Constitutions and Blockchains: Competitive Governance of Fundamental Rule Sets

Author:

Eric Alston[a]

March 2019

Working Paper 2019.003

[a] Scholar in Residence, Finance Division Faculty Director, Hernando de Soto Capital Markets Program, Leeds School of Business, University of Colorado Boulder

The Center for Growth and Opportunity at Utah State University

Abstract:

Constitutional rule sets determine how laws are enacted, administered, and adjudicated in a given society and are by design less subject to change than ordinary legislation. These rules' systemic importance means comparative constitutional design is not an understudied topic. But in the context of private governance—where rule sets are typically more fluid, centrally controlled, and exist in the shadow of law and regulation—developing generalizable insights about comparatively superior governance mechanisms is more difficult. I conclude that blockchains can be understood as a type of constitutional rule set that both defines and legitimizes the activities supported by the underlying permissionless distributed ledger technology. More specifically, I argue that the development of cryptocurrency blockchains has led to new forms of competition in private governance, which include exit costs as one of the fundamental margins upon which governance outcomes will be shaped between blockchains. I proceed by first reviewing insights from constitutional amendment processes and by also reviewing how comparatively more or less rigid constitutions have been linked to different outcomes in practice. I then describe the blockchains supporting major cryptocurrencies, identifying how the underlying network rules are similar to and distinct from constitutional rules. Next, I compare existing and proposed governance structures for blockchains, especially those supporting the cryptocurrencies Bitcoin and Ether, but also other permissionless use cases. My analysis not only identifies the choices in constitutional governance to which the proposed blockchain changes are analogous, but it also highlights the competitive benefits and costs that result, with a view to the intended functions of a given blockchain. Finally, I consider both the general trade-offs in governance created by competition between cryptocurrency blockchains and the surprising ways in which these unique competitive margins may influence downstream outcomes.

1. Introduction

Constitutions are the most famous example of what legal scholars refer to as secondary rules. More colloquially, secondary rules are the rules about making rules.[1] In the case of constitutions, these rule sets determine how laws are enacted, administered, and adjudicated in a given society. Constitutional rules are thus accorded a high level of importance in a given nation's legal system because they are quite literally the foundation upon which all subsequent legislation and government action rest. Because of constitutional rules' fundamental nature, these rules are by design less subject to change than ordinary legislation. In other words, constitutional rules are typically the most rigid rule set in a given legal system. Nonetheless, constitutions vary as to the means and ease by which they can be amended. Thus, the comparative flexibility of a given constitution is an institutional design choice that has long been treated in the scholarship on comparative constitutional design, which has linked flexibility both to endurance and to a diminished need for informal measures of constitutional adjustment.

Where there is a distinct understanding of the fundamental rules governing human interactions and transactions—perhaps because of the lack of a uniform standard of comparison and availability of underlying policies—is in the context of private governance. This may be in part because one of the benefits of firm structure is that decisions regarding policy change are typically validated through a centralized process, as opposed to a democratic one, which inherently creates less need for "governance of governance" in that the "law" is whatever the central firm authority says it is. From an economic perspective, the firm provides the quintessential example of private governance. Previous scholars such as Coase and Williamson have demonstrated how governance within the firm is an essential field of study for understanding economic outcomes.[2] The ubiquity of the firm as an organizational structure governing economic production has a corollary implication: the choice of private institutions by various firms provides a margin for competition. However, the extent to which firms can freely compete in terms of internal governance and the agreements struck with different employees and suppliers is an open question in a world of increased legislation and regulation of contractual agreements, especially in the case of publicly traded companies.

In a world of regulated and centralized firms, then, how do scholars derive insights about the comparative benefits of different choices in private governance institutions? The emergence of blockchains as the technology underlying cryptocurrencies provides a fruitful context in which to examine this question. The example of the different tensions faced by Ether and Bitcoin, and the different responses in terms of changes to the fundamental underlying structure of the blockchains supporting the two cryptocurrencies, suggests value in comparing how different mechanisms of blockchain governance result in different outcomes for cryptocurrencies and their intended functions. Using insights from constitutional amendment processes and their association with the endurance of constitutions and substantive outcomes in terms of constitutional jurisprudence, I explore the differences in blockchain governance mechanisms in this article. I conclude that blockchains can be understood as a type of constitutional rule set that both defines and legitimizes the activities supported by permissionless distributed ledger technology.[3] In particular, the exit costs defined by the "constitutional" regimes that blockchains define create a unique competitive margin that will shape the success of a given cryptocurrency as compared to others that make different governance choices.

I proceed by first reviewing the existing scholarship on constitutional amendment processes and by also reviewing how comparatively more or less rigid constitutions have been linked to different outcomes in

1 Lionel Adolphus Hart & Leslie Green, The Concept of Law (2012).

2 *See* Ronald Coase, *The Nature of the Firm,* 4(16) Economica 386–405 (1937); Oliver E. Williamson, *The Theory of the Firm as Governance Structure: From Choice to Contract,* 16(3) Journal of Economic Perspectives 172–95 (2002).

3 Other scholars have contemporaneously drawn a similar comparison to mine. *See, e.g.,* Shruti Rajagopalan, Blockchain & Buchanan: Code As Constitution (2019) (unpublished manuscript) (*in* James Buchanan, Theorist of Political Economy and Social Philosophy, (Palgrave MacMillan 2019). *See also* Alastair Berg, Chis Novak, & Mikayla Novak, *Blockchains and Constitutional Catallaxy* (December 4, 2018), *available at*: https://ssrn.com/abstract=3295477 or http://dx.doi.org/10.2139/ssrn.3295477.

practice. I then provide a brief description of blockchains supporting major cryptocurrencies, identifying the ways in which the underlying network rules are similar to and distinct from constitutional rules. Next, I compare existing and proposed governance structures for blockchains, especially those supporting the cryptocurrencies Bitcoin and Ether, but also other permissionless use cases. My analysis identifies not only the choices in constitutional governance to which proposed blockchain changes are analogous, but also the competitive benefits and costs that result, with a view to the intended functions of a given blockchain. Finally, I consider the trade-offs in governance that competition between cryptocurrency blockchains creates, examining how these unique competitive margins can influence downstream outcomes.

2. Constitutional Rules and Amendment

The principal bulk of our behavior is not governed directly by constitutional rules. Instead, our behavior is governed by the legislative, executive, and judicial output of public organizations defined by these constitutional rules. It is in this sense that "the rules about making rules" are secondary, as Hart described them.[4] Our primary day-to-day activities and the majority of our disputes and prohibited actions are governed by primary rules; secondary rules instead define the system that writes, administers, and adjudicates the primary rules governing our behavior. This is because there are significant benefits to agreeing to the means by which subsequent rules will be defined and changed. If, instead, every rule change also required a debate over the means by which the rule would be defined, creating new rules would be much harder, if not impossible. This is because if one actor foresaw an outcome that they did not prefer under the means by which rules were likely to be made, they would instead focus their objections on changing the process. A multi-tiered rule process focuses the margins of political competition on a more narrow set of issues, once the rules of the game have been agreed upon.[5] Put differently, the game cannot be played if no one agrees on the underlying rules. This is the essential argument for the ubiquitous emergence of constitutional rule sets in governance systems around the world.[6]

But what happens if the players of the game sufficiently agree the rules need to be changed? The realization that constitutional rules may not be perfectly articulated for all time has led to the need for amendment rules. Relatedly, constitutional rule sets' supremacy has an important corollary: the costs of exiting these rule sets are among the highest. Moving from state to state can allow a citizen considerable choice as to the rules governing their behavior; the rules of the United States Constitution are not among those that change from state to state. Thus, the higher the exit costs, the more important the process of dynamic constitutional legitimization becomes, and vice versa.[7] Therefore, amendment rules create a space within which the constitution can be changed, defined at one extreme by making a constitution unamendable, and at the other, by making constitutional change subject to the same requirements as ordinary legislation. At the extreme of unamendability, constituents would have considerable certainty as to the finality of constitutional rules governing them at any given time, while at the other, constituents could easily adapt the constitution to suit new circumstances and changing beliefs surrounding governance.[8] The fundamental underlying trade-off associated with constitutionalizing rules is clarified through this theoretical trade-off, which in practice strikes a balance between these two extremes. As one scholar has noted, though,

4 Hart and Green, *supra* note 1.

5 *See, e.g.*, James M. Buchanan, *The Relatively Absolute Absolutes, in* The Logical Foundations of Constitutional Liberty 448–50 (1999). *See also* Jonathan Riley, *Constitutional Democracy as a Two-Stage Game*, *in* Constitutional Culture and Democratic Rule 147–50 (2001).

6 For a thorough treatment of why constitutional rule sets could emerge as the result of purely self-interested decisions among constituents (an assumption made throughout this article about the incentives and beliefs of blockchain network participants and users), *see* James M. Buchanan & Gordon Tullock, The Calculus of Consent 60–80 (2004).

7 Exit costs have long been identified as a central determinant of the institutions of governance that emerge in both public and private organizations. *See* Albert Hirschman, Exit Voice and Loyalty: Responses to Decline in Firms, Organizations, and States (Harvard University Press, 1970). These costs have also been identified as important determinants of governance outcomes in the private sector. *See, e.g.*, Colin Mayer, *Corporate Governance and Performance,* 21(1) J. L & Soc'y. 152–76 (1997); John Coffee Jr., *Accountability and Competition in Securities Class Actions: Why Exit Works Better Than Voice,* 30 Cardozo L. Rev. 407 (2008).

8 Levinson Sanford, *Designing an Amendment Process*, *in* Constitutional Culture and Democratic Rule 272–74 (2001).

the need for constitutional amendment is so fundamental that "all constitutions admit the possibility of amendment,"[9] in great part because the option of exit is so costly for most individuals governed by a given constitution.

This first trade-off is necessarily defined by the choice of amendment rule or rules: a constitution can be comparatively more flexible or rigid, depending upon how difficult it is to amend.[10] This section emphasizes five core lessons from the comparative study of constitutional amendment processes worldwide: (i) constitutional flexibility has been linked to constitutional endurance, as well as a number of substantively and normatively important outcomes in subsequent political processes; (ii) amendment of amendment procedures themselves is more likely to signify major constitutional change; (iii) the act of making aspects of the constitution unamendable is expressive of deeply held beliefs on the part of the polity; (iv) consideration of amendment processes reveals the fundamental link between constitutional "beliefs" surrounding core governance principles and the written constitution itself; and (v) the need for constitutional change is a function of how well initial constitutional design choices dynamically facilitate economies of scale in governance while simultaneously minimizing agency costs.

Beyond the most basic structural trade-off between flexibility and rigidity, constitutional scholars have deepened the comparative understanding of choices of amendment rules. Thus, the trade-off between flexibility and rigidity has also been characterized as trading off between stability and flexibility;[11] but this characterization of stability is more focused on the stability of the underlying rule set, as opposed to the stability of governance overall. For example, the comparative flexibility of constitutions has been linked to increases in constitutional endurance.[12] The underlying intuition is a simple one: a constitution that faces more barriers to adjustment is less likely to be adaptable to changing circumstances in society, and hence, is more likely to provoke the need for wholesale constitutional overhaul in those cases where its fit is increasingly poor as compared to the needs and beliefs surrounding governance in society. Nonetheless, too much flexibility at some level undermines the basic principle of constitutionalism as a set of stable limits on ordinary politics.[13] However, the nature of constitutional jurisprudence provides an additional outlet by which constitutional change can occur: instead of amending the constitution, changing judicial interpretations of constitutional requirements can adjust the constitution to reflect changing social conditions. Because of the complexity of these trade-offs, constitutional scholars have focused on identifiable effects resultant from different amendment procedures, beyond the rate of change that more or fewer barriers to amendment imply.

9 Andrew Roberts, *The Politics of Constitutional Amendment in Postcommunist Europe,* 20 Const. Pol. Econ. 99 (2009).

10 Options in practice for amendment rules of comparatively more or less flexibility abound. If occurring via legislative change, adjustment of the threshold required for passage is a common choice, with a higher threshold accordingly making passage more difficult, and vice versa. Another margin defining the difficulty of amendment involves the extent to which different stakeholders' input is required in order for amendment to occur; if an amendment can only occur after it has successfully passed the legislative threshold and a popular referendum, this is more difficult than requiring either one of those options. Bjørn Erik Rasch & Roger D. Congleton, *Amendment Procedures and Constitutional Stability,* 12 Dem. Const. Design & Pub. Pol'y: Analysis and Evidence 536–49 (2006). Amendments can also require more than one successful passage, a requirement designed to increase the salience of the issue to any stakeholders who might favor or oppose the amendment. The assent of subsidiary authorities can also be required, as is the case with the United States; the much-bemoaned Article V requires the assent of state legislatures to any proposed changes to the constitution. *See* Levinson Sanford, Responding to imperfection: the theory and practice of constitutional amendment (Princeton University Press, 1995). Finally, separable amendment thresholds can be used to identify areas of the constitution subject to higher barriers to amendment, up to and including making certain aspects of the constitution unamendable altogether. Richard Albert, *The Expressive Function of Constitutional Amendment Rules,* 59(2) McGill L. J. 245, 235 (2013).

11 Nathalie Behnke & Arthur Benz, The Politics of Constitutional Change Between Reform and Evolution, 39 J. Federalism 213–81 (2009).

12 Zachary Elkins, Tom Ginsburg, & James Melton, The Endurance of National Constitutions (2009).

13 Id.

One such trade-off focuses on the extent to which the constitution includes high levels of detail as creating less need for downstream judicial interpretation.[14] This insight can also be examined empirically, for several scholars have linked the length and detail of constitution to the frequency of amendment.[15] A broader characterization of the institutional design trade-offs implicit to the choice of amendment rules surrounds the need for a constitution to adapt to new developments while entrenching the system from self-interested behavior;[16] at some point, amendment rules that are too flexible would mean none of the rules of the game are insulated from political pressures. Roger Congleton, a scholar who views constitutions as a bargain amongst powerful government actors (e.g., a legislature and a monarch or executive, typically), equates strengthening amendment rules with facilitating minority rights and the rule of law,[17] emphasizing the role of stability as a crucial input to the rule of law. Furthermore, the extent to which a given political system displays fragmentation of parties has been shown to interact with the nature of amendment procedures and the frequency.[18] The need for constitutional change has also been linked to political change and the dysfunctional performance of the existing constitutional regime.[19] Each of these insights displays the fact that amendment procedures (and the frequency of amendment the procedures create) exist in a complex dynamic with the political system in both prior and subsequent periods. This is no different in the case of blockchains—the rules for changing the underlying fundamental rule set are implicated in complex ways in the processes of governance and cryptocurrency output. In particular, constituents of blockchains face low exit costs, which provides an alternative to both enduring a rule set that is too rigid to change, as well as weathering changes of a greater frequency and magnitude than they would prefer.[20]

Furthermore, an important distinction exists in the literature between amending the constitution and amending the amendment procedures contained therein. A stable amendment procedure is a key measure of constitutional durability.[21] Changes to the constitution are expected, but changes to the means by which the constitution can be changed signal a very different kind of change. This is related to the fact that amendment rules have been characterized as directly expressing fundamental constitutional values.[22] Similarly, amendment processes themselves can be understood as having a revelatory function, whereby the basis for legitimacy of governance is revealed through both proposed and successful constitutional amendments.[23] Changing the means of amendment is thus more of a meta-amendment, as compared to the more common changes to the underlying structure, and may indicate that such a change implicates much more fundamental changes to governance than other amendments.[24] Different changes to cryptocurrency blockchains can be understood as implicating these concerns to very different degrees, as the discussion in

14 Albert, supra note 10. Depending on the rigidity of the amendment rule, judicial interpretation may achieve a high level of finality. In the United States, for example, only four Supreme Court rulings had been reversed by constitutional amendment by 1988. See, e.g., Louis Fisher, Constitutional Dialogues: Interpretation as Political Process 201 (1988). This trade-off between rigidity of amendment processes and informal means used to adapt the constitution to changing needs and circumstances has also been characterized as "reform" when change occurs via formal processes and as "evolution" when the change occurs through informal means. Nathalie Behnke & Arthur Benz, The Politics of Constitutional Change Between Reform and Evolution, 39(2) J. of Federalism 213–40 (2009).

15 Gabriel Negretto, Replacing and Amending Constitutions: The Logic of Constitutional Change in Latin America, 46 Law & Soc'y Rev 749–79 (2012); Elkins et al., supra note 12.

16 Tom Ginsburg & Eric A. Posner, Subconstitutionalism, 62 Stan. L. Rev. 1584–626 (2010).

17 Roger D. Congleton, Perfecting parliament: Constitutional reform, liberalism, and the rise of western democracy 287 (Cambridge University Press, 2010).

18 Gabriel Negretto, *Replacing and Amending Constitutions: The Logic of Constitutional Change in Latin America*, 46 Law & Soc'y Rev (2012).

19 *See*, *e.g.,* Negretto *supra* note 15; Norman Schofield, Architects of Political Change: Constitutional Quandaries and Social Choice Theory (2006).

20 Frequency of changes to a given blockchain network's rule set is already a margin defining distinct cryptocurrencies. Ethereum has changed its rules much more frequently than Bitcoin. *See* Primavera de Filippi & Aaron Wright, Blockchain and the Law: The Rule of Code 188 (Harvard University Press, 2018).

21 Rasch & Congleton, *supra* note 10.

22 Albert, *supra* note 10.

23 Richard Albert, *Nonconstitutional Amendments,* 22 Can. J. L. & Jurisprudence 5–47 (2009).

24 Not all changes to amendment procedures are necessarily so fundamental; Sweden's changes to its amendment procedures were a necessary consequence of reducing the number of chambers of the legislature, as opposed to being directly intended to significantly change the way the constitution could be changed in the future. *See* Congleton, *supra* note 10.

section VI emphasizes—some changes to blockchains are the equivalent of ordinary amendments, whereas others are the equivalent of changing amendment rules themselves.

Amendment rules have been characterized as necessarily corrective, recognizing the likelihood that a constitution will prove deficient in the light of unforeseen future events; instead of the inadequacy of a given constitution eventually leading to it being overturned and replaced, a second-best outcome is the adjustment of the constitution to prevent outright constitutional rupture.[25] Nonetheless, amendment procedures in practice can provide an expressive function in signaling those aspects of the constitution that are subject to a higher bar for change or are unamendable altogether.[26] Relatedly, the very act of amending a constitution raises the salience of the particular areas subject to amendment debates (as well as inflaming "constitutional passions," independent of the underlying political or social questions at issue).[27] If amendment proponents are successful, the act of amending a constitution increases the likelihood that government actors will be held accountable for the extent to which they adhere to new constitutional requirements. The ability to amend a fundamental charter also provides for dynamic legitimization; if those currently governed by a given constitution can change it, provided the need to do so is sufficiently agreed upon, then they are more likely to view the constitution as reflecting their needs and goals surrounding governance.

Constitutional law is different because its fundamental nature tends to require the clear articulation of the procedures required for change. Despite this fundamental need, scholars of amendment processes have long wrestled with the paradox of self-amendment. The question of where the authority comes from to amend the constitution, when the constitution itself defines its own amendment procedures, suggests a fundamental recursivity to constitutional amendment.[28] Related to this question is the emergence of a practice in many modern constitutional orders that permits the overturning of amendments that comply with the letter of constitutional procedures defining amendment processes but which are understood to be at odds with the spirit of the constitution.[29] A stylized example readily displays this tension. If the Constitution of the United States were amended to remove term limits for the president and the ability of Congress to override a presidential veto, this would stand as a fundamental alteration to the political system, at odds with the intent of constrained and balanced government as understood not only at the nation's founding but also in modern times.

This distinction between adherence to the letter of constitutional law and adherence to the principles that animated the creation of the constitutional order writ large has been well studied by constitutional scholars. Put simply, constituents in general, and political actors in particular, are guided by their beliefs as to what the constitution should (and should not) achieve.[30] Sufficient change to the underlying system of governance, even if strictly adherent to the amendment process specified in the constitution, has long been argued as capable of annihilating or eliminating the existing constitutional order altogether.[31] The justification for making some provisions unamendable clearly laid out the distinction between the unwritten constitutional principles that are crystallized through a constituent process into the written constitution: "the immutability of the principles…marked out a normative core that defined the constitutional identity

25 Richard Albert, The Expressive Function of Constitutional Amendment Rules, 59 McGill L.J. (2013).
26 Rasch & Congleton, supra note 10, at 542.
27 Rosalind Dixon & Tom Ginsburg, Deciding Not to Decide: Deferral in Constitutional Design, 9 Int'l J. Con. L. 636–72 (2011).
28 Peter Suber, The Paradox of Self-Amendment: A Study of Law, Logic, Omnipotence, and Change (1990).
29 Ulrich K. Preuss, The Implications of Eternity Clauses: The German Experience, 44 Isr. L. Rev. (2011).
30 Schofield, *supra* note 19, at 258–63.
31 Carl Schmitt, Constitutional Theory 150 (Duke University Press, 2008). Indeed, Schmitt's critique of the paradox created by substantively unconstrained amendment procedures has been linked to the emergence of unamendable provisions in the German Basic Law of 1949. *See, e.g.,* Ulrich K. Preuss, *The Implications of Eternity Clauses: The German Experience,* 44 Isr. L. Rev. 439 (2011). In particular, the emergence of the Nazi regime so at odds with the core constitutional principles that gave birth to the Weimar Republic in the first place led drafters of the Basic Law after World War II to adopt a specific substantive rigidity with respect to amendment: the government powers constituted by the Basic Law could not subsequently alter fundamental aspects of the structure of government. Put differently, no constitutional basis exists for changing these elements, and changing these elements would require the wholesale replacement of the Basic Law by German constituents through extra-constitutional means.

of the polity."[32] Unamendability thus serves a profound expressive function, albeit one that is fundamentally anti-democratic. Although unamendability provides a clear link between the formal constitution itself and the constitutional principles animating the creation of the written document, the existence of an underlying set of constitutional beliefs is not limited to contexts where a subset of fundamental rules are unamendable per se. Fundamental beliefs about blockchains' immutability and the need to punish bad actors stand as examples of these constitutional beliefs in the context of cryptocurrency communities, as the discussion in section V emphasizes.

Constitutional design writ large is seen as a trade-off between the economies of scale in governance that a single fundamental rule set creates and the agency costs associated with the necessarily representative government that governance at such a scale entails.[33] One of the fundamental challenges in constitutional design is to restrain the lawmaking power once this power has been vested in representative agents who are only periodically and at best imperfectly disciplined by the constituents whose governance preferences their choices ideally represent.[34] Of course, there is a dynamic element to these design choices, which implies that the fundamental rule set should, to the extent possible, minimize future transaction costs associated with governance to reduce the need for costly constitutional change.[35] This means a fundamental insight from the study of constitutions for design of fundamental rule sets is that these rule sets trade off between facilitating governance at scale (as well as the underlying processes being governed)[36] and creating principal-agent problems on the part of those individuals who directly take part in governance. In the case of permissionless blockchains, the network participants who process and validate cryptocurrency transactions are the equivalent of representative agents that are only constrained by the network rules and the choice of users to transact and store value in one cryptocurrency or another.

3. Blockchains and Governance

The blockchains supporting most major cryptocurrencies share two important definitional components: (i) changes to the underlying ledger update original entries in discrete blocks of information,[37] as opposed to overwriting them; and (ii) these changes to the ledger occur via a decentralized process among participants on a particular blockchain network.[38] The way in which decentralized updates to the common ledger occur is defined by the consensus algorithm put in place by a given blockchain. This consensus algorithm (the rules for determining how changes to the ledger occur) is part of the initial conditions that are coded into the architecture of the blockchain itself. In what is perhaps the most famous blockchain—that underlying Bitcoin— the consensus algorithm creates a race among network nodes ("participants")[39] to solve a

32 *Id.* at 441.
33 Ginsburg & Posner, *supra* note 16, at 1594–97.
34 Friedrich A. Hayek, THE CONSTITUTION OF LIBERTY 183–88 (1960).
35 Jonathan Riley, *supra* note 5, at 163–67.
36 For a discussion of law (including constitutional law) as a scalar mechanism facilitating social interactions and transactions, *see* Eric Alston, Lee Alston, Bernardo Mueller, & Tomas Nonnenmacher, Institutional and Organizational Analysis: Concepts and Applications, 307–16 (Cambridge University Press, 2018).
37 A blockchain is literally a chain of blocks of information (or code) referencing earlier states in the ledger duplicated across numerous network nodes.
38 A common misconception is that all blockchains use decentralized "permissionless" governance. In reality, many of the commercial applications already in use utilize permissioned blockchains, where a central authority grants permission to certain network nodes to make specific alterations to the underlying common ledger.. Supply chain innovations utilizing blockchain stand as a prominent example of this. All blockchains are a form of distributed ledger duplicated across numerous network nodes that can only be updated as opposed to amended, but only some blockchains are permissionless. For a discussion of blockchain's definitional properties, *see* Böhme, Rainer, Nicolas Christin, Benjamin Edelman, & Tyler Moore, *Bitcoin: Economics, Technology, and Governance,* 29(2) J. Econ. Persp. 213–38 (2015). *See also* Kevin Werbach, The Blockchain and the New Architecture of Trust 58–63 (MIT Press, 2018).
39 Network nodes are often referred to as miners because their incentives to process transactions are created by a reward of new units of the cryptocurrency. Throughout this piece I will refer to the individuals in control of these nodes as network participants, because of their role in the production, processing, and verifying of cryptocurrency transactions. Individuals who use cryptocurrency to transact or store value are instead network users, because they play no direct role in the maintenance of the network (unless they are also a network participant).

cryptographic hash function,[40] a method that, while largely secure against fraudulent attempts to update the ledger to reflect Bitcoins that do not exist,[41] is graphics processor-intensive and so consumes considerable amounts of energy.[42] This particular consensus algorithm, known as proof-of-work ("PoW"), operates in a winner-take-all fashion—when one network participant has successfully solved the cryptographic puzzle, the rest of the nodes that were processing potential solutions to the hash function are effectively back to square one. From the perspective of these miners, the energy expended in processing network users' transactions receives no reward until their set of proposed changes to the Bitcoin ledger is accepted through their successful resolution of the hash function.[43] Because each network participant's processor is engaged in an electrically costly race to solve the cryptographic puzzle, this method of achieving consensus over proposed changes to the network ledger is called "proof-of-work;" a successfully proposed block represents proof of energy expended to validate network transactions. To the layperson, this means processing transactions on the Bitcoin network is very electricity intensive, and only more so as the value of Bitcoin increases and more participants compete to receive a fixed amount of Bitcoins for each successful resolution of the hash function.[44] Because anyone who has a sufficiently powerful computer, internet access, and electricity can become a network participant, this makes these type of blockchains permissionless, meaning no central authority controls who can make changes to the network ledger.

What the choice of the PoW consensus algorithm has done for Bitcoin is to drive a wedge between its initially proposed dual functions as a store of value and a payment network. Bitcoin's increasing salience to potential adopters has made it an increasingly successful store of value (with the exception of the price volatility[45] associated with speculative interest and regulatory interventions in a variety of countries), but this increase in value has created problems for Bitcoin's ability to serve as a competitive payment network, given the cost and time required to process a single transaction. This has led to considerable debate within the Bitcoin community itself surrounding how to overcome these problems that are a direct result of the initial choice of consensus algorithm.[46] In the case of Bitcoin, changes to the rules governing the blockchain network's processes occur through a fork in the blockchain itself,[47] which is successful if a majority of other network nodes accept the new code as changed, as compared to the original code.[48] This has led to difficulties in successfully changing the underlying architecture of the network. While this is not to say a given proposed fork in the Bitcoin blockchain should or should not have occurred, a wide variety of net-

40 A cryptographic hash function is basically a puzzle that has a unique solution (typically a string of numbers or characters) that network participants race to guess the correct answer to. The Ethereum blockchain currently relies on a similar consensus method, although a proposed change to this consensus method is discussed in section V.

41 Proof-of-work consensus algorithms have one weakness associated with network processing power. If over 51 percent of the computing power on the network at any given time can be controlled by one entity, then the ledger can be updated to reflect transactions that would be at odds with network rules. This creates the possibility for double-spending Bitcoins. In practice, however, the major cryptocurrencies have sufficient network participants to where a 51 percent attack is unlikely. *See, e.g.*, Werbach, *supra* note 38, at 100. Less widely adopted cryptocurrencies (with accordingly lower numbers of network nodes) have suffered from 51 percent attacks, however. See Jordan French, Ethereum Classic's "51% Attack," $1 Million Loss, Raise Concerns About Security, The Street (Jan. 14, 2019), https://www.thestreet.com/investing/bitcoin/attack-against-ethereum-classic-14832327.

42 Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, & Steven Goldfeder, Bitcoin and cryptocurrency technologies: a comprehensive introduction (Princeton University Press, 2016). *See also* Harald Vranke, *Sustainability of Bitcoin and Blockchains*, 28 Current opinion in environmental sustainability 1–9 (2017).

43 Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, & Huaimin Wang, *An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends, in Big Data (BigData Congress), 2017 IEEE International Congress*, IEEE 557–64 (2017).

44 Christopher Malmo, *One Bitcoin Transaction Consumes as Much Energy as Your House Uses in a Week*, Motherboard (Nov. 1, 2017), https://motherboard.vice.com/en_us/article/ywbbpm/bitcoin-mining-electricity-consumption-ethereum-energy-climate-change.

45 Tony Klein, Hien Pham Thu, & Thomas Walther, *Bitcoin Is Not the New Gold–A Comparison of Volatility, Correlation, and Portfolio Performance*, 59 Int'l Rev. of Fin. Analysis 105–16 (2018).

46 Oscar Nilsson & Dorna Garagol, Public blockchain communities: A study on how governance mechanisms are expressed within blockchain communities (2018) (unpublished M.A. thesis, University of Gothenburg) (on file with the Department of Applied Information Technology).

47 A blockchain fork is when changes to the code are adopted by a subset of network participants, while other participants reject these same changes, resulting in two distinct blockchains moving forward from the point of rule disagreement. The following section discusses the predominant types of forks and their implications for governance, in greater detail.

48 Bruno Biais, Christohe Bisiere, Mathieu Bouvard, & Catherine Casamatta, The Blockchain Folk Theorem (Jan. 5, 2018) (unpublished manuscript) (on file with Swiss Finance Institute).

work participants have expressed frustration at the current means of changing the rules of the blockchain itself, which emphasizes the importance of blockchain governance.

The process described regarding the simultaneous processing and validation of a subset of network transactions, coupled with the reward of new units of cryptocurrency for doing so, creates a set of margins that together define the incentives of network participants. The margins of cryptocurrency reward amount, network fees,[49] block size, and puzzle difficulty together create an equilibrium expected payoff as a function of the energy expended by a given network participant to successfully resolve a given subset of proposed transactions on the network.[50] The greater the anticipated reward (increasing as puzzle difficulty decreases and rewards and fees increase), the greater the number of network participants likely to expend the energy in racing to solve the underlying hash function. Thus, one significant area of debate among network participants is how to calibrate these factors to the benefit of all participants. Of course, the nature of processing transactions is energy intensive, which means energy prices greatly determine where network participants are physically located,[51] as well as these participants' relative positions with respect to proposed changes to the rules governing the blockchain. Importantly, though, a final definitional component of participants' incentives is that of the costs of exit—to the extent that changes to their incentives on one blockchain are sufficiently undesirable, permissionless blockchain participants can (at some cost) opt into a different cryptocurrency blockchain that better matches their governance preferences.

This all suggests that even in the case of cryptocurrency networks, for which some of the comparative benefits depend in great part on the blockchain's immutability, the governance of system-wide processes (often tightly tied to the consensus algorithm by which changes to the ledger occur) and the process by which the rules of this governance can change, have significant implications for the intended outputs of the network itself. Put differently, the rules about making or changing rules governing a blockchain matter fundamentally. This insight comes as no surprise to any legal or constitutional theorist, of course. In addition to the Bitcoin community, other cryptocurrency blockchains (e.g., Ethereum) are confronting similar problems in scaling informational changes on the network and are instead proceeding with a different set of proposed changes, with the expressed intent of changing the underlying consensus algorithm itself. Ethereum has emerged as a competitor to Bitcoin among major cryptocurrencies, and is currently testing a different process by which rules as fundamental as the underlying consensus algorithm are changed suggests a clear example by which dominant cryptocurrencies are currently competing in terms of governance—a phenomenon discussed in detail in sections V and VI.

This concern over governance is unique to permissionless blockchains. In the case of a central authority tightly defining the location or powers of a particular network node, the means by which rule changes occur are not necessarily related to the network nodes' roles or preferences in any way and instead are a function of ordinary centralized firm decision-making.[52] In contrast, the design of permissionless blockchains means anyone with the right hardware, internet access, and reliable electricity can become a participant and hence have incentives and beliefs about the appropriate scope and form of blockchain governance. Decentralized validation of network processes coupled with distributed maintenance of the underlying ledger means that network participants necessarily have direct influence over the continuance or change of the rule set governing all network processes.[53] This implicates an aspect of governance typically reserved to public organizations, where constituents cannot opt out of the processes to which they are subject. Arguably, participants on a given blockchain are facing much lower exit costs in terms of their preferred

49 In addition to the rewards of new cryptocurrency units, network participants receive a set fee for every transaction they process. In the case of cryptocurrencies like Bitcoin that have a known upper limit to the amount of coins that will circulate, it is expected that these fees will prove sufficient to incentivize network participants once coin rewards have been exhausted.

50 Joshua A. Kroll, Ian C. Davey, & Edward W. Felten, *The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries, in* 13 Proceedings of WEIS, 11 (2013). *See also* Narayanan et al., *supra* note 42.

51 Paul Roberts, *This Is What Happens When Bitcoin Miners Take Over Your Town*, Politico (Mar. 9, 2018), https://www.politico.com/magazine/story/2018/03/09/bitcoin-mining-energy-prices-smalltown-feature-217230.

52 De Filippi & Wright, *supra* note 20, at 31.

53 Zheng et al., *supra* note 43.

governance than an employee subject to the centralized policies determined by private firm leadership. Their decision is more akin to investors who choose to move money from one firm to another based upon the governance decisions made by the firms in question. Nonetheless, on permissionless blockchains, the validation of network transactions is designed to prevent participants from evading the universal rules. This makes a similar influence over input to the rule set incentive compatible. Unlike traditional firms, the equivalent of shareholders in a given permissionless blockchain are also engaged in the output of that blockchain. This stands as a powerful departure from traditional models of private governance.[54]

Similarly, blockchain network participants, and to a lesser extent, users, also have strong beliefs about the appropriate scope and form of the functions to which a given blockchain will be applied. Thus, certain proposals to alter the fundamental rule set underlying a given blockchain are frequently argued to be at odds with the "constitutional" principles that guided the definition of the blockchain in the first place.[55] Originalist arguments have appeared in the context of proposed changes to the Bitcoin blockchain, and in the case of Ethereum, one of the founders plays a major role in ongoing debates about changes to the underlying blockchain.[56] Debates surrounding the intent for Bitcoin to become a major store of value and payment network, as compared to the intent for the currency to be immutable in terms of the rules governing its creation and transfer, are fundamentally debates about the true constitutional spirit of the blockchain as expressed through the specific rules governing network processes.

4. Blockchains and Constitutions

How, then, can blockchains be understood as a system of governance analogous to that created by a constitution? The participants, or network nodes, in a given blockchain play the role of the government, whereas the users of a given blockchain can be seen as constituents. While network participants are not representative agents in the exact sense politicians are, they are performing governance functions on behalf of users who request transactions on the cryptocurrency blockchain. The fundamental rules of the blockchain create a form of agency control by constraining the participants in the interest of the users, which creates an equilibrium that operates to the benefit of the constrained participants. Changes to cryptocurrency blockchains can thus affect any of the following: (i) the core definition of the underlying unit of value; (ii) the process of transactional validation by network participants; (iii) the incentives of network participants (often implicated by changes to transactional processes); or (iv) the comparative ability of a given blockchain to achieve its network objectives in comparison to the ability of competing blockchains to do so.

An important distinction between blockchain governance and modern constitutional democracies lies in the absolute lack of separation of powers. Blockchain participants exercise executive, legislative, and judicial functions simultaneously. As participants successfully solve the cryptographic hash function underlying the proof of work algorithm, they are simultaneously processing network transactions, generating network resources (the underlying cryptocurrency), and validating other participants' proposed transactions' conformity with underlying network rules.[57] Each of these processes can be likened to a distinct role of government. Cryptocurrency production and the proposal of minor rule changes are the equivalent of legislation. Processing transactions of existing cryptocurrency is like the execution of law. Ensuring conformity with network rules is akin to the judicial function of finally determining violations of the law by constituents.[58] Currently, the incentives to perform these functions are linked to the production func-

54 Nick Cowen, Markets for Rules: The Promise and Peril of Blockchain Distributed Governance (July 31, 2018) (unpublished manuscript) (on file at New York University School of Law).
55 Nilsson & Garagol, *supra* note 46.
56 Vitalik Buterin regularly discusses proposed governance changes publicly. *See, e.g.,* Ethereum.org and Vitalik.ca.
57 Narayanan et al., *supra* note 42.
58 For an extensive discussion of the relevance of blockchains to traditional legal processes, *see* De Filippi & Wright, *supra* note 20.

tion; miners engage in costly processing and verification of transactions due to the anticipated reward for successfully solving the underlying cryptographic hash function.

Blockchains, unlike government processes and judicial review, do not allow for the informal remedies for adjustments to the rule structure to better fit the needs and aims of those governed by the rule set. Granted, blockchain participants can adjust their uses of the blockchain to some limited extent, but they cannot directly interpret the underlying fundamental rule structure like government and judicial actors can in terms of constitutional implementation and interpretation. Put differently, the extent of discretion afforded to the government to make the Civil Rights Act a reality, or the extent of judicial interpretation that the Bill of Rights has required (and will continue to require), far exceeds the scope of choice blockchain network participants have in terms of the scope, form, and frequency of transactions to undertake. Coherence and supremacy are practically guaranteed in blockchain processes, which can be a double-edged sword when it comes to punishing bad-faith actors on the network, as the subsequent discussion about the DAO hack on the Ethereum blockchain emphasizes. Reversing a bad action under current governance processes takes the equivalent of a constitutional amendment.

One of most important distinctions between changes to blockchains and constitutional amendment processes surrounds the notion of forking the chain of code. Three distinct, predominant means[59] of forking exist: (i) a soft fork, which results in compatibility for network nodes that have not yet adopted the new rule change; (ii) a hard fork that would result in network nodes that have not accepted the new rule change rejecting blocks created under the new rule set; and (iii) hard forks that result in two permanently separate versions of the underlying blockchain, one under the old rule set and one under the new rule set.[60] Major rule changes, including updates to the block size, result in hard forks, which create the possibility for deterioration in network processes and outright errors, and as such, involve considerable debate in a given blockchain community prior to their adoption. In the second case of hard forks, unlike constitutional amendment, two blockchains can exist where there once was one, and participants and users subsequently decide (through their support of network processes and choice of transactional medium) which chain to support.[61] These choices in rule updates each influence the exit costs facing participants and users if they do not like a particular rule change.[62] With both soft and hard forks that do not result in a new cryptocurrency, the participants and users can only exit from the underlying blockchain entirely, as opposed to continuing their participation and use on the chain of the forked cryptocurrency that they most prefer. The choice of whether or not a hard fork will result in a viable second chain (and associated currency) is clearly utilized in cryptocurrency communities, with an announced hard fork of Ethereum (Constantinople) that will not result in a viable second chain, accompanied by discussion as to whether a second chain would emerge.[63] Such an outcome depends on the extent to which participants accept or reject the proposed rule changes.

In contrast, after a constitutional amendment, constituents are uniformly governed by the altered constitution, and the old constitution only governs those legal claims that emanated when the prior version of the constitution was in force. This means fundamental changes in rule sets on blockchains are subject to competitive pressures after the fact, with the former rule set potentially remaining a viable transaction and

59 A number of distinctions define how hard forks can proceed, which results in at least eight distinct types of hard forks. Nonetheless, for the purposes of this analysis focused on governance and exit costs, the key distinction is a hard fork that results in two viable chains, and one that does not. The former presents an exit option for network participants in a way that the latter does not. *See, e.g.,* Sean Stella, *What is a Hard Fork? Hard Forking Explained!*, Hardforking.com, *available at:* https://www.hardforking.com/what-is-a-hard-fork/.

60 *Supra* De Filippi &Wright at 24; Narayanan et al. *supra* note 42, at 73–75; Noelle Acheson, *Hard Fork vs. Soft Fork*, Coindesk (Mar. 16, 2018), https://www.coindesk.com/information/hard-fork-vs-soft-fork/.

61 *See* Biais et al., *supra* note 48. *See also* Arruñada, Benito, & Luis Garicano, Blockchain: The birth of decentralized governance (May 11, 2018) (unpublished manuscript) (on file with Pompeu Fabra Univeristy Economics and Business Working Paper Series).

62 Alastair Berg & Chris Berg, Exit, voice and Forking (2017) (unpublished manuscript), *available at:* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3081291.

63 Rachel Rose O'Leary, *What to Expect When Ethereum's Constantinople Hard Fork Happens*, Coindesk (Jan. 11, 2019), https://www.coindesk.com/what-to-expect-when-ethereums-constantinople-hard-fork-happens.

currency network, which allows for subsequent revelation of the perceived value of the network change. This distinction means blockchains are subject to competitive pressures on a number of margins which constitutional governance is not, notwithstanding the limited ability of constituents to move from one constitutional regime to another (to the extent they can afford to do so). This also means that in cases where a cryptocurrency forks to reflect distinct governance preferences on the part of different groups of network participants, this operates as a low-cost form of exit—both groups can be governed by their preferred set of constitutional rules, although they can no longer transact with one another on the same blockchain as before.[64] All of this implies that the choice to fork presents an important strategic margin for blockchain network participants considering rule changes.[65]

The scope of activities governed by a blockchain is much smaller than those defined by the legislative process in modern constitutional orders; the former is limited to a small number of processes, whereas the latter is only cabined by the boundaries the constitution places on the action of government. This variance in "legislative" scope has a corollary implication: the comparative importance of the judicial function increases as legislative scope increases. If a governance regime has a known and limited set of functions, the interpretation of the conformity of these functions with underlying network rules is a relatively simple process. However, as the nature and interpretability of network functions increases, the challenge, and hence, systemic importance of ensuring that these functions are in accordance with underlying rules similarly increases. This results in a comparative certainty of application of blockchain rules, as compared to constitutional rules; although, to the extent that blockchains follow through with proposed changes to include decentralized transactional processing and validation, this is likely to create unique challenges, as discussed in the section treating the Lightning Network and Sharding below. This means implementation of changes to the underlying blockchain rules are much more certain. Blockchain rule changes have less need for interpretation in subsequent periods, but are also less subject to downstream political pressures than constitutions, which require executive discretion in their implementation, coupled with judicial interpretation to oversee the constitutionality of this implementation.

Unlike constitutional government at the national level, those governed by a particular blockchain face much lower exit costs and can also be simultaneously governed by several blockchains to the extent they mine or transact in more than one cryptocurrency.[66] This provides an interesting analog to the decentralized governance arrangements studied in a number of contexts.[67] Consider the extent to which blockchain participants and users can freely enter and exit the governance arrangements of a given cryptocurrency, and compare it to the proposed and existing real-world governance schemes intended to harness similar governance benefits as a function of the largely voluntary presence of their constituents; there is significant overlap between the two.[68] The comparatively low-cost exit option both disciplines blockchain network participants in their choices of rule changes and serves as a margin of competition when rule changes implicate exit costs directly, as the discussion in section VI emphasizes.

The means by which constitutional amendment can proceed in ordinary political systems provides a blueprint by which to consider similarly fundamental governance changes on permissionless blockchains. Ultimately, the certainty of the application of blockchain network rules and the comparatively low exit costs facing cryptocurrency users reduce the importance of ex-post constitutional interpretation as amending the rule set itself. For example, in the case of judicial review, there is no clear analogy because of the

64 Narayanan et al., *supra* note 42, at 171–3.
65 Alastair Berg, Chris Berg & Mikayla Novak, Blockchains and Constitutional Catallaxy, (Dec. 4, 2018) (unpublished manuscript), *available at*: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3295477.
66 Cowen, *supra* note 54.
67 Tom W. Bell, *Special International Zones in Practice and Theory*, 21 Chap. L. Rev. 273 (2018). From early Chinese special economic zones to more sophisticated decentralization arrangements, there has been an increasing recognition of the value of competitive governance in facilitating more effective or representative institutions, as well as the political economy challenges associated with doing so. *See, e.g.,* Lotta Moberg, *The Political Economy of Special Economic Zones*, 11 J. of Institutional Econ. 167–90 (2015); Lotta Moberg, The Political Economy of Special Economic Zones: Concentrating Economic Development (Taylor & Francis, 2017).
68 Mark Frazier, *Emergence of a New Hanseatic League: How Special Economic Zones Will Reshape Global Governance*, 21 Chap. L. Rev. 333 (2018).

decentralized fashion in which network transactions are validated; absent an ex-ante agreement among over half of network participants, a given network node (run by a network participant) could not use its own discretion to validate transactions at odds with the rules of the blockchain.[69] The next informal means of constitutional change is that of adjustments in government processes and norms; in the case of blockchains, this involves participants and users' understanding of network capabilities and limitations, and their ability to adjust their network uses accordingly. One example of this would be users limiting their transactions on the Bitcoin network to a certain minimal threshold, below which the network fees for doing so do not make economic sense. Next, it is possible in theory to develop subsidiary layers of code governed by distinct rule sets (or simply rules that do not need to be validated by the entire network); in each case, these would operate like political and administrative decentralization, respectively. In the case of distinct rule sets, different network nodes (or a set of nodes) would operate their own rules or processes, although this would create coordination costs in reconciling different underlying processes with the primary chain itself; this is something the Ethereum blockchain may be better suited to facilitating, given its focus on more complex transactional processes.[70] In the case of the same rules, a subset of network nodes would be responsible for processing and validating network processes without wholesale validation occurring across the entire network. Importantly, in order for these decentralized processes to occur, this would require the support of a sufficient majority of network participants—blockchain's equivalent of a constitutional amendment. Finally, in the most well-known process (given the debates surrounding formal changes to the network rules), if a sufficient number of network nodes adopt a proposed rule change or changes, then the primary blockchain will be governed by these rules accordingly (with those set of network nodes that rejected the rule change operating under the old set of rules if a specific type of hard fork occurs).[71]

Accordingly, when it comes to governance, permissionless blockchain participants have three alternatives when it comes to adjusting governance. They can amend the rules underlying the blockchain itself (including those such as forking, which greatly shape exit costs), they can develop subsidiary governance processes that prevent the need for adaptation of the main blockchain, or they can adjust their use of a given blockchain, either directly, or by choosing to exit altogether and participate in or use another blockchain whose governance better resolves that participant's fundamental aims.

5. Cryptocurrency Governance Debates

Governance debates in cryptocurrency communities have resulted in a number of proposed and realized solutions that contain direct parallels to constitutional design choices intended to reduce agency costs while simultaneously capturing scale economies. These debates have implicated fundamental beliefs as to the most important governance principles that should be realized in the rule sets of a given cryptocurrency blockchain, as in the case of Ethereum and Ethereum Classic. Smaller changes to these blockchains (like block size) have nonetheless resulted in sufficient disagreement to where distinct governance regimes have emerged, such as the hard fork between Bitcoin and Bitcoin Cash. Different forms of subsidiary governance solutions have emerged as proposals, including both administrative and judicial decentralization, as well as elements of relational contracting, in the cases of the Bitcoin Lightning Network and the proposed Ethereum changes of Plasma and sharding. Wholesale change to governance processes is also being explored in the case of Ethereum's proposal of Casper, which would transition their blockchain from a proof-of-work consensus method to a proof-of-stake algorithm, in what would be the closest case to amending amendment rules themselves. Finally, new entrants have explicitly conditioned their competitive advantage on choices of blockchain governance, suggesting that permissionless blockchains will continue to be an important locus of innovation in private governance as participants and users exit from blockchains whose governance choices are less representative than others.

69 Narayanan et al., *supra* note 42.
70 Arruñada & Garicano, *supra* note 61, at 3.
71 De Filippi & Wright, *supra* note 20, at 31; Biais et al., *supra* note 48.

5.1 Ethereum and Ethereum Classic

In 2016, the Ethereum community was split between two governance alternatives in response to a well-publicized hack resulting in the loss of nearly $50 million of Ether. The Ethereum community had developed an organization for signaling community confidence in proposed applications (decentralized apps or dApps) for use on the Ethereum blockchain. The Decentralized Autonomous Organization (DAO)—effectively a complex smart contract running on the Ethereum blockchain—was intended to serve as a means of funding different proposed applications using the decentralized input of individual users. Following a screening process accomplished via known network figureheads, users who had bought tokens in the DAO could then in theory allocate these tokens to projects, and once projects had reached a 20 percent token threshold for acceptance, they would be funded via the Ether held by the DAO.[72] Taken at face value, the DAO presented a governance innovation in that the investment decisions would have involved human decision-making by screening projects ex-ante through existing reputation, social capital, and authority within the community. This presented the direct possibility that smart contracts can still involve relational contracting.

However, a flaw in the code intended to prevent "bank runs" (which required Ether withdrawn from the DAO in response to approved applications to be held for 28 days), enabled hackers to capture $50 million of Ether.[73] This flaw in the code resulted in a major governance challenge for network users. Maintaining fidelity to what were argued to be core principles governing the blockchain meant allowing the hackers to get away with $50 million. If, instead, the blockchain could be dialed back to the state immediately preceding the hack, then those who benefited from the coins that were withdrawn from the DAO would never have received their tokens. This latter option violated what many network participants saw as hard principles governing the creation and transfer of Ether on the Ethereum blockchain: transfers of Ether, once completed according to network rules, were immutable, and given that the blockchain had already updated in light of the funds transferred out of the DAO, these funds going to the individual (or individuals) who exploited the flaw in the DAO code was preferable to going against accepted rules governing the transfer of Ether on the Ethereum blockchain.[74] What came into conflict here was the extent to which participants believed faithfulness to the immutability of network processes should take precedence over punishing clearly wrongful activity, which is essentially a conflict of constitutional beliefs. As of the first of March 2019, Ethereum's market capitalization of $14.4 billion was over thirty times that of Ethereum Classic,[75] which suggests that more network participants and users believed in the importance of punishing bad actors, especially when it came to convincing new cryptocurrency adoptees that subsidiary systems on the Ethereum network had the willingness and ability to punish bad actors who exploited weaknesses in code.

5.2 Bitcoin v. Bitcoin Cash

One strain the existing Bitcoin blockchain has put on network participants and users is the ability to process payments in a timely fashion. The block size of the Bitcoin blockchain, along with the difficulty of the hash function miners are solving, effectively determines the number of transactions the network can process in a given time period. Transactions per second is the common measure among major payment networks like Visa, with the Visa network averaging 1,700 transactions per second (and an underlying

72 David Siegel, *Understanding the DAO Hack,* Coindesk (June 25, 2016), https://www.coindesk.com/understanding-dao-hack-journalists/.
73 Klint Finley, *A $50 Million Hack Just Showed That the DAO Was All Too Human,* Wired (June 18, 2016), https://www.wired.com/2016/06/50-million-hack-just-showed-dao-human/; Mathew Leising, *The Ether Thief,* Bloomberg (June 13, 2017), https://www.bloomberg.com/features/2017-the-ether-thief/.
74 Vitalik Buterin, *CRITICAL UPDATE Re: DAO Vulnerability*, Ethereum.org (June 17, 2016), https://blog.ethereum.org/2016/06/17/critical-update-re-dao-vulnerability/; *see also*, thehighfiveghost, *Critical Update RE: DAO Vulnerability*, Reddit.com, (2017), https://www.reddit.com/r/ethereum/comments/4oiqj7/critical_update_re_dao_vulnerability/.
75 Top 100 Cryptocurrencies by Market Capitalization, CoinMarketCap, *available at:* coinmarketcap.com.

capacity of 47,000 transactions per second).[76] In contrast, the Bitcoin network can process roughly seven transactions per second.[77] More problematically, as the number of users of Bitcoin increases, this number of transactions remains the same because of the fixed size of blocks of data that are added to the Bitcoin blockchain and the largely fixed rate at which the hash function is solved. Put differently, more network participants have to get in line for a process that only serves one customer at a time and that takes roughly the same time to conclude each time. Thus, the more people transacting in Bitcoin, the greater the delay each transacting party faces before their transaction can conclude.

The implications are clear when it comes to Bitcoin's ability to be a payment network that can effectively serve a greater number of users. As a result, one hard fork resulted in a distinct cryptocurrency called Bitcoin Cash. Bitcoin Cash uses similar network processes to those supporting Bitcoin but involves a larger block size, allowing for greater transactional speed. As of the first of March 2019, Bitcoin Cash's market capitalization stood at $2.3 billion, while that of Bitcoin stands at nearly thirty times greater, at nearly $68 billion.[78] Notwithstanding the large disparity in valuation, Bitcoin Cash is currently the sixth largest cryptocurrency by market capitalization, which suggests a large number of participants and users saw considerable value in the underlying network changes. However, the nature of comparative market capitalizations poses the question of the extent to which competition among closely related blockchains will result in multiple viable currencies. A given currency's value as a medium of exchange depends on widespread adoption, which creates a clear long-term downside to multiple closely related currencies. Can they compete as effectively as entirely distinct cryptocurrencies whose brand could more clearly signal underlying distinctions in blockchain governance choices? Forking as a means of reducing exit costs for network participants is not without its own costs to the network and may not always be a desirable option.

5.3 Lightning Network (BTC) & Plasma/Sharding (ETH)

Interestingly, both Bitcoin and Ethereum participants have begun to explore solutions from the realm of relational contracting and decentralized governance in order to overcome the problem of scale created by the proof-of-work algorithm underlying each blockchain. In the case of the Bitcoin blockchain, a proposed modification would effectively create a subsidiary network for handling transactions among network users who repeatedly transact with one another. This proposal, known as the Lightning Network, is in response to the same underlying problem that led to the fork between Bitcoin and Bitcoin Cash. The Lightning Network is a proposal to move transactions off-chain by relying on existing relationships among Bitcoin users. This would create a payment channel between users, effectively allowing a limitless number of transactions between two parties that have a payment channel between them. Once the parties have closed the channel, the resulting net balance between the two would be posted to the Bitcoin blockchain in a single transaction, significantly reducing the network load among users that repeatedly transact with and (likely) know one another. The proposal also envisions numerous channels open among multiple users, intended to create a web effect in which many transactions could occur off chain, requiring only a few transactions to finally post to the blockchain.[79] Existing constraints have meant that microtransactions in Bitcoin were impractical, given the long wait times and network fees that could outstrip the value of the transaction. This led to third parties willing to intermediate microtransactions, but the existence of such intermediaries stands in contrast to the founding principles of a decentralized payment system intended to fundamentally disintermediate transactions. By instead relying on the existing repeated relationships among Bitcoin network users, this proposed change leverages the power of relational contracting to overcome the problem of scalability created by the fundamental underlying rule set.

---

76 Manny Trillo, *Stress Test Prepares VisaNet for the Most Wonderful Time of the Year*, *available at:* http://www.visa.com/blogarchives/us/2013/10/10/ stress-test-prepares-visanet-for-the-most-wonderful-time-of-the-year/ index.html.

77 K. Croman et al., On Scaling Decentralized Blockchains, *in* Financial Cryptography and Data Security (2016) (lecture notes in computer science, vol. 9604. Springer, Berlin, Heidelberg).

78 Top 100 Cryptocurrencies by Market Capitalization, CoinMarketCap, available at: coinmarketcap.com

79 Joseph Poon & Thaddeus Drvia, The Bitcoin Lighting Network: Scalable Off-Chain Instant Payments, Draft version 0.5 9, 14 (2016).

Given the similarities between the underlying blockchains' protocols supporting Bitcoin and Ether, Ethereum participants have also developed an analogous solution, making the validation of smart contracts occur on a sublayer, a proposed update to network rules called Plasma. Plasma is similar to the Lightning Network, except it involves the validation of contracts as opposed to the validation of transactions among repeat players. In each case, only a small proportion of the activity on the subsidiary layer appears on and is validated by the network governing the primary blockchain.[80] Importantly though, this does not involve the uniform enforcement of formally encoded blockchain rules to be operative on the blockchain sublayer, unlike sharding, discussed subsequently. Thus, this form of governance solution is most akin to administrative or political decentralization, where a subset of participants wholly govern subsidiary processes without a new set of rules that they themselves define.

Another related governance solution explored by Ethereum participants is called sharding and is incorporated into recent proposals made by Ethereum founder Vitalik Buterin. These proposals address the amount of policy adaptation likely to take place on the second layer of protocol, as opposed to the primary layer of the Ethereum blockchain itself.[81] The proposed change is similar to classic governance solutions intended to overcome problems created by the increase in scale of processes, whether it be from scope of government policies, number of people governed by them, or both. Sharding involves the replication of some or all Ethereum blockchain processes in a subsidiary blockchain managed by one or more network participants.[82] The Ethereum logo is a crystal, which clarifies the governance design underlying sharding. Each fragment of a larger crystal, known as a shard, duplicates the internal molecular crystalline structure of the larger crystal. In practice, sharding is a blockchain-specific form of judicial decentralization, where the validation of network transactions occurs on only a subset of participants' nodes. Where this process stands as a unique governance innovation is that judicial decentralization is typically a function of political decentralization, where subnational governments define law that is subsequently adjudicated at the same level; here the blockchain rules would remain the same, but only a subset of network participants would be responsible for ensuring conformity with those rules.[83] A fundamental trade-off of decentralization is squarely apparent in the case of sharding: increases in terms of the scalability of network processes are weighed against the additional costs of governance on each individual shard, as well as the coordination costs of reconciling individual shard states with respect to the primary layer blockchain. The ability to maintain a greater number of transactions with greater variance in applicable rules can be seen as a governance solution designed to reduce the incentives to exit the blockchain due to the greater likelihood that a given user and participants' governance preferences will be accommodated in the more relational or decentralized arrangements intended to result.

5.4 Casper (ETH)

One of the most fundamental governance changes being debated among cryptocurrency network participants surrounds transitioning Ethereum from a proof-of-work (PoW) to a proof-of-stake (PoS) consensus algorithm. This proposed change directly approaches the problem of electricity intensity and network congestion leading to high transaction fees and slow processing time, two of the major obstacles to any cryptocurrency network functioning at scale. For commercial actors to readily adopt cryptocurrency payment methods, they need assurance that payments will process quickly and will not cost the vendor a

80 Joseph Poon & Vitalik Buterin, Plasma: Scalable Autonomous Smart Contracts, White Paper (2017).
81 Interestingly, Buterin noted that constant change to the blockchain's primary rule set would either result in considerable uncertainty for network participants or would require a high degree of centralized control—both are at odds with the fundamental beliefs surrounding stable decentralized governance that animated the creation of the Ethereum blockchain. *See* Pinaz Kazi, *Ethereum Co-founder Vitalik Buterin Shares His View on Plasma, Sharding & Layer-2 Solutions*, BCFocus (Aug. 29, 2018), https://bcfocus.com/news/Ethereum-co-founder-vitalik-buterin-shares-his-view-on-plasma-sharding-layer-2-solutions/21938/.
82 *See, e.g.*, Jordan Raul, *How to Scale Ethereum: Sharding Explained*, Medium.com (Jan. 10, 2018), https://medium.com/prysmatic-labs/how-to-scale-Ethereum-sharding-explained-ba2e283b7fce. *See also* Hsiao-Wei Wang, *Ethereum Sharding: Overview and Finality*, Medium.com (2017), https://medium.com/@icebearhww/ethereum-sharding-and-finality-65248951f649.
83 Id.

significant proportion of the underlying transaction. Perversely, buying a car with a cryptocurrency may currently present fewer obstacles than buying a latte with a given cryptocurrency.

Transitioning from PoW to PoS involves a wholesale change to the algorithm that produces, changes, and validates cryptocurrency ledger states. Instead of a race to solve a cryptographic hash function, network consensus about proposed changes to the underlying ledger is achieved through Ether holders staking a portion of their holdings on a particular proposed new block; if sufficient levels of stakeholders signal their intent to validate a given block of proposed transactions, then the block will be added to the Ethereum blockchain. Successfully proposed blocks will reward their relevant stakeholders not only in terms of new Ether but also via the fees associated with the transactions contained in a given block.[84] The proposed intent is to only validate network transactions via this process every 100th block, which makes this a phased transition, with the network eventually transitioning at a known rate to a blockchain exclusively supported by PoS as opposed to PoW processes. Ethereum's co-founder, Vitalik Buterin, is clearly concerned about governance compatibilities created by the simultaneous existence of difference consensus algorithms, as some of his recent technical output suggests.[85]

The phased transition reflects the profound change in network processes that changing the consensus algorithm would entail. Unlike adjusting the size of blocks, transaction fees, and new currency rewards, or even creating a subsidiary layer of governance, a change to the consensus algorithm is equivalent to changing the amendment rules of a constitution. Thus, the debates surrounding the change have been longer and more intense than debates over alterations in fees and hash function difficulty. If Ethereum transitions entirely to a PoS protocol, then all fundamental rule alterations in the future will proceed via a fundamentally different governance process. Essentially, Casper is a proposal to change the entire structure of government for the Ethereum blockchain, and as such, stands as an amendment to the amendment processes themselves, if not a wholesale constitutional overhaul. If successful, it will be worth observing closely how other competing blockchains react to the benefits and costs revealed by a completely new system of blockchain governance, especially in the case of blockchains like Tezos and EOS that have emerged in direct response to the governance tensions described thus far. However, the magnitude of change and the implications for all the network processes on the Ethereum blockchain have led to numerous missed deadlines associated with the launch of this change, which was originally rumored to be completed sometime in 2017.[86] Given how central to the long-term viability of the Ethereum network the Casper upgrade has been argued to be, it will be interesting to see whether network participants choose to support the upgrade, create a second currency based on the Ethereum blockchain up to that point (separate from Ethereum Classic), or exit the system altogether.

5.5 Emergent Governance Competitors: Tezos & EOS

This type of governance competition has already been occurring in the realm of cryptocurrencies, though. When Tezos was released in 2017, its initial coin offering (ICO) was one of the most successful to that point, raising $232 million.[87] The amount raised in an ICO can be seen as a version of an initial public offering, except governed by considerably less regulatory oversight. As investors have crowded into the space, there has been considerable fraud in terms of the extent to which companies issuing new coins actually have viable business models to support the bet in their business model that a purchase of an ICO typically implies.[88] In the case of Tezos, the innovation surrounded blockchain governance processes themselves,

84 Jon Choi, Ethereum Casper 101, Medium.com (Oct. 21, 2017), https://medium.com/@jonchoi/ethereum-casper-101-7a851a4f1eb0.
85 Vitalik Buterin, *A Guide to 99% Fault Tolerant Consensu*s, Vitalik.ca (Aug. 7, 2018), https://vitalik.ca/general/2018/08/07/99_fault_tolerant.html.
86 Amy Castor, *Ethereum's Difficulty Bomb: All Smoke, No Fire?,* Coindesk (Apr. 8, 2017), https://www.coindesk.com/ethereums-difficulty-bomb-smoke-no-fire.
87 Omri Barsilay, *Tezos' $232 Million ICO May Just Be the Beginning*, Forbes (July 16, 2017).
88 Dirk A. Zetzche, Ross P. Buckley, Douglas W. Arner, & Linus Föhr, *The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators* (2018).

a direct competitive response to the strains facing the dominant cryptocurrency blockchains supporting Bitcoin and Ether. Importantly, since the emergence of Tezos, Ethereum proposals have converged on a similar governance solution: that of Casper described above. Tezos allows for token holders to vote on proposed changes to the network's governance protocols—a node proposes a change along with a price associated with the cost they require to implement the change.[89] In theory, this would allow for dynamic network pricing of governance innovations. As importantly, the emergence of Tezos in response to existing governance problems among the dominant cryptocurrencies in terms of scalability displays competitive private governance in practice. However, it should be noted that Tezos has since faced profound governance issues in the real world, something that has held up its deployment and resulted in numerous lawsuits against the company.[90] While network participants and users should pay close attention to the governance changes being wrought on the networks in which they are invested, this does not mean that choices regarding corporate structure and regulatory compliance under public constitutional structures no longer matter. This lesson is often forgotten amidst the exuberance that early cryptocurrency adopters have for radical decentralization.

EOS is a competitor to the Ethereum and Bitcoin blockchains that emerged even more recently. EOS, in direct response to the scalability issues that created the governance challenges described thus far, will be based upon a delegated proof-of-stake system. Similar to Tezos, EOS was the most successful ICO of its time, raising several billion dollars in support, although the exact number remains subject to the volatility of Ether, the cryptocurrency in which the ICO was denominated.[91] Interestingly, the founders have directly argued that this system is analogous to the governance of a republic, where representative agents oversee processing and validation of network transactions.[92] These agents are elected by the network community, presumably with some form of punishment in subsequent electoral rounds if their adherence to network rules and fundamental governance beliefs is revealed to be lacking. Instead of staking the network's currency, participants and users vote on representative agents, with their number of votes being proportionally equivalent to the size of their stake in the network.[93] This method is designed to overcome another fundamental governance challenge not unique to blockchains: money in politics. In the case of Ethereum's proposed changes, those participants and users with large Ether holdings could validate proposed blocks due to self-interest, as opposed to those blocks' conformity with the underlying rule set of the network. By allowing participants and users to aggregate their votes behind network participants that those individuals believe will process and validate transactions in good faith, EOS's consensus algorithm is designed to mitigate the scale advantage that large holdings in the network are likely to create for certain Ethereum stakeholders.[94]

89 Liam Johnson, *Tezos (XTZ) Pros & Cons – Self-Amending Cryptocurrency Blockchain*, Bitcoin for Beginners (Aug. 15, 2018), https://www.Bitcoinforbeginners.io/cryptocurrency-reviews/tezos-xtz-review/.

90 Thijs Maas, *The Curious Tale of Tezos: From a $32 MILLION ICO to 4 Class Action Lawsuits,* Hackernoon.com (Apr. 6, 2018), https://hackernoon.com/the-curious-tale-of-tezos-from-a-232-million-ico-to-4-class-action-lawsuits-6f411b7aad7e.

91 Kate Rooney, *A Blockchain Start-up Just Raised $4 Billion without a Live Produc*t, CNBC (May 31, 2018), https://www.cnbc.com/2018/05/31/a-blockchain-start-up-just-raised-4-billion-without-a-live-product.html.

92 Aaron Stanley, *EOS: Unpacking the Big Promises Behind a Possible Blockchain Contender*, Coindesk.com (June 25, 2017), https://www.coindesk.com/eos-unpacking-the-big-promises-behind-a-possible-blockchain-contender/.

93 Berg, Berg, & Novak, *supra* note 65, at 10.

94 Nonetheless, not all cryptocurrency users are happy with the level of centralization that the traditional political institution of delegated representation implies. As compared to a PoW blockchain, EOS is unquestionably centralized, which gives it a greater ability to punish bad actors, as an EOS administrator's correction of a seemingly bad faith transaction indicates. *See* Stephen O'Neal, *EOS Proves Yet Again That Decentralization Is Not Its Priority*, Coin Telegraph (Nov. 15, 2018), https://cointelegraph.com/news/eos-proves-yet-again-that-decentralization-is-not-its-priority.

6. Competitive Constitutional Governance on Blockchains

Despite the numerous differences between the comparatively narrow set of network processes determined by a blockchain's fundamental rule structure and the broad range of human behavior governed by constitutions, those seeking to better understand governance debates surrounding blockchains would do well to consider the lengthy history of constitutions.[95] Debates about the fundamental principles of governance inevitably implicate constitutional amendment, and the extent to which a given governance structure can accommodate changes desired by a sufficient number of constituents can directly determine how well that governance structure can achieve its intended functions. In a competitive world, where network users and participants bet on the viability of one blockchain over another, governance provides an important margin for competition, effectively determining how well a blockchain can adapt to emergent network problems and the changing demands of network users. In an important sense, blockchain users are the ultimate sovereigns because the extent to which individuals choose to store value and transact on a given blockchain determines the valuation of the cryptocurrency, which in turn defines the incentives for network participants to verify and process transactions. In this sense, network participants are constrained by the changes to the network that their choices create; if the changes diverge sufficiently from network users' intended purposes, these users can simply use the network less or depart from it entirely.

Cryptocurrency blockchains provide a unique example of private governance whose core characteristics overlap with a number of those typically associated with public governance.[96] Unlike the traditional centralized hierarchy of firm governance, all participants in the collective output of a given cryptocurrency blockchain can influence the fundamental rules governing this output. Nonetheless, these rules are subject to market choice by users in a way that public governance at the nation-state level typically is not: cryptocurrency users can readily vote with their feet. This means the blockchains supporting cryptocurrencies are a unique case study in private governance,[97] in which unusually decentralized decisions surrounding fundamental rule sets are subject to competitive market pressures facilitated by relatively low exit costs. These blockchains thus mix governance features traditionally associated with public and private organizations, respectively. Allowing for uniform and clearly regulated input from all participants in the process as to the fundamental rule sets governing them, while simultaneously subjecting this governance process to competitive pressures, is a unique innovation in governance that should pique the interest of institutional scholars and practitioners.

This means that exit costs greatly define the incentives of individuals choosing to make costly bets on network participation and use. In a context where exit costs are relatively low, the stakes of any given group decision are necessarily lower[98] (provided, of course, that the group decision itself does not directly implicate exit costs). For anyone who lives sufficiently close to the border of a state rewriting its constitution, the downside risk associated with constitutional change is lower. If the outcomes are sufficiently undesirable for any given individual who faces low moving costs, that individual will choose to move rather than incur the costs associated with the change in governance. In practice, though, even moving a few miles across state lines poses a significant cost, especially as compared to the cost of choosing to mine or transact in another cryptocurrency. This simple fact of relatively low exit costs for cryptocurrency users and participants has important implications for the dynamics likely to result from constitutional level governance changes to a given blockchain. One cause of these low exit costs is the nature of blockchain rule changes themselves; the possibility for a fork that reflects both opposing participants' governance preferences on a given issue also lowers the stakes associated with a given rule change. Whether or not a given set of

95 *See* Rajagopalan, *supra* note 3; Berg, Berg, & Novak, *supra* note 65.
96 *See* Cowen *supra* note 54.
97 *Id.*
98 Hirschman, *supra* note 7, at 82–6.

cryptocurrency participants' governance preference on an issue carries the day, if a fork in the blockchain reflecting their preferences will persist after the rule change, this reduces the costs of such change in governance to the "losers." A second characteristic of cryptocurrency communities also reduces the cost of governance changes to losers: literal exit from participation or use of the cryptocurrency itself. Moving one's stake in a given cryptocurrency blockchain to another permissionless-blockchain-supported cryptocurrency, or into more traditional financial instruments altogether, facilitates exit to a level never enjoyed by individuals who are subject to traditional public constitutional governance.

Because exit costs directly influence the incentives of network participants, these exit costs themselves create a potential margin for competition over governance. Exit costs influence participants' and users' incentives both during periods of ordinary network operation as well as times when governance changes are being wrought. Similar to a variety of investment contexts, the speed at which one can convert a costly investment into a more liquid asset directly affects individuals' willingness to invest, and, accordingly, the return offered on the investment.[99] But the effects of exit costs are not limited to the individual incentives of network users and participants. Because exit costs influence the changes in governance that are likely to be realized, network participants have an additional channel by which their incentives are implicated. Is a reduction in network participants and the emergence of a competing but closely related cryptocurrency worth the benefit of the more representative governance that is likely to result in contexts where exit costs are lower? Participants must thus examine how a rule change will affect both their own incentives and the exit decisions of other participants. They must also consider how comparatively better or worse outcomes will then affect a similar calculus on the part of network users.

Lower exit costs thus facilitate greater competition in governance, which is often argued to result in benefits associated with both enhanced government accountability to citizens and experimental discovery.[100] Lower exit costs also suggest greater variance in policy change, to the extent that constituents self-select into the governance regime that most closely represents their preferences, as opposed to using their input to moderate governance change in a regime in which they are a minority.[101] However, cryptocurrencies dependent on proof-of-work algorithms need a sufficient number of miners to prevent attacks that result when one set of network nodes controls more than 51 percent of the computing power on the network. This means sufficient exit of miners carries costs to the network writ large in ways that are similarly costly to users choosing to stop transacting in the currency altogether. Because of this trade-off in terms of representativeness of governance and sufficiency of network participation and use to achieve its intended purposes, it is clear that lower exit costs are not uniformly better. In the context of Ethereum in particular, two things indicate attempts to influence exit costs on the margins in ways that mean participants cannot as easily choose to exit, whether to another Ethereum-based cryptocurrency or to another cryptocurrency altogether: (i) the use of hard forks that do not result in two viable chains[102] and (ii) the intent to make certain types of computer processors less profitable for network participants.[103] Another important aspect of exit costs surrounds the relationship between blockchain rule sets and the public legal systems in which blockchain participants and users reside.[104] EOS has a written constitution that specifies, among other things, forums for dispute resolution among network participants and users, suggesting that choice of public legal system as a backdrop for on-chain disputes will prove an additional margin of competition. Importantly, choosing to resolve a blockchain-related dispute before the costs is another exit cost that different blockchain governance regimes will likely compete on.

99 Douglas W. Diamond, *Liquidity, Banks, and Markets*, 105(5) J. Pol. Econ. 928–56 (1997).
100 Hirschman, *supra* note 7, at 3; *id.* at 32.
101 Scott Gehlbach, *A Formal Model of Exit and Voice,* 18(4) Rationality and Society 395–418 (2006).
102 O'Leary, *supra* note 63.
103 *Id.*
104 Alastair Berg, Chris Berg, & Mikalya Novak, Blockchains and Constitutional Catallaxy (Dec. 4, 2018) (unpublished manuscript), *available at:* https://ssrn.com/abstract=3295477 or http://dx.doi.org/10.2139/ssrn.3295477.

In sum, there are a number of competing forces resultant from governance choices that will greatly influence the number of viable cryptocurrencies: adoption, competition, and exit costs for participants and users. The need for sufficient adoption acts as a downward pressure on the number of cryptocurrencies; past a certain point, too many cryptocurrencies with tiny user bases will prevent their intended uses from being successful or will outright vitiate the benefits of permissionless blockchains altogether by making a 51 percent attack too easy. Competition between blockchains as a function of their outputs will similarly reward and discipline blockchains whose governance choices on these margins will determine their success and failure.[105] Finally, the low costs of exit both facilitate competitive pressures and present a direct governance design choice on which cryptocurrency blockchains can compete. Do cryptocurrency users and participants prefer the lower exit costs associated with forking the blockchain and moving to other currencies, or can barriers to exit actually improve on-chain governance outcomes?

These trade-offs can be understood by considering one example based on the currently dominant cryptocurrencies' governance structures. Rigidities in these governance structures lent most of the benefits in terms of their use as currencies but have revealed a hidden set of costs surrounding the inability of these currencies to adapt to changing demands (to which some users would argue they should not adapt). This implies a competitive benefit to more blockchains whose governance models are slightly to significantly different. In the long run, this should lead to more efficient blockchain governance, but it implies a trade-off for design of blockchains themselves, as well as the market more broadly. Is a greater diversity of blockchains more efficient, or are fewer, more flexible blockchains ideal? While flexibility has been linked to constitutional endurance, it is not as clear that mutability of network rules is the right competitive margin for blockchain participants and users, especially as compared to exit costs. Blockchains' value is only realized after a sufficient number of users adopt the use of cryptocurrency that a given blockchain supports. This suggests diminishing marginal returns to numerical competition in governance; the benefits of competition in governance between different blockchains cut against the benefits of scale that clearly exist in blockchains more generally. This means the optimal level of flexibility in blockchain governance can be seen as a function of the number of blockchains out there in a particular industry. Past a certain point, this could cut toward the need for fewer blockchains with more flexible governance mechanisms, including exit costs calibrated to make one's participation and use of a cryptocurrency more or less "liquid."

A related trade-off surrounds the current nature of governance change that can fork the blockchain into two chains of code, which could be construed as facilitating competitive governance processes, or as stymying them. Firm governance is subject to competitive pressures. In theory, blockchain forks create a possibility analogous to that of cloning a firm and subjecting it to two distinct governance structures. However, in the case of a blockchain forking, it is not as if a randomized controlled trial in governance is occurring with respect to a single firm. Once a cryptocurrency has forked, the two new currencies are by and large competitors.[106] Furthermore, competition among cryptocurrencies is occurring on a single originating blockchain, which creates an additional margin for competition. Is a cryptocurrency's ability to compete with other cryptocurrencies diminished when it forks? Put differently, is its brand diluted when this occurs?[107] A further interesting possibility surrounds the ability of blockchain participants and users to hold or divest the different currencies sometimes resultant from a hard fork. Someone holding Bitcoin and Bitcoin Cash could exchange all of their holdings in one currency for holdings in the other as soon as these transactions could be processed and validated after the fork occurred. This means prices of the distinct cryptocurrencies subsequent to the fork can (at least in theory) reflect participants' and users' expected valuations of the underlying rule changes. This is only true to the extent that blockchain participants

105 Cowen, *supra* note 54.

106 In theory, a cryptocurrency blockchain fork could occur to create complementary currencies, with the underlying distinctions in blockchain governance deliberately designed to create networks whose capabilities at a minimum do not compete with one another and at most would be direct complements to one another. Thus far, though, existing forks in cryptocurrency blockchains have not occurred with the express intent to achieve these outcomes.

107 Narayanan et al., *supra* note 42, at 172–3.

and users are sufficiently and accurately informed as to the underlying governance trade-offs described here, though.

Thus, it should be noted that the arguments contained herein about network participants' and users' input to governance depend upon awareness on the part of these individuals of potential changes in governance and the costs and benefits thereof. Accordingly, when considering blockchain governance changes, it is worth asking how many blockchain users are sufficiently familiar with these debates to be able to exercise costly *informed* choice along the margins of governance variation described thus far. In the case of network participants, incentives are well-aligned for them to be informed as to these trade-offs; participants' input is required at a high level for changes to occur, and the continued value of participants' costly investments in electricity and hardware depend significantly on the rules governing the creation of additional cryptocurrency.[108] In the case of users—those who simply invest and transact in a given cryptocurrency—it is unclear just how well informed they might be about the costs and benefits of proposed governance changes. Nonetheless, because of their direct effect on the liquidity and value of cryptocurrency investments, exit costs are arguably among those most likely to be salient even to ordinary users of cryptocurrencies. If these costs increasingly become a competitive margin, this suggests there may be increased variance in governance in cryptocurrency blockchains, as one chain increases exit costs to retain its existing user and participant base, and another keeps exit costs low at the cost of losing a subset of its users and participants, at least in the short term.

Granted, notwithstanding some level of ignorance on the part of users and participants as to the governance changes being debated, changes in the market valuation of cryptocurrency often follow the success or failure of a given proposed governance change. Nonetheless, given that network participants are by definition users—at least for the period following their successful mining of a given amount of the underlying cryptocurrency—their choices following successful and unsuccessful governance changes are likely to inform price signals accordingly. However, network participants account for only a fraction of network users. Furthermore, cryptocurrency price shocks occur for a variety of reasons other than governance changes, such as regulatory changes in countries with high levels of crypto users, or frauds or hacks of major exchanges. This paper is therefore intended to clearly spell out the economic and institutional trade-offs implicit in the seemingly esoteric governance debates occurring among cryptocurrency network participants.

7. Conclusion

These debates over the best set of rules about making rules, or more typically, constitutions, are not an understudied topic. But in the context of private governance—where rule sets are typically more fluid, centrally controlled, and exist in the shadow of law and regulation—developing generalizable insights about comparatively superior governance mechanisms is more difficult. Permissionless cryptocurrency blockchains provide a potentially fruitful context within which to explore these questions. These blockchain ecosystems can be understood as a type of constitutional rule set that both defines and legitimizes the activities supported by permissionless distributed ledger technology. The development of cryptocurrency blockchains has thus led to new forms of competition in private governance, which include exit costs as one of the fundamental margins upon which governance outcomes will be shaped between blockchains.

Constitutional and political theorists should therefore neither be baffled by nor disinterested in the innovation currently occurring in governance processes on permissionless blockchains. These processes share many similarities to constitutional processes, and insights from constitutional design surrounding implementation and amendment shed considerable light on current developments in the communities supporting major cryptocurrency blockchains. The trade-off between flexibility and rigidity has caused divides in

108 Berg, Berg, & Novak, *supra* note 65, at 5–6.

these communities as they debate how best to scale network processes while remaining true to the collectively expressed understanding of the constitutional rule set of each blockchain. Some changes to network processes that require the assent of a sufficient proportion of network participants do not fundamentally alter the rules by which network processes are governed; instead, they affect the costs and benefits network participants expect as a reward for facilitating network processes of currency creation, validation of transactions, and participation in ongoing governance. Changes to data block size, hash function difficulty, transaction fees, and reward for hash function resolution all stand as examples of this type of constitutional change on the blockchain. Other changes implicate more fundamental additions or alterations to governance processes, such as the definition of subsidiary governance or an overhaul of the entire process of governance change itself. While the Bitcoin network's most salient proposed changes have limited themselves to, at most, creating a sublayer of governance, Ethereum's changes not only include a related form of decentralized governance but also involve wholesale changes to the means by which future changes to network processes will occur.

The study of public and private governance is now ancient. Thus, while blockchain processes present unique expressions of governance questions in new contexts, it is not as if challenges in obtaining consensus surrounding a given group's processes and governance are new. This means that an understanding of the fundamental trade-offs associated with constitutional design questions, with a particular focus on amendment processes, could considerably benefit blockchain designers and participants. Flexibility in amendment is seen as allowing necessary adjustment absent which an entire constitutional order can be overturned. Nonetheless, amendment thresholds should be sufficiently high that fundamental rules are insulated from ordinary pressures. Constitutions are seen as trading off between facilitating economies of scale in governance while simultaneously creating agency problems among those individuals who provide direct input to legislative, executive, and judicial governance. Decentralization is one solution that allows for better representativeness while preventing a level of centralization that obviates the ability to govern the number of processes demanded by a given nation's constituents. Thus, the relationship between blockchain participants and users as a function of the processes governing them is clarified through understanding the trade-offs that have long been debated in the context of constitutional design and subsequent amendments.

Finally, decentralized processes similar to those of governance via executive, legislative, and adjudicative functions may never have been automated at the economic scale and complexity seen on permissionless cryptocurrency blockchains. Blockchains can therefore be seen as an early example of constitutional law as code.[109] This means the competition among blockchains resultant in unique governance solutions could be a valuably informative precursor to the application of automated governance in the public sector. The terms of blockchain network participation and use that define entry and exit will become important margins of competition that shed light on the myriad institutional forms of digital citizenship and exit that are likely to emerge across the 21st century. Of course, it should be emphasized in conclusion that the benefits of this competition are only obtainable if there is sufficient *informed* adoption of cryptocurrencies to where the competitive pressures described here yield efficiency-enhancing governance benefits.

109 De Filippi & Wright, *supra* note 20, at 193–204.