Distributed Self-Government in Protocol Communities

An Introduction and Index of Examples

TOM W. BELL

We live in exciting times for governance. Large and powerful institutions used to come in only a few standardized types, such as nation-states and commercial corporations. But the advent of distributed organizations, built on computer code and fueled by digital cash, has supercharged the evolution of social coordination systems. Richly capitalized global communities worth hundreds of billions of U.S. dollars now spring up seemingly overnight. They die just as quickly, too—taking high hopes and huge fortunes with them.

This article introduces newcomers to the fascinations of distributed-protocol communities and analyzes the self-governance of several of the largest and most innovative. It defines seven measures of governance and grades the performance of each of ten protocols on a scale of *safe*, *caution,* or *danger*. The resulting Distributed-Governance Index organizes and summarizes the latest developments in the evolution of distributed-protocol communities and provides a framework for continuing observation of this rapidly developing field. From these early efforts might come the

Tom W. Bell is professor in the Fowler School of Law at Chapman University.

The Independent Review, v. 25, n. 2, Fall 2020, ISSN 1086–1653, Copyright © 2020, pp. 293–317.

next South Sea Bubble or the next best form of self-governance. It all bears watching at the least.

The first section reveals the origins, aims, and still brief but already turbulent history of distributed-protocol communities. The second section explains how the Distributed-Governance Index works—how protocols qualified for indexing, the scoring system, and a frank assessment of the project's limitations. The third section applies the seven performance measures, each in turn, to the ten protocols included in the index. The fourth section concludes with an overall analysis of the past and possible future of the self-governance of distributed-protocol communities.

Innovation in Distributed Governance

Legacy political institutions and businesses have never allowed the average person much direct influence over their operations. And until recently if you did not want to play by those rules, you could not very easily opt for new ones. It was too difficult to connect with counterparts, to reach agreement on better rules, and to decide on joint action. High transaction costs made serious governance—the kind that affects millions of people and billions of dollars—expensive, inefficient, and monolithic.

Now, though, you can enter into a new kind of government just by wiggling your fingers (and wading through some awkward interfaces). First, internet communications brought down the costs of finding and connecting people with shared interests. Then Bitcoin and other digital payment systems made it easier to store and transfer value. Today, communities such as Ethereum, EOS, and Dash offer protocols sophisticated enough to provide voting, delegation, funds disbursement, and other administrative functions. These distributed-protocol communities mark the farthest frontier of self-governance.

The largest of these new protocol-based communities host hundreds of billions of dollars in assets and make daily transactions worth millions of dollars. Anonymity and pseudonymity make an exact census impossible, but the networks can easily boast of having tens of millions of members scattered widely across the planet. Despite having so much at stake, though, these burgeoning communities have thus far struggled to govern themselves well. Even the most successful of them have suffered embarrassing failures, such as hacking attacks, unplanned hard forks, and ad hoc control by connected insiders. Such stumbles have discouraged investment and encouraged skepticism about cryptoeconomics.

Market commentators have begun to notice the importance of governance in their assessments of the risk/return profiles of cryptocurrencies (S+C Intelligence 2019). Developers of newer and presumably more advanced protocols trumpet their devotion to the concept (Dash Core Group Inc. 2018; EOSIO 2018; Decred Developers n.d.; Horizen n.d.; Tezos Foundation n.d.). It remains unclear, however, whether *more* governance means *better* performance. The spectacular returns generated by Bitcoin,

the cryptoanarchic original, suggests . . . perhaps not. The *kind* of governance evidently matters, too. But what kind? Until now, commentators could only watch and wait to see which fledgling protocols would survive the brutally uncaring market.

Though these fledgling organizations have no trouble qualifying as communities, they fall short of having a huge impact on the everyday lives of everyday people. Even so, the billions of dollars in assets and millions of daily transactions hosted by leading distributed-protocol communities shows that this is no mere computer game. And to take them at their word, the leading proponents of distributed-protocol communities want such communities to take over the world (Bell forthcoming).

The Distributed-Governance Index (DGI) set forth in this article offers a framework for understanding this recent explosion in new kinds of government. It documents and compares the performance of the largest and most interesting protocol-based communities in several key areas, such as exposure to 51 percent attacks and funding for shared infrastructure. Table 1 summarizes the results. Its shade-coded assessment, with darker grays corresponding to greater danger, offers a quick look at how each of the indexed protocols fares under each of the variables, explained more fully later, that track the self-governance of these communities.

Table 1 necessarily omits many crucial details. Most notably, it does not indicate which variables matter the most. (The columns have equal width for mere aesthetics—not to indicate the relative importance of each variable.) Some readers might regard a protocol's susceptibility to 51 percent attacks, an existential risk, as far more important than other considerations of good governance. Other readers might care more about protecting a community from infections of liability-inducing data. The

Table 1
Summary of Protocols and Governance Variables

Protocol	51% Attack	Chain Cleaning	Secret Voting	Open Proposals	Self-Amending	Commons Funding	User Privity
Bitcoin (BTC)							
Ethereum (ETH)							
Ripple (XRP)							
Bitcoin Cash (BCH)							
Litecoin (LTC)							
EOS							
Tezos (XTZ)							
Dash (DASH)							
Decred (DCR)							
Horizen (ZEN)							

novelty of these questions counsels against the DGI taking a decisive stance on the relative importance of the variables it tracks. It reports, you interpret, and fate decides.

The rest of this article explains the DGI's methodology, analyzes the performance of the protocols under each of several variables, and summarizes what these findings suggest for best practices in distributed governance. Governance represents one of the hoariest of human problems. Distributed protocols represent a new and largely untested technology. What happens when they collide? This article can only begin to study this newest example of human sociability. It cannot tell exactly where any given protocol's form of self-governance will lead that protocol, of course. Nor can it say exactly where this ferment in self-governance will lead. But it does say: keep watching distributed governance.

Methodology of the Distributed-Governance Index

This section examines what qualifies protocols for inclusion in the DGI and how the index deals with the variables of governance that it tracks.

The DGI focuses on the biggest distributed protocols, measured in terms of the market capitalization of their associated cryptocurrencies. Capitalization serves as a rough but fair first pass for finding the most promising candidates because it indicates that investors do not regard a protocol as utterly incompetent or dishonest—at least not in the short term. The DGI also considers a select few other protocols that include good government among their express goals. Table 2 cites the protocols and their putative internet homes. The top six were chosen solely by merit of their leading market capitalizations. The bottom four were chosen for their expressed interest in governance. All data come from CoinMarketCap (2019).

Market capitalization and self-identification do no more than determine which protocols get into the DGI. To make more accurate and longer-term assessments of governance, the index combines a number of measures of a protocol-based community's institutional health. It is not easy to assess how well a network will operate in practice simply by reading its white papers. Not even going over its supporting code with a fine-toothed comb would identify flaws in the system's incentive structure. Market capitalization and transaction volumes, although important markers of vital functions, might reflect artificial stimulation. And even when a network attracts users the honest way, latent systemic defects can destroy it all.

Like a physician conducting an overall physical exam, the DGI examines a number of markers of good governance. None of these admits to direct quantitative measurement. The index instead relies on informed expert opinion to assess each variable under consideration. Like traffic signals, these shade-coded scores indicate assessments of *danger,* marked in a dark 35 percent gray, *caution* in a medium 20 percent gray, and *safe* in a light 5 percent gray. Although rough, these methods will have to suffice pending more direct, objective, and refined measures of governance.

Table 2
Indexed Protocols by Reason and Market Capitalization

Qualification	Protocol Name and Origin	Market Capitalization (est.)
Capitalization	Bitcoin (Bitcoin.org n.d.)	$130,187M
Capitalization	Ripple (Ripple 2019)	$14,126M
Capitalization	Ethereum (Ethereum 2019b)	$14,123M
Capitalization	Bitcoin Cash (bitcoincash.org 2019)	$3,708M
Capitalization	Litecoin (Litecoin Project 2019)	$2,631M
Capitalization	EOS (block.one n.d.)	$2,440M
Governance	Tezos (Tezos Foundation n.d.)	$952M
Governance	Dash (Dash n.d.)	$380M
Governance	Decred (Decred Developers n.d.)	$180M
Governance	Horizen (Horizen 2019b)	$71M

The DGI tracks seven variables:

- Exposure to 51 percent attacks
- Chain-cleaning mechanisms
- Secret-voting options
- Open access to proposals for improvements
- Processes for amending the protocol from within
- Systems for funding common goods
- Users placed in privity of contract

Details about each of these variables are given in the third section.

Notably, the DGI does not quantify the relative importance of these variables in providing good governance. Some variables doubtless matter more, granted, as suggested by the order in which the index addresses them. But it would brook hubris to take a firm stand on that ranking, much less to assign numbers to each variable. By similar token, though its *danger–caution–safe* scores could easily admit to some kind of numerical interpretation, the DGI does not pretend that its subject—the collective behavior of humans and machines experiencing rapid technological change and trying out complex and largely untested algorithms—admits to great precision. It instead offers an appropriately imprecise assessment of distributed governance and thus a more honest one.

Alternative variables considered but rejected for this study include:

- Financial indicators (beyond market capitalization as a first-pass filter)
- Number and recency of GitHub commits
- What might be called the "personality factors" of protocol leaders

Financial indicators get ample coverage elsewhere by traders, who understandably obsess about the many various measures and data sets. Given the emphasis here on governance, it would not pay to involve financial variables any further than the present use of market capitalization as a rough (and thus not exclusive) mark of a protocol worth studying. GitHub comments offer a popular and facially fair measure of the vitality of an important subcommunity of any distributed protocol but hide a bias against coders who use alternative services and a bias in favor of bugginess (Scott 2018). The influence of personality over code cannot be gainsaid, but exploring it further in this study, much less treating it like a quantifiable variable, would amount to little more than geek gossip.

Analysis of Protocols by Variable

This section analyzes the performance of each protocol, variable by variable. Each subsection includes a definition of the variable, observations of its embodiment in the indexed protocols, and thoughts on what best practices in governance would suggest. As noted earlier, one ought not make too much of the order in which variables get addressed or expect anything like quantitative precision in their assessment. Nonetheless, thoughtful readers should find much here to enrich their understanding of the governance of distributed-governance protocols.

Exposure to 51 Percent Attacks

What It Means. This variable assesses the risk that a malicious agent will acquire sufficient computational resources to seize control of a protocol, providing it with the power to undo apparently completed transactions, engage in double spending, and otherwise thwart the protocol's intended functions.

State of the Art. Only protocols that rely on a Proof of Work (POW) consensus algorithm to confirm network transactions suffer exposure to 51 percent attacks. Among the ten ranked protocols in the DGI, Bitcoin, Ethereum, Bitcoin Cash, Litecoin, Dash, and Horizen rely on POW consensus. All POW networks are thus marked dark gray in table 3 for "danger" unless they have taken action to mitigate against this risk. The risk is not a minor one, either, because a successful 51 percent attack could destroy all public confidence in a protocol, rendering it worthless.

Horizen responded to the relatively small 51 percent attack it suffered by armoring its protocol against further such threats. Litecoin and Dash, anticipating problems on

Table 3
Indexed Protocols and 51 Percent Attack Exposure

Protocol	51% Attack Exposure?
Bitcoin (BTC)	bad; might improve if Chinese ban crypto (Kaiser, Jurado, and Ledger 2018)
Ripple (XRP)	allegedly not vulnerable because uses POA (Hodor 2018)
Ethereum (ETH)	bad until move to POS (Hertig 2018)
Bitcoin Cash (BCH)	like BTC but worse; has suffered attack (Boddy 2019)
Litecoin (LTC)	better than BTC because less exposed to specialized processors (S+C Intelligence n.d.)
EOS	none because POS
Tezos (XTZ)	none because POS
Dash (DASH)	Chainlock reputedly makes exposure impossible (Szilard 2019c)
Decred (DCR)	very low because POW + POS hybrid (Fiach_Dubh 2019)
Horizen (ZEN)	amended protocol after attack (Horizen 2019a)

this front, have already upgraded their protocols. That qualifies all three for a medium-gray "caution" score on this variable. Their efforts do not yet earn them a "safe" status because of uncertainties surrounding these coded defenses to malicious attacks. Because Ripple, EOS, Tezos, and Decred do not rely on a POW algorithm, they earn light-gray shading for their "safe" status on this variable.

Best Practices. The advent of computational resources that can be rented on the open market has increased the risk of 51 percent attacks. Perhaps the largest protocols can continue to rely on their size to protect them; perhaps not. Bitcoin Cash and Horizen have already suffered successful 51 percent attacks that used computing power rented on the open market to temporarily overwhelm the coins' comparatively small mining pools (Hertig 2018). Only the latter responded by armoring its protocol.

Though the "rent an attack" technique would not presently work against larger POW networks, those networks nonetheless remain vulnerable to 51 percent attacks that coordinate the mining of sufficient resources through collaboration or coercion or that benefit from an unforeseen advances in mining technology. Some analysts argue that Bitcoin suffers considerable exposure to the risk of a 51 percent attack organized by the Chinese government (Kaiser, Jurado, and Ledger 2018). Proof of Stake (POS) protocols, although in theory not immune to 51 percent attacks, prove fundamentally resistant to them (Ethereum 2019c).

Best practices thus suggest that distributed-governance protocols use something other than a pure POW consensus mechanism. Better options include:

- Proof of Authority (POA), as in Ripple
- Pure POS, as in EOS and Tezos

- Hybrid POW + POS, as in Decred
- POW with added safeguards, as in Litecoin, Dash, and Horizen

Only the first three options win "safe" scores in table 3 because they appear to entirely remove the threat of 51 percent attacks by no longer relying on pure POW consensus algorithms. The last option—sticking with POW but armoring it against 51 percent attacks—earns only a "caution" score due to the risk that a malicious agent might penetrate coded defenses or in the particular case of Litecoin exploit unforeseen advances in the memory-intensive processing on which it relies.

Chain Cleaning

What It Means. This variable measures the degree to which a protocol can remove illicit data from shared databases in a predictable, effective, and well-governed manner in order to protect users from liability for harboring or otherwise dealing with the toxic data.

State of the Art. Those who champion blockchain technology often tout the supposed immutability of its data storage. However, several incidents of ad hoc rewrites and growing threats of 51 percent attacks suggest that blockchain databases are not as permanent as often claimed (Bitcoin Wiki 2016; Canellis 2018). Perhaps that is just as well. Immutability becomes a liability when a shared database gets infected with illicit data.

If careless or malicious parties record illegal data on a blockchain or other distributed-ledger database, node operators would face liability for storing and distributing it. That would raise the effective costs of participating in the network, thus discouraging participation. This is no merely theoretical problem; researchers have already found various forms of illicit data on the Bitcoin blockchain (Blockchain Content Research n.d.), and Bitcoin SV blockchain (which allows for storage of large files on-chain) recently suffered a child-porn infection (Button 2019).

Ungoverned permissionless distributed ledgers face varying levels of exposure to this attack, depending on technical and legal details beyond the scope of this document. Every protocol in the DGI has to worry about illegal-data infections, though. Even those protocols with the smallest exposure—including Bitcoin—could fall prey to a copyright attack.

How well do the ranked protocols defend themselves from infections of illicit data? Not very well. Many of them—and the largest ones in terms of market capitalization—earn "danger" ratings when it comes to data-cleaning procedures. A few protocols make it up to "caution." Only the least capitalized of the ranked protocols—ones that take special pride in their governance—earn "safe" scores for their ability to remove toxic data in a rule-governed manner. Table 4 summarizes.

Best Practices. The blockchain community has only recently noticed the threat posed by toxic data. Extant protocols leave that vector undefended only at their peril.

Table 4
Indexed Protocols and Chain Cleaning

Protocol	Chain Cleaning?
Bitcoin (BTC)	no; see value-overflow incident, which unwound transactions (Bitcoin Wiki 2016)
Ripple (XRP)	not evidently, but centralized management might aid
Ethereum (ETH)	no; Slock.it DAO incident unwound transactions ad hoc (Jentzsch 2016)
Bitcoin Cash (BCH)	no; same as BTC
Litecoin (LTC)	no; same as BTC
EOS	yes, if EOSIO updates can roll back transactions
Tezos (XTZ)	yes (Breitman 2017)
Dash (DASH)	probably in theory but disparaged in practice (Szilard 2019a)
Decred (DCR)	yes (Decred Project 2019a)
Horizen (ZEN)	not on mainchain, though on Zen DAO in sidechain (Horizen n.d.)

Given the impossibility of screening out illicit data beforehand, protocol-based communities will have to figure out how to deal with it after the fact. Relying on ad hoc, off-chain deliberations among major token holders might work in an emergency, but it will not suffice in the long term.

Once the first illegal-data attack succeeds in disrupting a protocol's operation, other attacks will likely follow. Why? The motives might range from curiosity to malice to competitive advantage. Any one of them could impel bad behavior.

Best practices in governance thus suggest that protocols should keep their common blockchains or other distributed-ledger databases clean of illicit data through predefined, effective, rule-bound processes. There might always remain protocols that do otherwise, of course, just as there might always remain towns that let trash collect in the streets. That will not win them points for good governance, though.

Secret Voting

What It Means. The protocol self-governs through strongly anonymous voting procedures.

State of the Art. The most popular protocols do no governance "on-chain" (i.e., via the protocol itself). They thus offer no voting at all, much less secret voting—hence, the "danger" marks earned by Bitcoin, Ethereum, Ripple, Bitcoin Cash, and Litecoin.

Protocols with ambitions toward self-governance make various provisions for voting, but privacy protection remains rare. "The blockchain space today, with predictable results, continues its tradition of ignoring decades of study and instead opts to implement the most naive possible form of voting: directly counting coin-weighted

votes in a plutocratic fashion, stored in plain text on-chain," claim researchers (Daian et al. 2018). The EOS, Tezos, Dash, and Decred protocols seem to fit that description. Only Horizen seems to have even noticed the need for secret voting and taken action to provide for it, at least until voting on a particular issue has closed. Table 5 illustrates.

Best Practices. The permissionless nature of blockchain and other distributed-ledger databases makes votes on issues of common governance, like other transactions, open to scrutiny by default. This default affords not anonymity but mere pseudonymity, typically based on persistent wallet addresses in the form of alphanumeric strings. It takes a conscious effort for a protocol to switch that default to make votes fully secret. Surprisingly, few seem to have tried.

Horizen at least shows a willingness to address the problem by promising secrecy during votes. Unless it preserves secrecy even after voting closes, however, collusion and coercion remain viable means to attack governance processes: "Despite any identity or second-layer based mitigation attempts, all permissionless voting systems . . . are vulnerable to the same style of vote buying and coercion attacks" (Daian et al. 2018). Only trusted hardware (or abandonment of on-chain voting) offers a sure fix.

Traditional polities take care to protect the secret ballot for good reason (Gilbert 2019). Pseudonymous voting exposes a governance system to risks of collusion or coercion. Anonymous voting mitigates that risk because without a way to connect a particular vote with a particular party, there is no way to reliably police an agreement to vote in a particular way. There is no reason to think that distributed systems could not fall prey to the same hazards as centralized ones and good reason to worry that they might prove even more vulnerable to collusive or coercive voting than their real-space, paper-based counterparts. Best practices thus counsel the adoption of secret voting for

Table 5
Indexed Protocols and Secret Voting

Protocol	Secret Voting?
Bitcoin (BTC)	not applicable (NA); no on-chain governance
Ripple (XRP)	NA; no on-chain governance
Ethereum (ETH)	NA; no on-chain governance (Madore 2019)
Bitcoin Cash (BCH)	NA; no on-chain governance
Litecoin (LTC)	NA; no on-chain governance
EOS	no; pseudonymous, only (Maas 2018)
Tezos (XTZ)	not evidently
Dash (DASH)	not evidently
Decred (DCR)	no; pseudonymous only (Decred Project 2019c)
Horizen (ZEN)	yes—at least during votes (Pabst 2018)

all on-chain governance processes, both during and after votes. Even the most secretive election will fail to safeguard good governance, after all, if records of who voted for what can be retrieved after the fact.

The problem, however, lies not so much in recognizing that ideal as in implementing it. No less than Vitalik Buterin, creator of Ethereum, observed that "it is much harder, and more likely to be outright impossible, to make [governance] mechanisms that maintain desirable properties in a model where participants can collude, than in a model where they can't" (2019). Anonymous voting guards against that risk but at the same time introduces another bane of distributed protocols: Sybil attacks. These attacks rely on using manifold fake identities to subvert voting mechanisms and have proven something of a Gordian knot to the industry. Distributed protocols have not yet figured out how both to protect voter anonymity and to fend off masked attackers.

Open Access to Proposals for Improvements

What It Means. A protocol invites suggestions for improvements to its code-based infrastructure from users and other interested parties and provides for the publication of those suggestions to the same.

State of the Art. When it comes to asking for and accepting free help, distributed protocols do very well, somewhat unsurprisingly. All but one of the indexed protocols, Ripple, has a system in place for inviting proposals from the public about improvements to shared code. As perhaps befits its permissioned, authenticated, private nature, Ripple does not evidently invite suggestions from outsiders.

Most protocols accept proposals only in the sense that the communities that have sprung up around them have developed systems for collecting and evaluating suggestions. Bitcoin, Ethereum, Bitcoin Cash, Litecoin, and EOS fall into that camp. A few protocols go further, building into their governance mechanisms for encouraging the submission of proposals that meet defined specifications, such as adoption by a majority of participating nodes. Tezos, Dash, Decred, and Horizen offer incentives—native tokens typically—to get good ideas from anyone who has them.

Getting good ideas is not enough, however. A protocol needs a way to sort the wheat from the chaff, finding the proposals worth acting on among all those put forward. Approaches to that problem vary widely from protocol to protocol. Litecoin relies on a traditional git process, exemplified by the popular open-source programming platform GitHub, allowing anyone to suggest changes to the code through a "pull" request (Litecoin Project n.d.). Tezos, in contrast, has implemented a fully on-chain system (Pozzi 2019), wherein those who make a proposal must stake value (limiting spam) and both bakers (validators) and participants (token holders) vote to approve the proposal or not. Table 6 shows the DGI's evaluation of the ten protocols with respect to the open-proposal variable.

Best Practices. Best practices would suggest doing at least as much as most distributed protocols already do: accept proposals by third parties for improvements to the

Table 6
Indexed Protocols and Open Proposals

Protocol	Open Proposals?
Bitcoin (BTC)	yes, via BIP (Bitcoin n.d.)
Ripple (XRP)	not evidently
Ethereum (ETH)	yes, via EIP (Ethereum 2019a)
Bitcoin Cash (BCH)	yes, via Bitcoin DApps Improvement Proposal (web3bch 2018)
Litecoin (LTC)	yes (Litecoin Project n.d.)
EOS	yes, via Enhancement Proposals (EOSIO Enhancement Proposals n.d.)
Tezos (XTZ)	yes and pays for proposals (Kim 2019)
Dash (DASH)	yes and pays for proposals (Dash Central n.d.)
Decred (DCR)	yes and pays for proposals (Decred Project 2019d)
Horizen (ZEN)	yes and pays for proposals (Blockops 2017)

community's code. But a mere suggestion box, open to all comers, risks attracting a particular kind of proposal: one that will redound to the benefit of the suggesting party. That incentive structure need not lead to ruin, as the most heavily capitalized protocols demonstrate. But nor does a suggestion box seem optimal for discovering the kinds of proposals that will redound to the benefit of everyone participating in a distributed community—both those providing infrastructure and those using the protocol.

To attract proposals less shaped by self-interest, distributed protocols should invite submissions from all parties and reward those that meet specified protocols. Relying on neighboring institutions, as many protocols now do, runs the risk of capture by off-chain interests. Best practices suggest that protocols should continue their current drive to bring more self-governance on-chain.

It would not be wise to rush this migration. The game-theoretic complexities of collusive voting and agenda control counsel in favor of proceeding carefully, with controlled testing and incremental adoption. If distributed protocols can solve the problem of finding good ideas for reform, though, they will have solved one of government's oldest problems.

Self-Amendment

What It Means. Those communities governed by a distributed protocol can change it at least by hard fork and ideally by other more-controlled and less-severe means.

State of the Art. Most indexed protocols at least allow hard forking—the functional equivalent of an entire community abandoning bad code to move en masse to a new standard. The largest protocols tend to allow nothing more. Some smaller protocols do

more to provide rule-bound mechanisms for the community to alter its own code. These efforts reflect good intentions and hold great promise for making distributed protocols adaptable to changing circumstances, but they also hold the risks of putting complex and unpredictable dynamics into play.

Unsurprisingly, almost every indexed protocol admits to hard forking. One might quibble about even taking note of so basic a feature, but users' power to exit from outmoded or buggy code and migrate to a similar, upgraded version of a protocol evidently cannot be taken for granted. Ripple, for instance, does not encourage or even allow such free-form opting out (xrp_sea 2019). The protocol locks nobody in, of course. It just disallows anyone who chooses to leave from taking with them the nodes necessary for validating transactions. See table 7 for the DGI's assessment of the self-amendment process.

A hard fork represents a desperate effort to improve a failing protocol, akin to fleeing a country wracked with corruption and revolution. As such, it represents a crucial foundational principle supporting negotiations for less-severe and less-blunt mechanisms. This soft governance in the shadow of exit has worked reasonably well for the largest protocols. Commentators decry governance by hard fork, however, as ill suited for networks on which so much value now depends (Springer 2018). Responding to those concerns, the smaller of the indexed protocols have launched or at least announced "on-chain" methods to govern the adoption of new code.

Tezos and Decred have made the greatest progress on uploading governance. Both provide not only financial incentives for making suggestions to their code but also purely automated mechanisms for structuring and measuring user approval and, if the requisite limits are met, for implementing the approved code.

Table 7
Indexed Protocols and Self-Amendment Processes

Protocol	Self-Amending?
Bitcoin (BTC)	only via hard fork
Ripple (XRP)	not evidently (xrp_sea 2018)
Ethereum (ETH)	only via hard fork
Bitcoin Cash (BCH)	only via hard fork
Litecoin (LTC)	only via hard fork
EOS	yes, via vote of EOSIO Core Developers (EOSIO Enhancement Proposals n.d.)
Tezos (XTZ)	yes (Pozzi 2019)
Dash (DASH)	yes, via spork (soft fork)
Decred (DCR)	yes (Decred Project 2019a)
Horizen (ZEN)	planned (Viglione, Versluis, and Lippencott 2017)

EOS offers a well-developed system for Core Developers to receive, consider, and vote on proposed improvements to the community's protocol (EOSIO Enhancement Proposals n.d.). It seems to stop just short of making adoption of approved code automatic, however. It instead requires that even duly approved code be "implemented by EOSIO Core Developers and integrated into one of the EOSIO chains" (EOSIO Enhancement Proposals n.d.).

Despite its sophisticated proposal and funding mechanism, Dash appears to lack a means to automatically implement approved changes to the protocol. It instead appears content to use its open proposal system and funding system to encourage the production of quality upgrades, which node operators will adopt or not as each sees fit. The possibility of "sporks" (soft forks) in Dash perhaps makes this more discretionary approach to self-amendment less disruptive than alternatives offering only a hard fork as the alternative (Dash Core Group Inc. n.d.).

Horizen's original white paper forecast a decentralized autonomous organization (DAO) that would "be responsible for building, maintaining, and improving the infrastructure that keeps the system going" and "for implementing changes to the Zen software applications" (Viglione, Versluis, and Lippencott 2017). It appears that Horizen still relies on mere persuasion to ensure adoption of amendments by participating nodes, however.

Best Practices. It remains an open question exactly how and to what degree human discretion should play a role in governing distributed protocols. The least-automated means of amending a community's code—the hard fork—has functioned well enough that the largest distributed protocols continue to attract hundreds of billions of dollars. Yet even larger and longer-lived institutions demonstrate the benefits of adopting rules that allow for their own amendment. The U.S. Bill of Rights came out of such a process, for instance.

For reasons discussed later, humans must remain in the loop if distributed protocols want to offer upgraded forms of government. Humans have to express their preferences, for one thing, such as by voting on proposed upgrades. But humans should not have direct control over administrative functions such as tabulating those votes. In these areas, distributed protocols can improve on both traditional governments and protocols that govern solely through hard forks.

The trust created by blockchains and other distributed-ledger technologies will greatly aid the efforts of Tezos, Decred, and the other protocols to pursue on-chain governance. These efforts face terrific challenges in advancing from mere record keeping, the blockchain's great gift to governance, to more complicated administrative functions such as setting agendas, structuring deliberation, verifying identities, holding votes, and implementing approved policies. A game theorist can only gaze upon the wilderness and solemnly caution, "Monsters be there."

Best practices thus suggest what, indeed, leading protocols appear to do: strive to harness the potential benefits of on-chain governance while recognizing the risk of unforeseen problems. This calls for studying the best available theory to avoid

game-theoretic pitfalls yet also for not trusting theory alone. Think an individual human is unpredictable? Try putting a lot of them together in a system of governance. Only proven success should engender confidence in distributed-protocol governance, and even success should not lull anyone into complacency.

Common-Goods Funding

What It Means. Through this mechanism, a distributed protocol pays for developing and maintaining its shared code.

State of the Art. As the previous subsection discussed, protocol-based communities typically have some sort of mechanism for soliciting suggestions about how to improve their shared software. Less often, however, do they provide the means for funding those improvements. Bitcoin, Ripple, Bitcoin Cash, and Litecoin do not. Ethereum does so, but only via rather conventional off-chain foundation grants. EOS and Horizen likewise rely on off-chain methods of funding common goods, though they have made moves toward implementing on-chain ones.

It seems that Dash was first to launch an on-chain system for collecting and disbursing funds in support of the common good (Dash Core Group Inc. 2018). Dash allows Masternode operators to vote on proposals for doing specified acts—usually writing code—intended to benefit the entire Dash community. Decred's Politeia system, launched in the fall of 2018, offers a system that, like Dash's, funds common goods through on-chain governance (Yocom-Piatt 2018). Tezos's Athens upgrade offers the most recent and advanced on-chain commons-funding mechanism by allowing proposals to include an invoice, which gets paid automatically if the community adopts the proposal. See table 8 for ratings on common-goods funding.

Best Practices. Best practices in distributed governance suggest having on-chain mechanisms for choosing and funding common goods. Bitcoin seems to have done well enough relying on outside interest to fund research and development for protocol improvements. It arguably represents an exception in many ways, though, including the relative simplicity of its code and the network effects it enjoys as a first mover in the industry. More complicated protocols playing catch-up might find they need to prime the pump, so to speak, by providing for their own improvement.

Note, too, that research and development funded by off-chain sources risks generating improvements designed to favor off-chain parties. On-chain mechanisms for funding common goods offer the prospect, if well structured, of encouraging improvements more likely to promote the common good. This is not merely a question of the protocols "eating their own cooking," though it does seem fair to expect a system of governance worth the name to provide for its own sustenance. The lack of an on-chain mechanism for funding common goods suggests a lack of foresight, distrust in governance, and overpossessiveness. Such symptoms do not bode well for the health of a community.

Table 8
Indexed Protocols and Common-Goods Funding

Protocol	Commons Funding?
Bitcoin (BTC)	no
Ripple (XRP)	not evidently
Ethereum (ETH)	yes, but off-chain, via Ethereum Foundation (Ethereum Foundation. n.d.)
Bitcoin Cash (BCH)	no
Litecoin (LTC)	no
EOS	struggling to implement on-chain funding system (Karbowiak 2019)
Tezos (XTZ)	yes, on-chain (McKenzie 2019)
Dash (DASH)	yes (Dash Core Group Inc. 2018)
Decred (DCR)	yes, via online stakeholder vote with Manager veto (Yocom-Piatt 2018)
Horizen (ZEN)	off-chain process in operation; on-chain planned (Pabst 2018)

Users in Privity of Contract

What It Means. Each user of a protocol enters into a legally enforceable agreement defining the terms of users' mutual governance.

State of the Art. At present, it is not common practice for a distributed protocol to have users agree to legally binding terms of mutual governance. The prevailing approach invokes contract law only incidentally at the point of sale or gift of the token through which a protocol interacts with users. Someone who purchases Bitcoin with U.S. dollars, for instance, engages in a kind of sales contract. But such an agreement has too few terms to create a system of mutual governance. For that, users must enter into mutually binding and continuing agreements with many and various terms.

Of all the ranked protocols, only EOS shows any awareness of the need to formally document the rights and responsibilities of parties using its platform. EOS's constitution proclaims itself "a multi-party contract entered into by the Members by virtue of their use of this blockchain" (EOS Core Arbitration Forum Ltd. 2018a). That alone cannot suffice, however, to put users on notice of the proposed contract. As currently configured and operated, therefore, the EOS platform fails to establish the elements of a binding legal agreement. See table 9 for ratings on privity of contract.

In sum, distributed protocols do a poor job of binding users to the sort of ongoing and detailed commitments necessary to support self-governance. These communities thus lack means to enforce choice-of-law and choice-of-forum clauses—the usual devices through which contracting parties choose what general background rules will apply to their relationship and the means through which they will resolve disputes

Table 9
Indexed Protocols and User Privity

Protocol	User Privity?
Bitcoin (BTC)	no
Ripple (XRP)	not evidently
Ethereum (ETH)	no
Bitcoin Cash (BCH)	no; same as BTC
Litecoin (LTC)	no; same as BTC
EOS	probably claimed inaccurately
Tezos (XTZ)	not evidently
Dash (DASH)	not evidently
Decred (DCR)	not evidently
Horizen (ZEN)	not evidently

arising under those rules. This lacuna proves surprising given the commonplace use of such clauses in other commercial relationships and their widespread acceptance and indeed vigorous enforcement by traditional sovereigns.

With regard to local law, as with regard to privity of contract more generally, EOS represents the only protocol to address the issue. Given that its effort to create binding agreements with and among users almost certainly fails, EOS's attempt to choose the parties' law and the forum for resolving their disputes proves an exercise in futility. But perhaps that is not all for the bad given that EOS does a poor job of defining the applicable rules and creating institutions for interpreting them. EOS offers as binding law only the threadbare invocation, in article X, of the law of "this Constitution and the Maxims of Equity" (EOS Core Arbitration Forum Ltd. 2018a). That is hardly enough detail to handle millions of users engaging in manifold transactions worth billions of dollars.

Article IX of the EOS constitution puts all disputes arising under that document into the EOS Community Arbitration Forum (EOS Core Arbitration Forum Ltd. 2018b). That process at least offers the prospect of keeping EOS disputes local to the community, although, as discussed earlier, EOS has failed to establish the privity necessary to enforce that choice of forum. But, again, that is perhaps not all for the bad; critics have faulted the EOS Community Arbitration Forum for deciding cases in an unprofessional manner (Floyd 2018).

It bears noting that Decred offers something it calls a "constitution" but that in fact operates more like a statement of principles (Decred Project 2019b). Though this statement sometimes speaks in the language of rule making, it explicitly defers to "the Decred network's consensus rules" in the event of conflict. Constitutions typically speak

with more authority. Decred's version does not offer detailed rules for interuser conflicts, specify inviolable rights, or provide for dispute resolution, thus making it not much at all like a constitution proper.

Best Practices. When parties form a legally binding agreement, they enter into a powerful kind of relationship: privity of contract. Without privity of contract, a protocol cannot structure relations between the parties within its network in a regular, predictable, rule-bound manner. With privity of contract, a protocol can justly claim to have the consent of those it governs. In this way, distributed governance can improve on traditional terrestrial governments.

Most protocols allow the public to participate in their functions, to some degree, by dint of purchasing their crypto-tokens. Such a purchase typically occurs in a spot transaction, without the offer or acceptance of detailed contract terms. The seller offers so much Ether for so much Bitcoin; the buyer accepts; the funds duly transfer; and miners update the distributed public ledger accordingly. The parties do not agree to any other duties; they walk away strangers.

Airdrops of cryptocurrencies, wherein promoters make gifts of their tokens to potential users, do even less to define the terms of the parties' new relationship. The putative members of these new distributed communities are not in privity of contract with the protocol or with each other. There is no other way to impose obligations on the recipient, except perhaps through computational limits on the tokens' use.

Despite operating something like corporations or cooperatives, distributed-protocol communities do not typically possess legal personality. They are not persons in the law, capable of holding title, entering into contracts, and engaging in civil litigation. Most protocols have some kind of supporting foundation—Dash uses an exotic Cayman Islands "foundation company" structure allowing for an ownerless and memberless investment fund (Szilard 2019b)—but such foundations generally do not have the same power to control a protocol's functions that a company has over its operations. Someone who buys a token, which affords voting and other rights, does not typically thereby enter into a contract with the distributed community itself. There is no legal person on the protocol side to contract with.

However, each participant in a cryptocommunity could enter into privity with every other participant. They would do so via a mutual and continuing contract that sets forth the terms of their self-governance. This contract would resemble a traditional constitution in many respects but would claim the justification of express (not merely hypothetical or implied) consent.

It might not be practical to establish mutual privity among every holder of every cryptocurrency. It should be possible to put those who run network nodes under a common agreement, though. Most will download software to take part in the network, providing an apt point to build in a step to click "OK" on the co-contract (as one might call it). To bring into privity those parties accessing the network with self-authored software, the protocol could include contract-formation processes as part of routine internode handshakes.

So goes the theory of how to build a protocol community on the solid foundations of contract. How does it go in actual practice? Right now, not so well.

Even the best industry practices at present fall far short of ideal. That is not an insignificant problem. Without a foundation built on privity of contract, distributed protocols can never self-govern effectively. If a distributed community offers no laws or fora for resolving user disputes, terrestrial sovereigns will rush to fill the void.

For protocols ready to upgrade to more robust and independent processes, it should happily not be too difficult to establish distributed governance on the firm legal foundation of mutual privity. How? Include a choice-of-law and choice-of-forum clause in the contract mutually binding protocol users. Without this essential piece of self-governance, a distributed community faces exposure to laws and courts from the world over—an anathema to predictability. With it, a protocol secures the rule of law.

A protocol could choose any number of rule sets and dispute-resolution processes. It is most important to choose something in the first instance. A protocol could, for instance, specify the laws of Singapore and a professional arbitration service. The functional structure of distributed protocols suggests, however, that they would do better to adopt (or generate) local law and to resolve interuser disputes in native bodies.

EOS's constitution has the right idea in invoking its own (rather threadbare) law, but a protocol can do better than a vague wave at "the Maxims of Equity." If distributed systems aim to offer an alternative to traditional governments, as they loudly proclaim they do, they will have to offer detailed rules for a wide range of disputes. Protocol users might disagree about matters including contracts, trusts, property, negotiable instruments, secured transactions, and even real property, estates, and family law. Where people go, their many various problems follow.

But how can a protocol offer its users a full-blown set of laws without tying itself to a traditional sovereign's lawmakers? Ulex offers a ready-made solution (Bell 2019). It was written to solve a similar problem for special jurisdictions that wanted to import quality laws without also importing foreign flags. A protocol trying to avoid relying on real-space law could in the alternative try writing everything from scratch—a daunting prospect and one not likely to sway skeptics. Or perhaps it could interpret Ulex in its own courts to develop a native common law over time, a rather more attractive option.

Having once established privity of contract among its users, a protocol can ensure that they agree to have their disputes resolved solely by the community's own laws in its own courts. The parties could choose other laws or fora by mutual agreement after the fact, of course. Best practices in governance call for having workable rules already in place, however, to serve as trusted defaults. They also call for choosing laws and dispute-resolution mechanisms that users can count on as independent, impartial, and effective at keeping the peace.

Conclusion: Upgrading Distributed Governance

This article introduced distributed-protocol communities as worthy subjects for the study of self-governance and offered an early assessment of some leading examples. The

Distributed-Governance Index aimed more at reporting practices in the field than at assessing their value. It remains unclear whether the good intentions behind plans for increasingly complicated systems of governance will have equally good results. What did the DGI discover about the current state of the art? Table 10 summarizes the results by protocol; table 11 does likewise by variable.

As noted earlier, the DGI reveals a roughly inverse relation between a protocol's market capitalization and the sophistication of its system of self-governance. One might draw the conclusion that good governance does not attract investors or perhaps even repels them. Additional evidence suggests another cause for that apparent correlation, however: maturity. Consider figure 1, which reports the age of each indexed protocol as measured in days since first use. It shows that protocols with higher market capitalization, toward the top of the list, tend also to have been around longer. That should not cause surprise. It takes time to attract investments—especially an amount rivaling the more than $100 billion invested in Bitcoin.

It thus seems most likely that sophisticated governance correlates with low market capitalization not because one causes the other but because relative youth causes both.

Table 10
Summary of Protocols' Overall Performance in the Distributed-Governance Index

Protocol	Summary of Overall Performance in Index
Bitcoin (BTC)	Low in all measures of governance except open proposals and self-amendment
Ripple (XRP)	Low in most measures except vulnerability to 51 percent attack and chain cleaning
Ethereum (ETH)	Low in all measures but open proposals, self-amendment, and commons funding
Bitcoin Cash (BCH)	Low in all measures of governance except open proposals and self-amendment
Litecoin (LTC)	Low except for vulnerability to 51 percent attacks, open proposals, and self-amendment
EOS	Medium to high in all measures except secret voting; one of three protocols with self-amendment
Tezos (XTZ)	High in five measures; low in two; one of three protocols to provide on-chain amendments and commons funding; one of two protocols scoring high on chain cleaning
Dash (DASH)	Mixed results—high in three measures, medium in two, low in two; one of three protocols to provide on-chain commons funding
Decred (DCR)	High in five measures, low in two; one of three protocols to provide on-chain amendments and commons funding; one of two protocols scoring high on chain cleaning
Horizen (ZEN)	Fair performance in all measures except user privity; only protocol to take steps toward secret voting

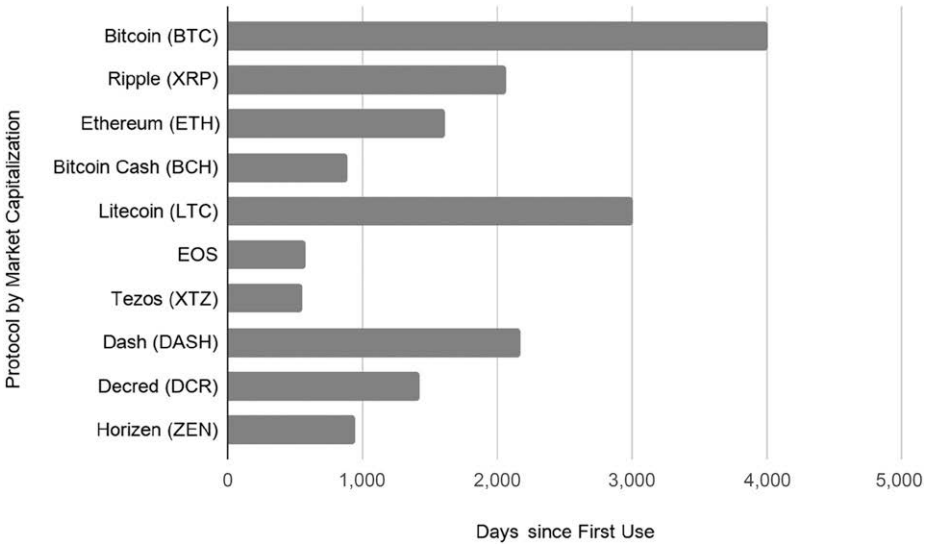
Table 11
Summary of Protocols' Overall Performance in the Distributed-Governance Index

Variable	Summary of Observations in Index
51 Percent Attack	Largest protocols (except Ripple) score lowest; smaller ones, higher.
Chain Cleaning	Largest protocols score lowest; smaller ones, higher.
Secret Voting	All score low except for Horizen, with a medium score.
Open Proposals	All except Ripple score fair; smallest tend to score best.
Self-Amendment	All score low except EOS, Tezos, and Decred, but almost all offer something.
Commons Funding	Largest protocols tend to score lowest; smaller ones higher.
User Privity	All score low except EOS, with a medium score.

Newer protocols tend to focus on governance because they aspire to do better than their predecessors, which naturally tend to rest on their laurels, confident in what has thus far worked for them. It will take upstart protocols time to get governance figured out in the first instance and then more time to attract well-earned investment.

It therefore remains uncertain whether it hurts a distributed protocol to have a comparatively well-developed governance system. Whether such a system helps remains

Figure 1
Ages of Indexed Protocol



an open question, too. A few protocols have attracted investment and use thanks to their express commitments to satisfy common goals efficiently and equitably through well-intentioned, well-documented, and well-executed procedures. Promising good governance evidently sells. So far, however, the nascent state of the industry leaves good governance only that: a promise.

A comprehensive review of how often promises of good governance have historically come to fruition would doubtless reveal a long history of disappointments. Perhaps the speed and agility of distributed protocols will help them do better than conventional governments on that count. Success will probably not come from automating everything, however. Institutions that govern humans must include human choice.

This is not merely a question of ethics—of guaranteeing that whatever governs humans remains *humane*. Computers cannot govern humans well for, appropriately enough, *computational* reasons. At least as far back as the 1950s, under the heading of cybernetics, researchers of information-control systems recognized the Law of Requisite Variety (a.k.a. Ashby's Law): "A control system must be able to embody at least as much variety as the variables it regulates" (Principia Cybernetica 2001).

This means that mere code cannot presently suffice to regulate all the many various things that humans will do on distributed protocols. Perhaps artificial intelligence will someday outstrip human complexity, granted, but that day has yet to come. In the meantime, computer code falls far short of the sophistication of even a solitary person, much less a whole community of people. Machines thus cannot govern humans. They can help, though. As Vitalik Buterin (2017) forecasts, the future of governance will likely find computers and humans working together toward a *multifactorial consensus*.

The question is not whether a distributed protocol can govern humans without humans. It cannot. The question is: Can humans govern themselves through distributed protocols? And, more than that, if they can do so, can self-governance through distributed protocols improve on governance services provided by conventional, centralized, territorial sovereigns? The Distributed-Governance Index offers not so much answers to these questions as ways to answer them, a vantage for continuing observations of fascinating and potentially significant developments in the evolution of distributed-protocol communities.

References

Bell, Tom W. 2019. Ulex. Github, December 19. At https://github.com/proftomwbell/Ulex/blob/master/README.md.

———. Forthcoming. DAOs Gone Wild: The Evolution of Decentralized Autonomous Organizations. In *Blockchain and the Law,* edited by Giovanni De Gregorio and Oreste Pollicino. Cheltenham, U.K.: Edward Elgar.

Bitcoin. n.d. bips. Github. At https://github.com/bitcoin/bips.

Bitcoincash.org. 2019. Home page. At https://www.bitcoincash.org/.

Bitcoin.org. n.d. Bitcoin—Open Source P2P Money. At https://bitcoin.org/en/.

Bitcoin Wiki. 2016. Value Overflow Incident. July 22. At https://en.bitcoin.it/wiki/Value_overflow_incident.

Blockchain Content Research. n.d. A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin. At https://blockchain.comsys.rwth-aachen.de/.

Block.one. n.d. EOSIS. At https://eos.io/.

Blockops. 2017. How to Create a Proposal for ZenCash. *Horizen Forum: Pitchdeck,* July 25. At https://forum.horizen.global/t/how-to-create-a-proposal-for-zencash/235.

Breitman, Arthur. 2017. There Is No Need for Hard Forks. *Medium,* May 14. At https://medium.com/tezos/there-is-no-need-for-hard-forks-86b68165e67d.

Buterin, Vitalik. 2017. Notes on Blockchain Governance. December 17. At https://vitalik.ca/general/2017/12/17/voting.html.

———. 2019. On Collusion. April 3. At https://vitalik.ca/general/2019/04/03/collusion.html.

Button, M. 2019. Against Illegal Content on the Blockchain. *Moneybutton* blog, January 31. At https://blog.moneybutton.com/2019/01/31/against-illegal-content-on-the-blockchain/.

Canellis, David. 2018. EOS Startup Utilizes Backdoor to Access User Wallets, Retrieve Airdropped Tokens. *TNW Hardfork,* December 12. At https://thenextweb.com/hardfork/2018/09/12/eos-platform-botched-airdrop/.

CoinMarketCap. 2019. Website, various pages. December 12. At https://coinmarketcap.com/.

Daian, Philip, Tyler Kell, Ian Miers, and Ari Juels. 2018. On-Chain Vote Buying and the Rise of Dark DAOs. July 2. At http://hackingdistributed.com/2018/07/02/on-chain-vote-buying/.

Dash. n.d. Your Money, Your Way. At https://www.dash.org/.

Dash Central. n.d. Getting Started. At https://www.dashcentral.org/gettingstarted.

Dash Core Group Inc. 2018. Understanding Dash Governance. At https://docs.dash.org/en/stable/governance/understanding.html.

———. n.d. Features: Dash Latest Documentation—Sporks. At https://docs.dash.org/en/stable/introduction/features.html?highlight=spork#sporks.

Decred Developers. n.d. Decred Is an Autonomous Digital Currency. At https://decred.org/.

Decred Project. 2019a. Consensus Rule Voting. At https://docs.decred.org/governance/consensus-rule-voting/overview/.

———. 2019b. Decred Constitution. At https://docs.decred.org/governance/decred-constitution/.

———. 2019c. Navigating Politeia Data. At https://docs.decred.org/advanced/navigating-politeia-data/

———. 2019d. Politeia. At https://docs.decred.org/governance/politeia/overview/.

EOS Core Arbitration Forum Ltd. 2018a. ECAF Rules of Dispute Resolution. At https://www.eoscorearbitration.io/home/governance/.

———. 2018b. EOS Constitution. June 26. At https://www.eoscorearbitration.io/home/governance/.

EOSIO. 2018. *EOS.IO Technical White Paper v2.* March 16. At https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md#governance.

EOSIO Enhancement Proposals. n.d. EEPs. At https://eeps.io/.

Ethereum. 2019a. EIP Purpose and Guidelines. December 21. At https://github.com/ethereum/EIPs/blob/master/EIPS/eip-1.md.

———. 2019b. Home page. December 17. At https://ethereum.org/.

———. 2019c. Proof of Stake FAQ. August 2. At https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ#what-are-the-benefits-of-proof-of-stake-as-opposed-to-proof-of-work.

Ethereum Foundation. n.d. Ethereum Foundation Grants. At https://ethunicorns.typeform.com/to/XhZlnp.

Fiach_Dubh. 2019. Comparing Double Spend Resistance: Decred VS Bitcoin — Part 1. *Medium,* May 15. At https://medium.com/coinmonks/comparing-double-spend-resistance-decred-vs-bitcoin-part-1-330c8081b2a9.

Floyd, David. 2018. The EOS Arbitrator Problem: A Crypto Governance Breakdown Explained. *CoinDesk,* June 27.

Gilbert, Michael D. 2019. Transparency and Corruption: A General Analysis. *University of Chicago Legal Forum* 6:117–38.

Hertig, Alyssa. 2018. Blockchain's Once-Feared 51% Attack Is Now Becoming Regular. *CoinDesk,* June 9.

Hodor. 2018. Why Consensus Is Better Than Proof of Work. *XRP Blog,* June 7. At https://xrpcommunity.blog/consensus-model-vs-proof-of-work/.

Horizen. 2019a. The Rise from a Malicious Attack—Horizen's 51% Attack Solution. February 15. At https://blog.horizen.global/horizens-51-attack-solution/.

———. 2019b. Unbounded by Design. At https://www.horizen.global/.

———. n.d. ZenDAO Treasury and Voting System. At https://www.horizen.global/zendao/.

Jentzsch, Christoph. 2016. The History of the DAO and Lessons Learned. *Medium,* August 24. At https://blog.slock.it/the-history-of-the-dao-and-lessons-learned-d06740f8cfa5.

Kaiser, Ben, Mireya Jurado, and Alex Ledger. 2018. The Looming Threat of China: An Analysis of Chinese Influence on Bitcoin. October 5. At https://arxiv.org/pdf/1810.02466.pdf.

Karbowiak, Aneta. 2019. EOS Worker Proposal System (WPS) Being Considered Again. *Decentium,* October 25. At https://decentium.org/eosnetworkxx/eos-worker-pb.

Kim, Christine. 2019. Welcome to Athens: Tezos Completes "Historic" First Blockchain Vote. *CoinDesk,* March 20.

Litecoin Project. 2019. Litecoin. At https://litecoin.org/.

———. n.d. Litecoin Project. At https://github.com/litecoin-project.

Maas, Thijs. 2018. Everything They Don't Want You to Know about EOS, the "Ethereum Killer." *Hackernoon,* June 8. At https://hackernoon.com/everything-they-dont-want-you-to-know-about-eos-the-ethereum-killer-9939c43aa2df.

Madore, P.H. 2019. Vitalik Buterin: Ethereum Governance Is Currently Underrated. *Cryptocurrency News,* March 19. At https://www.ccn.com/vitalik-buterin-ethereum-governance-is-currently-underrated/.

McKenzie, William. 2019. Inflation in Liquid Proof-of-Stake Models. *Medium,* July 9. At https://medium.com/tezoscommons/inflation-in-liquid-proof-of-stake-models-5d19c3076605.

Pabst, Rosario. 2018. ZenCash Treasury and Voting Model Update. *Horizen Blog,* March 23. At https://blog.horizen.global/zencash-treasury-and-voting-model-update/.

Pozzi, Daniele. 2019. The Land of the Free: Why Decentralization Matters in the Crypto Republic. *Cointelegraph,* June 5. At https://cointelegraph.com/news/the-land-of-the-free-why-decentralization-matters-in-the-crypto-republic.

Principia Cybernetica. 2001. The Law of Requisite Variety. At http://pespmc1.vub.ac.be/REQVAR.html.

Ripple. 2019. XRP. At https://ripple.com/xrp/.

S+C Intelligence. 2019. Cryptoasset Report: Decred. March 1. At https://sci.smithandcrown.com/research/decred-report.

———. n.d. Litecoin. At https://sci.smithandcrown.com/projects/litecoin.

Scott, Tamara. 2018. 9 GitHub Alternatives for Source Code and Version Control. *Technology Advice,* September 1. At https://technologyadvice.com/blog/information-technology/github-alternatives/.

Springer. 2018. A Reliable Cryptocurrency Needs Good Governance, Say Researchers. *Science Daily,* September 12.

Szilard, Justin. 2019a. Binance Considers Rollback of Bitcoin to Reverse Hack Casting Immutability Doubts. *DashNews,* May 9.

———. 2019b. Dash Launches Dash Investment Foundation to Expand Growth Opportunities. *DashNews,* May 10.

———. 2019c. Dash Version 0.14, Including Anti-51% Attack ChainLocks, Released on Testnet. *DashNews,* March 29.

Tezos Foundation. n.d. A Digital Commonwealth. At https://web.archive.org/web/20190706212440/https://tezos.foundation/a-digital-commonwealth.

Viglione, Robert, Rolf Versluis, and Jane Lippencott. 2017. *Zen White Paper*. At https://www.horizen.global/assets/files/Zen-White-Paper.pdf.

web3bch. 2018. BDIPs. November 3. At https://github.com/web3bch/BDIPs/blob/master/BDIPs/bdip-1.md.

xrp_sea. 2018. Could XRP Fork? *XRP Chat,* November 17. At https://www.xrpchat.com/topic/28967-could-xrp-fork/.

Yocom-Piatt, Jake. 2018. Politeia in Production. *Decred Blog,* October 15. At https://blog.decred.org/2018/10/15/Politeia-in-Production/.

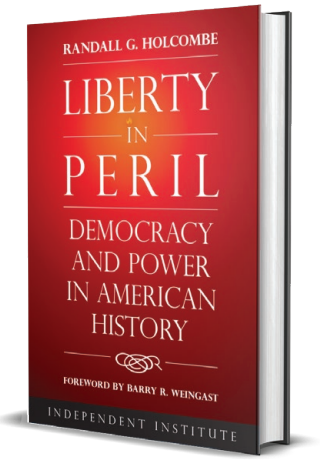
Acknowledgments: The author thanks Reflector Network for supporting the research for and writing of this essay under a Service Agreement with Chapman University, though he alone bears responsibility for its contents, which do not represent the views of any other party. Thanks for inspiration go to John Merrells and for research assistance to Alec Isaac.

SUBSCRIBE NOW AND RECEIVE A FREE BOOK!

"***The Independent Review*** does not accept pronouncements of government officials nor the conventional wisdom at face value."
—**JOHN R. MACARTHUR**, Publisher, *Harper's*

"***The Independent Review*** is excellent."
—**GARY BECKER**, Nobel Laureate in Economic Sciences

Subscribe to ***The Independent Review*** and receive a free book of your choice such as ***Liberty in Peril: Democracy and Power in American History***, by Randall G. Holcombe.



Thought-provoking and educational, ***The Independent Review*** is blazing the way toward informed debate. This quarterly journal offers leading-edge insights on today's most critical issues in economics, healthcare, education, the environment, energy, defense, law, history, political science, philosophy, and sociology.

Student? Educator? Journalist? Business or civic leader? Engaged citizen? This journal is for YOU!

Order today for more *FREE* book options

SUBSCRIBE

The Independent Review is now available digitally on mobile devices and tablets via the Apple/Android App Stores and Magzter. Subscriptions and single issues start at $2.99. **Learn More.**

Download on the App Store | GET IT ON Google Play | Available on MAGZTER

INDEPENDENT INSTITUTE, 100 SWAN WAY, OAKLAND, CA 94621 • 1 (800) 927-8733 • ORDERS@INDEPENDENT.ORG