICAL THEORY OF A COMPOUND REPUBLIC: DESIGNING THE AMERICAN EXPERIMENT (2008); VINCENT OSTROM, THE INTELLECTUAL CRISIS IN AMERICAN PUBLIC ADMINISTRATION (2008); VINCENT OSTROM, THE MEANING OF AMERICAN FEDERALISM: CONSTITUTING A SELF-GOVERNING SOCIETY (1994). For overviews of the Ostroms' polycentric approach to political and legal institutions, *see* PAUL DRAGOS ALIGICA & PETER J. BOETTKE, CHALLENGING INSTITUTIONAL ANALYSIS AND DEVELOPMENT: THE BLOOMINGTON SCHOOL (2009); Paul Dragos Aligica & Peter Boettke, *The Two Social Philosophies of Ostroms' Institutionalism*, 39 POL'Y STUD. J. 29 (2011); Michael D. McGinnis & Elinor Ostrom, *Reflections on Vincent Ostrom, Public Administration, and Polycentricity*, 72 PUB. ADMIN. REV. 15 (2011); Roberta Q. Herzberg, *Governing Their Commons: Elinor and Vincent Ostrom and the Bloomington School*, 163 PUB. CHOICE 95 (2015); Paul Dragos Aligica & Vlad Tarko, *Polycentricity: From Polanyi to Ostrom, and Beyond*, 25 GOVERNANCE 237 (2012).

[21] LIYA PALAGASHVILI, ENNIO PIANO & DAVID SKARBEK, THE DECLINE AND RISE OF INSTITUTIONS: A MODERN SURVEY OF THE AUSTRIAN CONTRIBUTION TO THE ECONOMIC ANALYSIS OF INSTITUTIONS (2017); ERIC ALSTON ET AL., INSTITUTIONAL AND ORGANIZATIONAL ANALYSIS:

that there are four distinct, yet interrelated, levels of governance of permissionless blockchains. Governance at the *protocol* level is necessary because codes and rules need to be changed periodically in ways that cannot be anticipated ex ante, as well as requiring procedures to adjudicate disputes arising during these changes. 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.[22] 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.[23] The need for governance at the *subsidiary* level arises from the need for communities to draft protocol updates and from the possibility that specific protocol design choices create concentrations of political power within the network. Dilemmas of *competitive* governance arise because cryptocurrency networks are constrained by the possibility of exit of participants and users to other alternatives. Finally, in terms of *superior* governance, 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 and discuss their implications for the ongoing development of these novel organizational forms, with emphasis on how an understanding of these governance aspects informs legal and regulatory responses to increasing deployment of permissionless blockchains.

Section I of the paper sets the stage by arguing that blockchain, often viewed in terms of complete contracts, is, like all governance systems, incomplete, and that as a result, its organization is dynamic, costly, and polycentric. Section II delves into the core aspects of permissionless blockchains and the contention that governance by code is replacing more traditional governance. Sections III-VI consider each of the four aspects of governance: protocol, subsidiary, competitive, and superior. The Conclusion discusses the implications for regulation and law: while we provide no specific recommendations for how blockchain ought to be governed, our analysis clarifies that regulation and legal reforms ought to take as a starting point that blockchain networks are adaptive, evolving enterprises that are subject to internal and external governance dilemmas, much like any large, complex organization.

CONCEPTS AND APPLICATIONS (2018); Simon Deakin et al., *Legal Institutionalism: Capitalism and the Constitutive Role of Law*, 45 J. COMPAR. ECON. 188 (2017).

[22] *See* William J. Luther & Sean Stein Smith, *Is Bitcoin a Decentralized Payment Mechanism?*, J. INST'L. ECON. (2020) (arguing that as a payment mechanism, Bitcoin is a distributed payment technology in that it relies not only on the parties to a transaction, but the network of users, to validate transactions). *But see*, Ben R. Craig & Joseph Kachovec, *Bitcoin's Decentralized Decision Structure*, ECON. COMMENT. (FED. RSRV. BANK OF CLEVELAND, CLEVELAND, OH) July 16, 2019, at 1 (claiming that as a decision-making structure, it is decentralized in that the parties participate directly in governance.)

[23] Jeffery Atik & George Gerro, *Hard Forks on the Bitcoin Blockchain: Reversible Exit, Continuing Voice*, 1 STAN. J. BLOCKCHAIN L. POL'Y 24 (2018).

I. INCOMPLETE GOVERNANCE AS DYNAMIC, COSTLY AND POLYCENTRIC

Public governance often organizes around geospatially delimited jurisdictions to which individuals belong (e.g., counties, cities, states, and nations). Private governance tends to involve the associations that one voluntarily joins (e.g., soccer leagues, churches, employers, etc.).[24] 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,[25] and may in part explain the ubiquity of formal constitutions, notwithstanding the wide variety of forms of governments that create these constitutions.[26]

Blockchains can themselves be understood as a form of secondary rules shaping and constraining the incentives of network participants and users.[27] Secondary rules are rules about making rules; they 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."[28] This

---

[24] Private governance also involves enforcement and coercion such that they are not fully "voluntary," such as in criminal organizations or gangs. *See* DAVID SKARBEK, THE SOCIAL ORDER OF THE UNDERWORLD: HOW PRISON GANGS GOVERN THE AMERICAN PENAL SYSTEM (2014); Peter T. Leeson, *An*-arrgh*-chy: The Law and Economics of Pirate Organization*, 115 J. POL. ECON. 1049 (2007); Peter T. Leeson & Douglas Bruce Rogers, *Organizing Crime*, 20 SUP. CT. ECON. REV. 89 (2012); DIEGO GAMBETTA, THE SICILIAN MAFIA: THE BUSINESS OF PRIVATE PROTECTION (1996); ANJA SHORTLAND, KIDNAP: INSIDE THE RANSOM BUSINESS (2019). Indeed, fully voluntary forms of governance would likely require one's contracting into a set of institutions that subsequently involve enforcement or coercion as against those found in transgression of the rules as against other members of the governance unit. *See* David Friedman, *Efficient Institutions for the Private Enforcement of Law*, 13 J. LEG. STUD. 379 (1984); David Friedman, *Private Creation and Enforcement of Law: A Historical Case*, 8 J. LEG. STUD. 399, 402–03 (1979).

[25] H.L.A. Hart, *Social Solidarity and the Enforcement of Morality*, 35 U. CHI. L. REV. 1, 10 (1967).

[26] ZACHARY ELKINS, TOM GINSBURG & JAMES MELTON, THE ENDURANCE OF NATIONAL CONSTITUTIONS (2009); David S. Law & Mila Versteeg, *Sham Constitutions*, 101 CALIF. L. REV. 863 (2013); David S. Law & Mila Versteeg, *The Evolution and Ideology of Global Constitutionalism*, 99 CALIF. L. REV. 1163 (2011).

[27] Nick Cowen, *Markets for Rules: The Promise and Peril of Blockchain Distributed Governance*, 9 J. ENTREP. & PUB. POL'Y 213 (2019); Shruti Rajagopalan, *Blockchain and Buchanan: Code as Constitution*, *in* JAMES M. BUCHANAN: A THEORIST OF POLITICAL ECONOMY AND SOCIAL PHILOSOPHY 359 (Richard E. Wagner ed., 2018); Eric Alston, *Constitutions and Blockchains: Competitive Governance of Fundamental Rule Sets*, 11 CASE WEST. J. LAW TECH. & INTERNET (2020); Alastair Berg, Chris Berg & Mikayla Novak, *Blockchains and Constitutional Catallaxy*, 31 CONST. POL. ECON. 188 (2020).

[28] Eric Alston, Lee J. Alston & Bernardo Mueller, *Leadership and Organizational Hierarchies* (2020), https://ssrn.com/abstract=3549964 (last visited Jan. 22, 2021).

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."[29] Thus, for an organization's rules to be effective, there must be a means in the organization to change them.[30]

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.[31] Contracting in the face of complexity means we contract away from 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.[32] Public governance deals with problems of incompleteness as well because the articulation of rules for future conduct faces the same uncertainty associated with the dynamic and complex nature of the world.[33] This uncertainty gives rise to the fundamental political dilemma, which is that any government that can establish the rule of law can violate it.[34] In the context of interest to us here, the ongoing need for adjustment to blockchain network protocols shows how

---

[29] GILLIAN K. HADFIELD, RULES FOR A FLAT WORLD: WHY HUMANS INVENTED LAW AND HOW TO REINVENT IT FOR A COMPLEX GLOBAL ECONOMY (2016); Gillian K. Hadfield & Barry R. Weingast, *Microfoundations of the Rule of Law*, 17 ANN. REV. POL. SCI. 21 (2014); Gillian K. Hadfield & Barry R. Weingast, *Law Without the State: Legal Attributes and the Coordination of Decentralized Collective Punishment*, 1 J. L. & CT. 3 (2013); Gillian K. Hadfield & Barry R. Weingast, *What is Law? A Coordination Model of the Characteristics of Legal Order*, 4 J. LEGAL ANALYSIS 471 (2012); Gillian K. Hadfield, *The Problem of Social Order: What Should We Count as Law?*, 42 LAW & SOC. INQUIRY 16 (2017).

[30] *See* ELINOR OSTROM, GOVERNING THE COMMONS: THE EVOLUTION OF INSTITUTIONS FOR COLLECTIVE ACTION (1990) (arguing analysis of governance recognized the importance of collective decision-making as one of the criteria for long-standing self-governance of organizations).

[31] For this reason, trust and reciprocity are essential to business relations. *See* Stewart Macaulay, *Non-Contractual Relations in Business: A Preliminary Study*, 28 AM. SOCIO. REV. 55, 64 (1963); Janet T. Landa, *A Theory of the Ethnically Homogeneous Middleman Group: An Institutional Alternative to Contract Law*, 10 J. LEGAL STUD. 349 (1981); JANET T. LANDA, TRUST, ETHNICITY, AND IDENTITY: BEYOND THE NEW INSTITUTIONAL ECONOMICS OF ETHNIC TRADING NETWORKS, CONTRACT LAW, AND GIFT-EXCHANGE (1994); Robert Cooter & Janet T. Landa, *Personal Versus Impersonal Trade: The Size of Trading Groups and Contract Law*, 4 INT'L. REV. L. & ECON. 15 (1984); Avner Greif, *Institutions and Impersonal Exchange: From Communal to Individual Responsibility*, 158 J. INST'L. & THEOR. ECON. 168 (2002).

[32] Force majeure clauses stand as a significant example of this in contracting practice, a contractual feature the salience of which has increased significantly during the COVID-19 pandemic. *See, e.g.*, David A. Shargel, Matthew G. Nielsen & W. Stephen Benesh, *Revisiting Force Majeure and Other Contractual Considerations Amid COVID-19*, THE NAT'L L. REV. (Nov. 6, 2020) https://www.natlawreview.com/article/revisiting-force-majeure-and-other-contractual-considerations-amid-covid-19.

[33] Douglass C. North & Barry R. Weingast, *Constitutions and Commitment: The Evolution of Institutions Governing Public Choice in Seventeenth-Century England*, 49 J. ECON. HIST. 803 (1989); Hilton L. Root, *Tying the King's Hands: Credible Commitments and Royal Fiscal Policy during the Old Regime*, 1 RATION ALITY & SOC'Y. 240 (1989); Lizhi Liu & Barry R. Weingast, *Taobao, Federalism, and the Emergence of Law, Chinese Style*, 111 MINN. L. REV. 1563 (2018).

[34] Barry R. Weingast, *The Economic Role of Political Institutions: Market-Preserving Federalism and Economic Development*, 11 J. L. ECON. & ORG. 1 (1995).

the notion of ex-ante defining all possible governance outcomes flies in the face of how governance actually proceeds in practice.[35]

Since 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.[36] 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, then better it be discarded due to its rigidity.[37] In the context of permissionless blockchains, the need for significant protocol updates, including an upcoming transition of consensus mechanism for the Ethereum protocol,[38] directly suggests that some measure of 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 resolving conflicts is intrinsically costly, people do not tend to want to dispute, let alone harm, one another.[39] 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.[40] 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

---

[35] 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. *See* Pedro Bustamante et al., *Spectrum Anarchy: Why Self-Governance of the Radio Spectrum Works Better than We Think*, J. INST'L. ECON. (June 11, 2020); Colin Harris, *Institutional Solutions to Free-Riding in Peer-to-Peer Networks: A Case Study of Online Pirate Communities*, 14 J. INST'L. ECON. 901 (2018); Jason Potts, *Governing the Innovation Commons*, 14 J. INST'L. ECON. 1025 (2018).

[36] Alston, *supra* note 28.

[37] ELKINS ET AL., *supra* note 26.

[38] Vitalik Buterin at al., *Incentives in Ethereum's Hybrid Casper Protocol*, 30 INT'L J. NETWORK MGMT. 1 (2020).

[39] Roger Myerson, *Justice, Institutions, and Multiple Equilibria*, 5 CHIC. J. INT. LAW 91 (2004); Phillipe Aghion, Nicholas Bloom & John Van Reenen, *Incomplete Contracts and the Internal Organization of Firms*, 30 J. L. ECON. & ORG. i37 (July 19, 2013); Benito Arruñada, *Registries*, 1 MAN ECON. 209–230 (2014), https://www.researchgate.net/publication/287136659_Registries.

[40] NEIL K. KOMESAR, LAW'S LIMITS: RULE OF LAW AND THE SUPPLY AND DEMAND OF RIGHTS (2001); NEIL K. KOMESAR, IMPERFECT ALTERNATIVES: CHOOSING INSTITUTIONS IN LAW, ECONOMICS, AND PUBLIC POLICY (1994).

of individuals' and organizations' actions.[41] This means the resolution of policy issues is costly, both mechanically and in terms of distribution. 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.[42] 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.[43] Nonetheless, while payments are largely irreversible,[44] 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.[45] Because disputes occur within and may be addressed by the legal and regulatory framework, blockchain is a polycentric enterprise, which refers to multiple levels of governance sharing autonomy.[46] Polycentric enterprises are characterized by limited and autonomous prerogatives operating under an overarching set of rules.[47] Central to this notion of polycentrism is autonomy, as an organization may be decentralized but lack meaningful autonomy.[48] 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.[49]

Given the specific structure of permissionless blockchains, it meets the autonomy criteria of polycentricity in that outcomes on the blockchain network are greatly influenced by the deliberative governance choices of network participants.[50] Currencies on permissionless blockchain platforms such as Ethereum or the Bitcoin network are therefore 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 of the decisions of countless individuals making decisions deliberately, but without a third party with a formal role in coordinating them. Permissionless blockchains also operate under a set of superior governance institutions.

---

[41] Eric Alston, *Piercing the Veil of Political Altruism*, *in* ECONOMIC HISTORY AND AUSTRIAN THEORY IN THE 21ST CENTURY (Daniel J. D'Amico & Adam Martin eds., forthcoming 2021).

[42] Primavera De Filippi & Benjamin Loveluck, *The Invisible Politics of Bitcoin: Governance Crisis of a Decentralized Infrastructure*, 5 INTERNET POL'Y REV. (2016).

[43] Nakamoto, *supra* note 11.

[44] 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.

[45] Werbach & Cornell, *supra* note 19.

[46] Giuseppe Eusepi & Richard E. Wagner, *Polycentric Polity: Genuine vs. Spurious Federalism*, 6 REV. LAW ECON. 329-345 (2010).

[47] *See generally* Aligica & Tarko, *supra* note 20.

[48] OSTROM, UNDERSTANDING INSTITUTIONAL DIVERSITY, *supra* note 20 at 132.

[49] Alston, *supra* note 28.

[50] Rajagopalan, *supra* note 27.

In this regard, they are not like the anarcho-capitalist view of institutions arising in the absence of institutions but operate within a broader legal and regulatory framework. Though as we note in the section on superior governance mechanisms, the ability of such an institutional framework to regulate permissionless blockchain participants and users depends integrally on the enforcement ability of a given authority, which in many jurisdictions around the world, is observably lacking.[51]

Permissionless 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 presents 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, permissionless blockchains are polycentric. These networks' 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 next discuss the basic structure of permissionless blockchain governance.

II. DECENTRALIZED GOVERNANCE BY CODE: PERMISSIONLESS BLOCKCHAINS

Bitcoin, which emerged without lawyers or regulators, offers a payment 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.[52] 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 institutional technology alongside governments and firms.[53] 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.[54] Despite these potential cost-saving benefits in terms of governance, we argue that permissionless cryptocurrency blockchains cannot avoid the forces of governance, both within and external to blockchain networks themselves.

Cryptocurrency networks are private organizations–people can join and exit at will with relatively low exit costs. Nonetheless, these networks' governance structure is decentralized and transparent in a way

[51] Katherine Kirkpatrick et al., *Virtual Currency in Sanctioned Jurisdictions: Stepping Outside of SWIFT*, J. INV. COMPLIANCE (2019); Usman W. Chohan, *Assessing the Differences in Bitcoin & Other Cryptocurrency Legality Across National Jurisdictions*, SSRN (Sep. 20, 2017).

[52] Böhme et al., *supra* note 13.

[53] Davidson, et al., *supra* note 17; ALLEN, ET AL., *supra* note 3; DE FILIPPI & WRIGHT, *supra* note 14.

[54] KEVIN WERBACH, THE BLOCKCHAIN AND THE NEW ARCHITECTURE OF TRUST (2018).

that the vast majority of private organizations in society do not share.[55] 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. In the realm of currencies, this level of decentralization and (technically) egalitarian access to controlthe processes of currency issuance and transactions is unparalleled.[56] Compared to politically controlled processes of currency maintenance and issuance, this makes these structural features of network governance particularly innovative.[57]

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 their wallet key's having been included in another user's transfer request) units of value enumerated on the distributed ledger maintained by network participants.[58] 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 .[59] 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.

[55] The decentralized aspects also give rise to potential for criminality. *See e.g.*, Tyler Moore & Nicolas Christin, *Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk*, INT'L. CONF. ON FIN. CRYPTOGRAPHY AND DATA SEC. 25 (2013).

[56] Luther et al., *supra* note 22.

[57] Joshua R. Hendrickson, Thomas L. Hogan & William J. Luther, *The Political Economy of Bitcoin*, 54 ECON. INQ. 925-939 (2016).

[58] Victoria L. Lemieux, *A Typology of Blockchain Recordkeeping Solutions and Some Reflections on their Implications for the Future of Archival Preservation*, IEEE INT'L. CONF. ON BIG DATA 2271-78 (2017); Rui Zhang, Rui Xue & Ling Liu, *Security and Privacy on Blockchain*, 52 ACM COMPUTING SURV. 34-51, (2019).

[59] 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. *See* Leslie Lamport, Robert Shostak & Marshall Pease, *The Byzantine Generals Problem*, CONCURRENCY: THE WORKS OF LESLIE LAMPORT 203–26 (2019).

III. GOVERNANCE BY BLOCKCHAIN PROTOCOL

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.[60] 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.[61] 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 across Bitcoin users' wallets that always sums to the total Bitcoins in circulation.[62]

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

---

[60] Alston, *supra* note 28 at 13, n.44. *See also* Karl Wüst & Arthur Gervais, *Do You Need a Blockchain?*, 2018 CRYPTO VALLEY CONF. BLOCKCHAIN TECH. 45 (2018).

[61] Benito Arruñada & Luis Garicano, *Blockchain: The Birth of Decentralized Governance*, (Universitat Pompeu Fabra Univ. Barcelona Dep't. of Econ. and Bus. Working Paper No. 1608, 2018) (Spain); DE FILIPPI & WRIGHT, *supra* note 14.

[62] Granted, some of these wallets are dead wallets, in that the human user lost their private keys. In the case of Bitcoin and most other permissionless cryptocurrencies, a user who is the sole possessor of their private keys should be very careful not to lose or forget their keys, because once lost, they are effectively irretrievable. This question poses interesting challenges for enforcement authorities surrounding the ability of the authorities to compel revelation of keys that someone under criminal investigation claims they have forgotten. *See* Andrew M. Hinkes, *Throw Away the Key, or the Key Holder? Coercive Contempt for Lost or Forgotten Cryptocurrency Private Keys, or Obstinate Holders*, 16 NW. J. TECH. INTELL. PROP. 225 (2019).

processing power on the network. Coordination of such mining pools has advantages for miners, though it introduces adversaries, including the possibility of predation by larger mining pools.[63] 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.[64] 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.[65] 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 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, this interaction between different layers of protocol-based governance will become increasingly salient.

A. Consensus Mechanisms/Amendment Rules

The technical answer to how the network reaches consensus across the numerous distributed copies of the ledger when it comes to a proposed block of potential updates is called the consensus mechanism, which needs to prevent two types of fraud: (i) the original sender tries to send bitcoins they do not have, or have simultaneously spent; and (ii) other members of the network alter the message when transmitting to the rest of network.[66] The way in which a given network confronts these challenges varies in practice, though, a distinction in governance by

---

[63] Joshua A. Kroll, Ian C. Davey & Edward W. Felten, *The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries*, THE TWELFTH WORKSHOP ON THE ECON. OF INFO. SEC. (June 2013).

[64] 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. *See* Okke Schrijvers et al., *Incentive Compatibility of Bitcoin Mining Pool Reward Functions*, INT'L CONF. FIN. CRYPTOGRAPHY AND DATA SEC. 477 (2017).

[65] Indeed, larger mining pools have been argued to have incentives that make them more likely to engage in attacks to harm competitors. *See* Benjamin Johnson et al., *Game-Theoretic Analysis of DDoS Attacks Against Bitcoin Mining Pools*, INT'L CONF. FIN. CRYPTOGRAPHY AND DATA SEC. 72 (2014); A. Laszka, B. Johnson & J. Grossklags, *When Bitcoin Mining Pools Run Dry: A Game-Theoretic Analysis of the Long-Term Impact of Attacks Between Mining Pools*, FIN. CRYPTOGRAPHY DATA SEC. 63 (2015); Ville Savolainen & Jorge Soria, *Too Big to Cheat: Mining Pools' Incentives to Double Spend in Blockchain Based Cryptocurrencies* (2019).

[66] There are differences in these protocols in practice, though the basic consensus mechanism idea is similar across variation in real-world consensus protocols. *See* Christian Cachin & Marko Vukolić, *Blockchain Consensus Protocols in the Wild*, (2017); Zhang, et al., *supra* note 58.

protocol that will continue to shape observed 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.[67] 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 be the first to obtain a solution that has enough zeros in front to satisfy the current algorithmic difficulty level. Importantly, due to the nature of the cryptographic hash function, no one can predict ex-ante which highly specific strings of characters will generate a result below the specifically defined threshold.[68] The conformity of proposed transactions with network rules is the result of a 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.[69] 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. However, as we have already stressed, 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.[70]

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 design.[71] Each 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.[72] 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

---

[67] Aviv Zohar, *Bitcoin: Under the Hood*, 58 COMMC'N. ACM 104 (2016); Bin Cao et al., *Performance Analysis and Comparison of PoW, PoS and DAG Based Blockchains*, DIGIT. COMMC'N. NETW. (2020); Karl Wüst, *Security of Blockchain Technologies* (2016) (Master Thesis ETH Zurich).

[68] Michael Crosby et al., *Blockchain Technology: Beyond Bitcoin*, 2 APPL. INNOV. 71 (2016).

[69] Seyed Mojtaba Hosseini Bamakan, et. al., *A Survey of Blockchain Consensus Algorithms Performance Evaluation Criteria*, EXPERT SYS. APPL. 113385 (Apr. 13, 2020).

[70] Craig & Kachovec, *supra* note 22.

[71] Christian Stoll, Lena Klaaßen & Ulrich Gallersdörfer, *The Carbon Footprint of Bitcoin*, 4 JOULE 1647 (2019); Ulrich Gallersdörfer, Lena Klaaßen & Christian Stoll, *Energy Consumption of Cryptocurrencies Beyond Bitcoin*, 4 JOULE 1843 (2020).

[72] Harald Vranken, *Sustainability of Bitcoin and Blockchains*, 28 CURRENT OP. ENV'T. SUSTAINABILITY 1 (2017).

consumes in 18 days,[73] 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.[74] This stands as a major change to network processes, and is tantamount to changing the entire system of government altogether.[75] 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 therefore 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.[76] 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,[77] 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 become 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

---

[73] Christophe Schinckus, *The Good, the Bad and the Ugly: An Overview of the Sustainability of Blockchain Technology*, 69 ENERGY RES. SOC. SCI. 101614 (2020); Karl J. O'Dwyer & David Malone, *Bitcoin Mining and its Energy Footprint* (2014); Vranken, *supra* note 72.

[74] Fahad Saleh, *Blockchain Without Waste: Proof-of-Stake*, 34 REV. FIN. STUD. (forthcoming 2021).

[75] Vitalik Buterin & Virgil Griffith, *Casper the Friendly Finality Gadget*, ETHEREUM FOUNDATION (2017).

[76] Barton E. Lee, Daniel J. Moroz & David C. Parkes, *The Political Economy of Blockchain Governance*, 34 REV. FIN. STUD. (forthcoming 2021).

[77] Roman Beck, Christoph Müller-Bloch & John Leslie King, *Governance in the Blockchain Economy: A Framework and Research Agenda*, 19 J. ASS'N. INF. SYS. 1020 (2018); Wessel Reijers et al., *Now the Code Runs Itself: On-Chain and Off-Chain Governance of Blockchain Technologies*, TOPOI (Dec. 17, 2018); Alastair Berg & Chris Berg, *Exit, Voice, and Forking*, 8 COSMOS AND TAXIS 76 (Feb. 13, 2020).

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 prefer. 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.[78] 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,[79] 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.[80] 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, 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 the proposed LAN technologies had different technical features intended to

---

[78] *See* Alston, *supra* note 28 at 12.

[79] Paul A. David & Shane Greenstein, *The Economics of Compatibility Standards: An Introduction to Recent Research,* 1 ECON. INNOVATION AND NEW TECH 3 (1990).

[80] The general history of LAN standards has been recorded and analyzed in some detail. For analyses of the development of LAN technologies *see* Marvin Sirbu & Kent Hughes, *Standardization of Local Area Networks*, FOURTEENTH ANN. TELECOMM. POL'Y RSCH. CONF. (1986); Martin BH Weiss & Marvin Sirbu, *Technological Choice in Voluntary Standards Committees: An Empirical Analysis*, 1 ECON. INNOVATION & NEW TECH. 111 (1990); Urs Von Burg & Martin Kenney, *Venture Capital and the Birth of the Local Area Networking Industry*, 29 RES. POL'Y 1135 (2000).

prioritize certain tradeoffs in network processes over other ones.[81] 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. 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.[82] Thus, the ideal of having a single LAN standard was incompatible with the diversity of uses to which this technology would be applied.

A diversity of governance standards (as defined by protocol design choices) created the need for interfacing between the different networks, an example of the competitively polycentric nature of network governance by protocol. 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.[83]

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.[84] Heterogeneity of constituents is linked to increased benefits of subsidiarity, but given sufficient heterogeneity, entirely discrete governance units might indeed be optimal.[85] Accordingly, heterogeneity is a potential challenge within a permissionless blockchain, and the initial constitutional framework may act like an "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

---

[81] 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.

[82] Ethernet was developed with office automation functions in mind, where loads are variable and priority communications are 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.

[83] *See* Vitalik Buterin, *Chain Interoperability*, R3 RSCH. (Sept. 9, 2016); Rafael Belchior, et al., *A Survey on Blockchain Interoperability: Past, Present, and Future Trends*, ARXIV (May 28, 2020) https://arxiv.org/abs/2005.14282.

[84] Alberto Alesina & Enrico Spolaore, *On the Number and Size of Nations*, 112 Q. J. ECON. 1027 (1997); Alberto Alesina, William Easterly & Janina Matuszeski, *Artificial States*, 9 J. EUR. ECON. ASS'N. 246 (2011).

[85] Eric Alston, *Demand for Constitutional Decentralization* (2020), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3406947.

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 the realm of theory, although there has been considerable scholarly interest in the process of forking itself.[86] 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.[87] 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.[88] 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.[89] When malicious actors were able to steal tens of millions in Ether[90]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.[91]

These forks have been chosen as examples because they surround some of the most prominent (and highly market-capitalized) cryptocurrencies, but as importantly, the forks resulted 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.[92] This signals that for a sufficient proportion of

---

[86] Lee, et al., *supra* note 76; Vojislav B. Mišić, Jelena Mišić & Xiaolin Chang, *On Forks and Fork Characteristics in a Bitcoin-Like Distribution Network*, *in* 2019 IEEE INT'L CONF. BLOCKCHAIN 212 (2019); Yahya Shahsavari, Kaiwen Zhang & Chamseddine Talhi, *A Theoretical Model for Fork Analysis in the Bitcoin Network*, *in* 2019 IEEE INT'L CONF. BLOCKCHAIN (BLOCKCHAIN) 237 (2019).

[87] Yujin Kwon et al., *Bitcoin vs. Bitcoin Cash: Coexistence or Downfall of Bitcoin Cash in* 2019 IEEE SYMP. SEC. & PRIV. 935 (2019).

[88] Jimmy Song, *Bitcoin Cash: What You Need to Know*, MEDIUM (July 24, 2017), https://medium.com/@jimmysong/bitcoin-cash-what-you-need-to-know-c25df28995cf.

[89] Muhammad Izhar Mehar et al., *Understanding a Revolutionary and Flawed Grand Experiment in Blockchain: The DAO Attack*, 21 J. CASES INF. TECH 19 (2019).

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

[91] Alston, *supra* note 28 at 155–56.

[92] COINMARKETCAP, https://coinmarketcap.com (last visited Jan. 23, 2020).

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.[93] 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.[94] Among these subsidiary processes are "smart" contracts, self-enforcing contracts that exist on a blockchain.[95] 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.[96] DAOs promise to realize digitally the view of firms as a nexus of contracts,[97] 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 individuals and machines, with rules that are determined beforehand and not subject to manipulation.

Yet as discussed above, 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 dynamics are greatly defined by its protocol design choices, which include its chosen consensus

---

[93] Buterin, *supra* note 16.

[94] Alexander Savelyev, *Contract law 2.0: 'Smart' Contracts as the Beginning of the End of Classic Contract Law*, 26 INF. COMM. TECH. LAW 116 (2017); Daniele Magazzeni, Peter McBurney & William Nash, *Validation and Verification of Smart Contracts: A Research Agenda*, 50 COMPUTER 50 (2017); Reggie O'Shields, *Smart Contracts: Legal Agreements for the Blockchain*, 21 N. C. BANK. INST. 177 (2017); Marc Hamilton, *Blockchain Distributed Ledger Technology: An Introduction and Focus on Smart Contracts*, 31 J. CORP. ACCT. FIN. 7 (2020).

[95] Buterin, *supra* note 16.

[96] DE FILIPPI AND WRIGHT, *supra* note 14.

[97] Michael C. Jensen & William H. Meckling, *Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure*, 3 J. FIN. ECON. 305 (1976); OLIVER E. WILLIAMSON, THE MECHANISMS OF GOVERNANCE (1996); Ronald H. Coase, *The Nature of the Firm*, 4 ECONOMICA 386 (1937).

mechanism and the possibility of forking to better accommodate heterogeneity of network participants, as we have detailed in this section.

IV. 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 the medium term.[98] 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.[99] 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.[100] This means the extent to which a potentially highly decentralized system is decentralized in practice can vary quite widely.[101] 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) give 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.[102]

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.[103] Specific political institutional design choices in the United States' otherwise decentralized political system have centralized power on certain margins, resulting in the functional

---

[98] De Filippi & Loveluck, *supra* note 42.

[99] Zohar, *supra* note 67.

[100] OSTROM, UNDERSTANDING INSTITUTIONAL DIVERSITY, *supra* note 20 at 138.

[101] LIESBET HOOGHE ET AL., MEASURING REGIONAL AUTHORITY: A POSTFUNCTIONALIST THEORY OF GOVERNANCE (2016).

[102] De Filippi & Loveluck, *supra* note 42.

[103] GARY W. COX, MAKING VOTES COUNT: STRATEGIC COORDINATION IN THE WORLD'S ELECTORAL SYSTEMS (1997).

dominance of two political parties.[104] 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.[105] 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, mfvajor 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 crypto institutional scholars) is that of moving away from a proof-of-work to a proof-of-stake consensus algorithm. The importance of such a change, and likelihood that the implementation of the consensus mechanism will require ongoing adjustment, have 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.[106] Interestingly, the transition to the new network relies on a sufficient number of individuals already well-vested in Ether (or willing to commit costly capital to do so) voting with their money to validate the new network in its entirety. 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).[107] Ethereum has a public process by which proposals can be submitted, and

---

[104] ALSTON ET AL., *supra* note 21 at 197–205.

[105] Reijers et al., *supra* note 77.

[106] *See* BEANCONSCAN (last visited Jan. 23, 2021) https://beaconscan.com/ for the beacon chain network. For a discussion of updates, *see* Danny Ryan, *Eth2 Quick Update No. 14*, ETHEREUM BLOG (last visted Jan. 23, 2021) https://blog.ethereum.org/2020/08/03/eth2-quick-update-no-14/; *Development Update #4 – ethereum.org*, ETHEREUM BLOG (last visited Jan. 23, 2021) https://blog.ethereum.org/2020/08/05/ethereum-dot-org-development-update-4/.

[107] Jonas Valbjørn Andersen & Claire Ingram Bogusz, *Self-Organizing in Blockchain Infrastructures: Generativity Through Shifting Objectives and Forking*, 20 J. ASS'N. INFO. SYS. 4 (2019).

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.[108] In contrast, Bitcoin improvement proposals are submitted to an email listserv and then posted by Bitcoin developers on a public Github page.[109] 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.[110] 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. As is evident from the proposed and accepted proposals in the case of Bitcoin[111] and Ethereum,[112] a small group of individuals plays a large role in proposing successful 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.[113] Similarly, in permissionless cryptocurrency communities, there is considerable discussion surrounding the intended benefits a given proposal will provide, which tends to track the magnitude of change the proposal entails for the network itself.[114] 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

[108] Hudson Jameson, *Ethereum Protocol Development Governance and Network Upgrade Coordination*, SOUPTACULAR, http://souptacular.github.io/2020-03-23-ethereum-protocol-development-governance-and-network-upgrade-coordination/.

[109] De Filippi & Loveluck, *supra* note 42.

[110] Jameson, *supra* note 108.

[111] *Bitcoin Improvement Proposals*, GITHUB, https://github.com/bitcoin/bips.

[112] *Ethereum Improvement Proposals*, ETHEREUM, https://eips.ethereum.org/.

[113] Arruñada & Garicano, *supra* note 61; Luther & Smith, *supra* note 22.

[114] In the case of EIPs, a change that only affects a subsidiary protocol layer 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, we have discussed how 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.

processes, which surround the administration or application of a law that has already been enacted, "enactment" is necessarily final for a given blockchain. This stage of governance thus stands as more akin to public consultation than to legislative processes in a formal institutional sense.

V. COMPETITIVE GOVERNANCE OF CRYPTOCURRENCY BLOCKCHAINS

One feature distinguishing permissionless 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 a costly option. It is similarly costly 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 their value is a function of the size of the user bases. 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,[115] and is also deemed the ability to vote with one's feet.[116] 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.

The ideology that governance can be entirely replaced by algorithms does not appear to be realistic. For example, the block size limit debate triggered a governance crisis within the Bitcoin circle,[117] the failure to identify selfish miners,[118] and other unforeseen challenges in security, scalability, and vulnerabilities.[119] All these challenges require collective decisions and thus require some measure of conventional governance along the lines that we have described thus far. For example, as bitcoin miners have consolidated into large mining pools, mining activities are now practically centralized.[120] In the development layer, the

[115] Charles M. Tiebout, *A Pure Theory of Local Expenditures*, 64 J. POL. ECON. 416–424 (1956); ALBERT O. HIRSCHMAN, EXIT, VOICE, AND LOYALTY: RESPONSES TO DECLINE IN FIRMS, ORGANIZATIONS, AND STATES (1970).

[116] ILYA SOMIN, FREE TO MOVE: FOOT VOTING, MIGRATION, AND POLITICAL FREEDOM (2020); Ilya Somin, *Foot Voting, Political Ignorance, and Constitutional Design*, 28 SOC. PHIL. POLICY 202–227 (2011).

[117] Chris Berg, Sinclair Davidson & Jason Potts, *Institutional Discovery and Competition in the Evolution of Blockchain Technology* (2018).

[118] Ittay Eyal & Emin Gün Sirer, *Majority is not Enough: Bitcoin Mining is Vulnerable*, INT'L CONF. FIN. CRYPTOGRAPHY & DATA SEC. 436 (2014).

[119] Felix Irresberger, Kose John & Fahad Saleh, *The Public Blockchain Ecosystem: An Empirical Analysis* (Sept. 27, 2020), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3592849.

[120] De Filippi & Loveluck, *supra* note 42.

core developers also have concentrated power.[121] Because of this, one lens to understand the competitive dynamics between permissionless cryptocurrencies (and other close substitutes) is as competing firms in the market. This is especially true when one considers these networks through the lens of organizations competing for similar to identical user bases. Some scholars[122] consider the governance of blockchain as a political process in which users vote with their feet that in turn determines which fork would survive. However, a key distinction between electoral and market processes is that all users consume the same product after the election, but each user consumes the product of their choice in the market. Network externalities might be present where the product (e.g., Bitcoin) is more useful when more people are using it. But the consumer still consumes their choice as compared to the available alternatives in a given period. Therefore, the competitive governance of cryptocurrencies must by necessity draw lessons from the study of firm governance, product differentiation, and product competition in the field of industrial organization.

In the terminologies of industrial organization in economics, competition can present itself in the vertical (quality) dimension or the horizontal (product differentiation) dimension.[123] 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.[124] 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. 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.[125]

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. Even if current technology might not allow a single provider to dominate the market, the market forces may speed up the development of new

[121] Böhme et al., *supra* note 13.

[122] *E.g.*, Lee, *supra* note 76.

[123] *See generally* Harold Hotelling, *Stability in Competition*, 39 ECON. J. 41 (1929).

[124] Market capitalization as of Tue, 16 Jun 2020 19:00:00 UTC. For real time updates *see Global Charts, Total Market Capitalization*, COINMARKETCAP (last visited Jan. 23, 2021) https://coinmarketcap.com/charts/.

[125] Martin Garriga et al., *Blockchain and Cryptocurrencies: A Classification and Comparison of Architecture Drivers*, ARXIV (July 23, 2020).

technology or new rules. This suggests the possibility that in markets where digital currencies are highly substitutable, market forces may consolidate the networks into a natural monopoly as much as the technology allows. For many purposes surrounding scarce units of digital value, the nearly identical nature of these units makes these networks have characteristics similar to other highly concentrated network industries.[126] As the number of dominant players decreases, the constraints in governance from the competition could thus relax over time, although the necessarily dynamic nature of governance suggests that governance choices on these networks will continue to matter just as private firms require ongoing adjustment to their governance institutions on the margins.[127] 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.

But there are important ways in which competitive governance forces are likely to vary within permissionless cryptocurrency networks due to their unique protocol and subsidiary governance equilibria. Permissionless blockchains vary from firms in a variety of structural ways. There are no residual benefits from network activity that are then dispersed between owners and managers. Indeed, there are no owners and managers – people just transact in and hold the output of the network. This has implications for competition because presumably one network's choices are influenced by their competitor's choices. But how these choices are implemented (say, for a given protocol update) is directly a function of the structure of the permissionless network, which is not like a decision being wrought by a CEO or a company board and its shareholders. Therefore, the competitive forces in a context where "firm" decisions occur via a very different process are likely to themselves be influenced by this variation.

The very process by which decisions are made on permissionless cryptocurrency networks is structurally distinct. This has implications for the way they compete, especially when it comes to governance itself.[128] The structure of collective decision making itself matters in addition to the observed level of centralization at any given point in time. Market participants allocating resources for something other than immediate consumption intend to realize benefits, but the nature of the relationship between founders, ongoing "managers" (permissionless blockchain network participants), and investors (users and participants) is significantly different than in the case of startups and publicly traded firms. The distinct nature of this relationship means governance within and between permissionless cryptocurrencies differs in important ways. If a founder knows an investor has no legal recourse against them and can only divest their crypto as a means of exit, this results in significantly different incentives than the case where the founder has distinct (and well

[126] Florian Tschorsch & Björn Scheuermann, *Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies*, 18 IEEE COMMC'N. SURV. TUTORIALS 2084 (2016).

[127] Berg et al., *supra* note 27 at 196; *See generally* Cowen, *supra* note 27.

[128] Democratic political systems vary considerably as to their level of contemplated (and realized) decentralization, but that does not render them autocratic on the side of more centralization of authority. *See* HOOGHE ET AL., *supra* note 101.

understood) fiduciary duties as against their sources of capital. Any informed investor also knows this, so their incentives are also directly influenced by the ongoing governance structure implicated by permissionless blockchains.

Exit costs are currently quite low for cryptocurrency network participants, but a concern is that this 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.[129] 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. Finance scholars have explored 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 to increased participation in governance by active 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.[130] This split between two classes of stakeholders with the ability to exit a given public company 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.

VI. SUPERIOR GOVERNANCE OF CRYPTOCURRENCY BLOCKCHAINS

Permissionless blockchain networks are also subject to superior governance forces. While permissionless cryptocurrencies may not be

---

[129] Laila Metjahic, *Deconstructing the DAO: The Need for Legal Recognition and the Application of Securities Laws to Decentralized Organizations*, 39 CARDOZO L. REV. 1533, 1544–46 (2018).

[130] *See generally* Alex Edmans, Vivian W. Fang & Emanuel Zur, *The Effect of Liquidity on Governance*, 26 REV. FIN. STUD. 1443 (2013).

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.[131] Blockchain reduces certain narrow classes of contracting costs, thereby reducing the demand for lawyers - hence, increasing access - though the costs are shifted to up front contracting, such as the extent to which blockchain network user interfaces are easily accessible. Yet even if certain classes of contracts are more tractable to automated execution, there will inevitably be disputes. Such considerations have led to calls for *lex cryptographia* - a flattening of law to adapt to a changing environment.[132]

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?[133] 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,[134] 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,[135] although the tax status of the rewards for mining

---

[131] Eric Alston, *Blockchain and the Law: Legality, Law-like Characteristics, and Legal Applications*, *in* HANDBOOK ON BLOCKCHAIN AND CRYPTOCURRENCIES (James Caton ed., 2020).

[132] HADFIELD, *supra* note 29; Gillian K. Hadfield & Iva Bozovic, *Scaffolding: Using Formal Contracts to Support Informal Relations in Support of Innovation*, WIS. L. REV. 981 (2016); Werbach & Cornell, *supra* note 19.

[133] Charles Draper, *Cryptocurrencies: Practical Considerations in Insolvencies*, THE NAT'L L. REV., (2019), https://www.natlawreview.com/article/cryptocurrencies-practical-considerations-insolvencies.

[134] Werbach & Cornell, *supra* note 19; Guido Governatori et al., *On Legal Contracts, Imperative and Declarative Smart Contracts, and Blockchain Systems*, 26 ARTIFICIAL INTELLIGENCE L. 377 (2018).

[135] Kyleen Prewett, Roger W. Dorsey & Gaurav Kumar, *A Primer on Taxation of Investment in Cryptocurrencies.*, 36 J. TAX'N. INV. (2019).

cryptocurrencies remains less settled.[136] 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. In contrast, though, many cryptocurrencies which intended to ultimately be permissionless have run afoul of securities law in the United States surrounding 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.[137]

Implicit in most of our discussion thus far of the superior governance mechanisms to which a given permissionless blockchain network is subject is these networks' treatment under U.S. law. From this discussion the more general point should be made that the jurisdiction in which a given cryptocurrency user, network participant, or exchange owner resides or does business will by definition determine the jurisdictional authorities to which that individual is subject. Laws governing the possession of cryptocurrency vary significantly; in some countries it is illegal to hold or exchange cryptocurrencies. In others, individuals can hold or exchange them, but larger financial institutions are prohibited from doing so. Increasingly, though, regulatory authorities around the world have come to permit the holding and exchange of cryptocurrencies, although individuals are required to declare realized gains for income tax purposes, and more sophisticated organizations engaging in the space are subject to even larger disclosure and other requirements.[138] In the United States, for example, permissionless cryptocurrencies are considered commodities, and are accordingly subject to oversight from the CFTC.[139] However, permissionless cryptocurrencies are also increasingly subject to regulation by subnational jurisdictions (especially centers of financial activity like New York City).[140] Other jurisdictions, ranging from states like Wyoming to countries like Estonia, Malta and Switzerland, have developed explicitly welcoming regulations for permissionless cryptocurrencies (and larger economic ecosystem that surrounds them).[141]

Due to the relative complexity of the network processes of permissionless blockchains, they have presented a challenge to regulatory authorities and the law more generally since their inception. Nonetheless, because permissionless cryptocurrencies implicate stores of economic value as exchanged between individuals within and across

---

[136] Gamze Öz Yalaman & Hakan Yıldırım, *Cryptocurrency and Tax Regulation: Global Challenges for Tax Administration*, *in* BLOCKCHAIN ECON. AND FIN. MKT. INNOVATION 407 (Umit Hacioglu ed., 2019).

[137] Michael Mendelson, *From Initial Coin Offerings to Security Tokens: A US Federal Securities Law Analysis*, 22 STAN. TECH. L. REV. 52 (2019).

[138] Alston, *supra* note 41.

[139] CFTC, *Federal Court Finds that Virtual Currencies Are Commodities* (2018), https://www.cftc.gov/PressRoom/PressReleases/7820-18 (last visited Aug 13, 2020).

[140] Bradford H. Buck, *The Regulation of Virtual Currencies in The United States*, 40 NORTH EAST J. LEG. STUD. (2020); Greg Strong & Rodrigo Seira, *Aspects of State Securities Regulation.*, *in* GLOBAL LEGAL INSIGHTS – BLOCKCHAIN & CRYPTOCURRENCY REGULATION (Josias Dewey ed., 2019).

[141] Mikayla Novak, *Crypto-Friendliness: Understanding Blockchain Public Policy*, J. ENTREPRENEURSHIP. PUB. POL'Y (2019).

jurisdictions, the application of some bodies of law to these networks was inevitable. But the effective application of legal and regulatory authority requires enforcement, which makes the capacity of the enforcement authorities in a given jurisdiction a key consideration in addition to the formal legal status of a permissionless cryptocurrency within a given jurisdiction. The pseudonymous nature of permissionless cryptocurrency transactions has made them popular for a variety of criminal purposes, including drug transactions, tax avoidance and evasion, and truly sinister crimes such as murder-for-hire and child pornography.[142] In places like Venezuela, the comparative inability of the government to track cryptocurrency transactions makes them an attractive alternative, in great due to the comparative instability of the Venezuelan currency itself.[143] However, the nature of exchanging economic value typically carries a number of additional signifiers concomitant to the actual exchange of value as payment. Therefore, enforcement authorities in jurisdictions of high state capacity have typically been able to uncover the identity of someone attached to a wide variety of cryptocurrency transactions, although doing so requires a high level of technical sophistication and an associated financial cost, which places this level of enforcement beyond the ability of many enforcement authorities around the world.[144]

Ultimately, 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. Our analysis of these forces would therefore be incomplete absent our treatment here of the governance forces superior to any given permissionless blockchain network.

CONCLUSION

Ledgers for centuries were centralized, with trust placed in firms or governments.[145] Permissionless blockchains are a uniquely decentralized system to record information. Despite the novelty of permissionless blockchains, governance dilemmas arise within these organizations, and each cryptocurrency blockchain is further nested within higher-level institutions. There is also a diversity of governance

---

[142] Olga Kharif, *Bitcoin Criminals Set to Spend $1b on Dark Web This Year*, BLOOMBERG (July 2, 2019, 3:33 PM); Sean Foley, Jonathan R. Karlsen & Tālis J. Putniņš, *Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed Through Cryptocurrencies?*, 32 REV. FIN. STUD. 1798 (2019).

[143] Mathew Di Salvo, *Why are Venezuelans Seeking Refuge in Crypto-Currencies?*, BBC NEWS (March 19, 2019), https://www.bbc.com/news/business-47553048.

[144] Simon Dyson, William J. Buchanan & Liam Bell, *The Challenges of Investigating Cryptocurrencies and Blockchain Related Crime*, 1 J. BR. BLOCKCHAIN ASS'N. 1 (2018).

[145] DOUGLAS W. ALLEN, THE INST. REVOLUTION: MEASUREMENT AND THE ECONOMIC EMERGENCE OF THE MODERN WORLD (2012).

design choices in practice across permissionless blockchains, which reflects the competitive nature of cryptocurrency markets.

Our analysis clarifies that a permissionless blockchain is much like any other complex organization: organizations require rules, and the performance of blockchains depends on how the blockchain itself interacts with governance alongside and above it. Cryptocurrency blockchains shape users' and participants' incentives through protocol choices, which creates units of governance subsidiary to each protocol. Beyond protocol, there is governance that is competitive and superior to each permissionless cryptocurrency blockchain network that shape outcomes as well. Competitive forces contribute to a diversity of institutional arrangements of permissionless blockchains – rejecting any view of institutional isomorphism – while the superior forces operate to constrain and enable permissionless blockchains. In this regard, these networks are at their core polycentric, nested enterprises. They require legal governance superior to the network, as well as internal governance to overcome dilemmas identified through the institutional analysis of organizations more generally.

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. This is because 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.[146] 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 a 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 an analytical framework for cryptocurrency legal scholars, practitioners, and users to begin to understand, let alone predict, governance outcomes in practice. Which set of network participants support a specific objective of network processes, and what are their reasons for doing so resultant from their incentives and the larger institutional context?

Our analysis therefore provides a more comprehensive starting point for regulators and legal practitioners to begin to define the boundaries of these emerging asset classes in practice. To understand the likely effects of recent changes in custody rules for national banks for cryptocurrencies,[147] a broad understanding of these permissionless blockchain networks' structure and ongoing governance processes is necessary. To consider the likely effects of ongoing monetary and fiscal policy choices in major market democracies on cryptocurrency market

[146] Aligica & Tarko, *supra* note 20; Vlad Tarko, *Institutional Complexity and the Public Choice Analysis of Feasible Policy Changes*, *in* OSTROM'S TENSIONS: REEXAMINING THE POL. ECON. AND PHIL. OF ELINOR C. OSTROM 147 (Roberta Q. Herzberg, Peter J. Boettke & Paul Dragos Aligica, eds., 2019).

[147] Hailey Lennon, *Bitcoin Meets Banking As U.S. Bank Regulator Permits Cryptocurrency Custody*, FORBES (July 22, 2020) https://www.forbes.com/sites/haileylennon/2020/07/22/bitcoin-meets-banking-as-us-bank-regulator-permits-cryptocurrency-custody/#2383339c5479.

capitalizations,[148] an understanding of the competitive and superior governance forces to which these networks are subject is necessary. As a final example, as central banks and private companies consider the issuance of their own digital currencies,[149] how will these currencies' governance features compare to those that have come to predominate[150] in cryptocurrency markets? The continued need for bankruptcy, tax and criminal courts to deal with questions that implicate cryptocurrencies and their governance structures is increasingly clear. But the need to apply granular contract law, for example, to new contexts requires an understanding of the different incentives and expectations of users within a given market and asset class. When a court is called upon to adjudicate a dispute surrounding millions of dollars of economic value implicated by the algorithmic processes of a blockchain-supported DAO, lawyers and judges will benefit from a clearer understanding of the diverse governance forces to which permissionless blockchain networks are subject.

---

[148] Shaen Corbet et al., *Cryptocurrency Reaction to FOMC Announcements: Evidence of Heterogeneity Based on Blockchain Stack Position*, 46 J. FIN. STAB. 1 (2020); Thai Vu Hong Nguyen et al., *Asymmetric Monetary Policy Effects on Cryptocurrency Markets*, 48 RES. INT'L. BUS. FIN. 335 (2019).

[149] Jonathan Cheng, *China Rolls Out Pilot Test of Digital Currency*, WALL STREET JOURNAL (April 20, 2020), https://www.wsj.com/articles/china-rolls-out-pilot-test-of-digital-currency-11587385339; Sarah Allen et al., *Design Choices for Central Bank Digital Currency: Policy and Technical Considerations*, (Nat'l Bureau of Econ. Rsch., Working Paper No. 27634, 2020), https://www.brookings.edu/blog/up-front/2020/07/23/design-choices-for-central-bank-digital-currency/.

[150] Not all major digital or cryptocurrencies are supported by permissionless blockchains. Nonetheless, given the uniqueness of their governance structure (and in the interest of brevity), we confine our analysis of governance forces to this important (and dominant) class of cryptocurrencies.