KARPETA

Teknokultura. Revista de Cultura Digital y Movimientos Sociales
ISSNe: 1549-2230

http://dx.doi.org/10.5209/TEKN.64523

EDICIONES COMPLUTENSE

Decentralizing democracy: approaches to consensus within blockchain communities

Christopher Tozzi[1]

Recibido: 28 de mayo 2019 / Aceptado: 14 de octubre 2019 Open peer reviews

Abstract. Creating fair, transparent and genuinely democratic modes of decentralized decision-making has been a key concern for many developers and users of blockchains. This article evaluates several popular methods of maintaining consensus and achieving decentralized decision-making on blockchain networks in order to assess the extent to which blockchains challenge the norms of the liberal-democratic order. In particular, it compares and contrasts Proof-of-Work, Proof-of-Stake and Practical Byzantine Fault Tolerance consensus mechanisms, assessing not just how they operate in a technical sense but also (and most important) the political, economic and social dimensions of these different blockchain governance strategies. This comparison highlights efforts by blockchain communities to redefine or push the bounds of democracy, as well as the challenges they have faced in their efforts to create digital democracies that do not reproduce the same economic and social inequalities present in traditional democratic systems.
Keywords: bitcoin; democracy; governance; Proof-of-Work.

[en] Descentralizando la democracia: planteamientos de consenso entre las comunidades de blockchain.

Resumen. La creación de modelos justos, transparentes y genuinamente democráticos de toma de decisiones descentralizadas ha sido una preocupación clave para muchos desarrolladores y usuarios de blockchain. Este artículo evalúa varios métodos populares para mantener el consenso y lograr una toma de decisiones descentralizada en las redes blockchain para evaluar en qué medida las blockchains desafían las normas del orden liberal-democrático. En particular, compara y contrasta los mecanismos de consenso de Prueba de trabajo, Prueba de estaca y Tolerancia práctica a la falla bizantina, evaluando no solo cómo operan en un sentido técnico sino también (y lo más importante) cómo operan las dimensiones políticas, económicas y sociales de estas diferentes estrategias de gobierno de blockchain. Esta comparación destaca los esfuerzos de las comunidades blockchain para redefinir o empujar los límites de la democracia, así como los desafíos que han enfrentado en sus esfuerzos por crear democracias digitales que no reproduzcan las mismas desigualdades económicas y sociales presentes en los sistemas democráticos tradicionales.
Keywords: bitcoin; demogracia; governanza; Prueba-de-Trabajo.

[1] Rensselaer Polytechnic Institute (EEUU)
E-mail: tozzic@rpi.edu

Cómo citar: Tozzi C. (2019). Decentralizing democracy: approaches to consensus within blockchain communities. *Teknokultura. Revista de Cultura Digital y Movimientos Sociales, 16*(2), 181-195.

1. Introduction

Francis Fukuyama famously argued in 1989 that the world had stumbled into "the end of history". He meant that the liberal-democratic order had triumphed, and that the societies rooted in capitalist economic thought and representative democracy would never again face serious, existential threats to their ideological frameworks.

Thirty years later, Fukuyama's thesis has now been the butt of many jokes. Fukuyama himself retreated somewhat from the argument a couple of years ago, telling a journalist that the liberal-democratic order that had seemed to triumph at the end of the Cold War is now heading "backward" (Tharoor, 2017).

To date, the lion's share of the criticism of Fukuyama's "end of history" thesis has been fueled by the trend toward authoritarianism, or the scaling back of democratic institutions, in a number of societies once considered bastions of liberal democracy, such as France, Italy and the United States. The resurgence of Russian territorial aggrandizement, and the global ascendancy of a China that hardly fits the liberal-democratic framework, have also been cited to dismiss the meaning that Fukuyama affixed to the collapse of the Soviet Union (Tharoor, 2017).

These criticisms are valid, but for two main reasons, they don't present a full picture of the threats that the liberal-democratic order faces today. First, they focus on challenges to democratic societies that originate either within those societies' own institutions, or from rival states. The reason liberal democracies are not as safe as Fukuyama thought, we are told, is that they are at risk of electing authoritarians, or of being subsumed by foreign powers opposed to liberal-democratic ideology.

Second, conventional criticisms of the end of history thesis imply that the chief threat to the liberal-democratic order arises only from anti-democratic forces that seek to destroy liberal democracy entirely. In other words, they focus on efforts to scale back, subvert or destroy entirely the democratic institutions and principles that are at the core of liberal-democratic societies.

In this article, I'd like to shed light on another type of challenge to the liberal-democratic order, one that has so far garnered little attention from the political scientists and economists who are engaged in evaluating the health of liberal democracies. That challenge is the ideologies of decentralized consensus that have developed within the communities of programmers and users who have created blockchain-based software platforms over the past decade. In this context, consensus refers to the strategies and processes that allow computers connected to a blockchain to determine which data is accurate or genuine, and therefore reflects the consensus of the community. Because blockchains lack a central authority that can make decisions on behalf of the community about what to consider valid, blockchain developers and users have implemented various technical solutions for establishing consensus in a decentralized fashion, by weighing the preferences of different computers (or nodes) on the blockchain in various ways. As I explain below, the different decentralized consensus techniques developed to date reflect different approaches to thinking about democratic governance.

A study of how members of blockchain communities think about democratic norms and values reveals two key insights into the state of liberal democracy today that conventional analyses of the end of history thesis miss. First, they show that it is not only illiberal politicians and state actors who pose a threat to the liberal-democratic order as Fukuyama conceived it. Equally subversive, at least in potential, are the radically new paradigms of governance and decentralized decision-making that have emerged within the technological realm of the blockchain.

Second, blockchain communities' challenge to the liberal-democratic order is significant in that it arises not from anti-democratic motives, but, on the contrary, from actors who believe that the democratic institutions and processes on offer in Western liberal-democratic societies are not democratic or fair enough. In theorizing new modes of self-directed community governance, blockchain enthusiasts seek to pioneer novel strategies of social and political organization, marked by heavy investment in the concept of decentralization and the leveraging of digital technologies and processes to make possible modes of collective decision-making that would not be feasible in most non-digital contexts.

2. The political essence of blockchain technology

It may seem unusual to turn to blockchain platforms as a way of studying contemporary innovations in democratic governance. Blockchain projects have made few headlines in the mainstream press related to political or social questions. If most people have heard of blockchain today, it is only because of the financial speculation that propelled the value of a Bitcoin to around 20,000 dollars in late 2017 (Kharpal, 2018). That trend spawned much debate about the economic significance of cryptocurrency, how governments should regulate cryptocurrency trading and whether non-governmental currencies such as Bitcoin could ever become practical for real-world financial use.

Yet questions of economics and finance reveal only part of the significance of blockchain technology. Below the surface, ideological concerns over political and social equality have played equally foundational roles in the development of many blockchain projects. Indeed, the origins of the first blockchain, Bitcoin, suggest that resentment of conventional, centralized institutions – and, perhaps, a sense that the liberal-democratic order was not as liberal or democratic toward ordinary citizens as it claimed – was critical in birthing blockchains and the concept of decentralized consensus in the first place. We don't know the real-world identity of the creator of Bitcoin, or why exactly he, she or they chose to do it; we know only the pseudonymous name of Bitcoin's purported creator, Satoshi Nakamoto. We do know, however, that among the first set of data appended to the Bitcoin blockchain at the time of its creation on January 3, 2009, was the message "Chancellor on brink of second bailout for banks" (Abridged History, 2013). The text referenced a headline from the *London Times* about plans by the British government to issue massive taxpayer-funded loans to the country's teetering financial industry.

Bitcoin's creator did not elaborate on the message, and so interpretations of its significance can only be speculative. It is possible that the headline was chosen at random, as part of an effort to attest to the date on which the Bitcoin blockchain came into existence. However, given that no other references to news events have been

encoded within the Bitcoin blockchain, it seems more likely that Bitcoin's creator chose to include this statement at the very start of the blockchain in order to send a political and economic message. In calling out the British government's decision to bail out banks, Bitcoin's creator probably sought to highlight both the shortcomings of the conventional finance industry, which had made itself virtually insolvent and then turned to the government for rescue, and the fact that ordinary citizens were allowed no opportunity to participate directly in the process of deciding whether public funds should be allocated to those failing institutions.

Bitcoin theoretically offers a solution to both of these problems. By providing a virtual currency that anyone can use without depending on a government or banks to regulate it, Bitcoin promises to free individuals from having to interact with the conventional finance industry. And by pioneering a new mode of decentralized decision-making for controlling that cryptocurrency and the blockchain on which its transactions are recorded, Bitcoin provides an alternative to the centralized, representative-democratic government institutions that, in the eyes of Bitcoin's creator, had seemed to fail to empower their constituents fairly during the post-2008 financial crisis.

If upending traditional finance and government institutions was indeed the goal of Bitcoin's creator, then Bitcoin would appear to have been conceived as a direct challenge to the liberal-democratic order that had produced a political and economic system in which large financial institutions could count on low-cost government loans in times of trouble, without affording taxpayers a role in the governance process.

Thus, there is likely a direct link between the rise of blockchain technology as a whole and anxiety over the liberal-democratic that fascinated Fukuyama. Moreover, as I show below, debates about the meaning of democracy, and how best to implement democratic decision-making within a decentralized network of constituents, have featured prominently in conversations about other blockchain projects and initiatives. While political and social questions are hardly the only concern of blockchain enthusiasts, it is impossible to divorce the technical dimensions of blockchain technology from their social and political implications.

In studying how political ideology has impacted strategies for governance in blockchain communities, I aim not to present blockchain as an abstract test case for evaluating political thinking within technological communities, but instead to assess to what extent blockchain communities have succeeded in achieving the Bitcoin creator's apparent goal of contesting the end of history supposedly imposed by the liberal-democratic order.

The democratic ideologies that have evolved within blockchain communities take multiple forms. It would be wrong to speak of "blockchain democracy" as a singular entity. And indeed, part of my goal in this article is to demonstrate the various forms of democratic governance that different blockchain communities have developed or envisioned. I seek, then, to evaluate the extent to which, and the reasons why, they diverge from conventional liberal-democratic ideology.

In short, my argument is that communities within the blockchain ecosystem are pioneering new modes of governance that present radical challenges to the liberal-democratic framework that supposedly triumphed at the end of the Cold War. An examination of the governance strategies of blockchain communities, and debates about the technical as well as political and social merits of different approach-

es to governance and consensus, reveals how the new technological frontier of the blockchain is breeding alternative notions of democratic organization that Fukuyama could hardly have imagined in 1989.

3. Governance and consensus in blockchain communities

Before evaluating different governance strategies used by blockchain communities, let me first provide an overview of what governance means on a blockchain, how it relates to consensus and which unique challenges blockchains must resolve in order to achieve effective governance and consensus.

A blockchain is a specialized type of database that stores data in such a way that the data is distributed across a number of independent computers or other devices, typically called nodes (Some newer blockchains, such as Ethereum and NEO, also allow nodes to share compute resources, in addition to data storage, across the network). Blockchains allow data only to be added to the database; they are designed to make it effectively impossible to remove or modify data once it has been recorded to a blockchain.

Unlike conventional databases, where data may be distributed across multiple host servers but is centrally controlled by one organization, blockchains are composed of nodes operated by independent parties. This is why they are said to be decentralized.

This decentralized architecture is blockchain's killer feature. By eliminating centralized control over the data or other resources that are shared between nodes, a blockchain makes it very difficult for a single malicious party to delete or manipulate resources. Resources can be modified only with the consensus of a majority of nodes on the blockchain, a feat virtually impossible for a malicious actor to achieve provided that the blockchain is sufficiently large, and that the nodes composing it are sufficiently independent of and disinterested from one another.

Yet the decentralized nature of blockchains also presents a significant technical and social challenge: Maintaining consensus between nodes in order to ensure that all members of the network agree with any decisions made by the network.

This is critical for two main reasons. First, it is essential for storing data reliably, since a lack of consensus would mean that one node's copy of the blockchain's data might conflict with another node's, leading to inconsistency and ineffective data storage. Second, consensus allows a blockchain's underlying protocol, meaning the rules that govern how it is organized and how nodes interact, to be updated. In the history of most of the mainstream blockchains that exist today, such as Bitcoin and Ethereum, it has periodically been necessary to modify the protocol in response to security or performance issues (Galea, 2018). When a protocol change is proposed, all nodes must agree to accept the change, because it would be impossible for different nodes to use different protocols on the same blockchain.

Given that the nodes on a blockchain are decentralized and operate independently, and in general no node can compel another node to behave in a particular way, maintaining consensus poses a complex problem, which different blockchain communities have addressed in different ways. As I will argue below, the various governance and consensus solutions developed or proposed to date reflect not only efforts at technical but also political and social innovation.

4. Classic consensus: "Nakamoto" Proof-of-Work

Peer-to-peer networks that resemble blockchains in some ways have existed for decades. What made the Bitcoin blockchain so innovative when it debuted in early 2009, however, was the novel solution for decentralized consensus that Bitcoin's pseudonymous creator, Satoshi Nakamoto, developed for Bitcoin. That solution, known as Nakamoto Proof-of-Work (or PoW), was the consensus architecture for the first blockchains, and it remains the most widely used solution today.

Under the Nakamoto Proof-of-Work model, nodes on the blockchain have the option, but not obligation, of participating in the process of data verification and governance by operating as so-called miners. A miner nodes solves a complex cryptographic puzzle that, when complete, earns the node the right to add a new string of data, known as a block, to the blockchain. Other nodes on the network can perform simple cryptographic operations to ensure that the miner indeed solved the cryptographic puzzle correctly and is appending legitimate data to the blockchain. When a miner's block is confirmed as valid by the blockchain network, the miner receives a reward in the form of cryptocurrency.

Because any node on the blockchain has the opportunity to confirm whether a newly mined block is valid based on the cryptographic puzzle that was solved to produce the block, the Proof-of-Work mining process ensures that the network as a whole participates in the confirmation of data that is added to the blockchain. Thus, mining achieves consensus across the decentralized network.

An additional feature of the Proof-of-Work strategy is that the cryptographic puzzle that must be solved to mine a new block is based in part on data that was previously added to the blockchain. As a result, the mining of new blocks serves to confirm and reconfirm the legitimacy of existing data stored by the decentralized network, thereby allowing the blockchain to maintain the integrity of historical data.

For blockchains that have adopted Proof-of-Work as their consensus solution, such as Bitcoin and Ethereum, the strategy has worked well in most technical respects for achieving its core mission of maintaining a single version of data across a large, decentralized network. These blockchains have not suffered major problems associated with a lack of consensus.

Yet in other respects, the Proof-of-Work method has proved to have deep flaws. Some of these shortcomings are technical in nature; the most well-known problem within this category is the slow pace of data recording that results from the process of requiring miners to solve cryptographic puzzles before new blocks can be appended to the blockchain. It is for this reason that the Bitcoin blockchain, for example, can currently record only about a half-dozen transactions per second, a limitation that has led more than few observers to question the real-world viability of Bitcoin's blockchain as a way of recording cryptocurrency transactions. ("Blockchain speeds", 2018).

Sustainability activists have also raised concerns about Proof-of-Work governance due to the enormous amounts of electricity that miner nodes consume in order to solve the cryptographic puzzles described above. According to one study (de Vries, 2018) the total annual energy consumed by Bitcoin mining is approximately equivalent to that expended yearly by the entire population of Ireland. Given the environmental implications of this energy consumption, and the fact that it serves no other purpose than maintaining consensus, Bitcoin and other blockchains that

use Proof-of-Work as the foundation for decentralized decision-making have faced increasing pressure to adopt alternative governance strategies (Hugo, 2018).

But it's not only on technical and environmentalist grounds that Proof-of-Work has proved controversial. Some members of blockchain communities have questioned the core political and social assumptions that underlie the Proof-of-Work model, and it is at this juncture that blockchain's implications for the liberal-democratic order begin to become clearest.

As one blockchain enthusiast wrote on Reddit in 2018, "Bitcoin is NOT a democracy" because "not every node gets to vote". Instead, it's only miner nodes that enjoy the privilege of making decisions about which data to record on the blockchain. The rest of the nodes store data that is verified by the miners, but they do not actively participate in the governance process.

By some measures, that arrangement might seem fair. Miner nodes perform the work required to achieve consensus, and so far they have done a good job of producing the intended results, so it's not unreasonable to vest governance power solely in them. Some advocates of the Proof-of-Work model have gone so far as to say that the consensus method used by Bitcoin and other major blockchains actually does a better job of achieving community consensus than do traditional democratic institutions. As the investor Roger Ver wrote on Twitter in 2017, "Proof of Work is several orders of magnitude better than democracy as a consensus mechanism".

But others don't see it this way. Criticizing Ver's claim, one Reddit user wrote that Proof-of-Work is only better than traditional democracy if one is a libertarian and believes that "poor people don't deserve representation" (Proof of work). Although the user did not elaborate on the statement, the message seems clear enough: By placing governance power only in the hands of miner nodes, Proof-of-Work disempowers the "poor" nodes that lack the compute resources necessary to participate in the mining process.

On this point, it is important to note that for an individual joining a device to a blockchain like Bitcoin, choosing whether to participate in Proof-of-Work as a miner or operate as a simple node is not a mere matter of personal preference, technical skill or even commitment to the blockchain community. What matters above all in order to participate in Proof-of-Work mining is access to high-cost computer hardware. Although it was once possible to mine Bitcoin using a simple PC, Nakamoto Proof-of-Work was designed in such a way that the cryptographic operations associated with mining become increasingly intense as the blockchain grows larger. As a result, for the past several years, solving the cryptographic puzzles required to participate in governance on most large Proof-of-Work blockchains requires so much computing power that a conventional device is not capable of delivering it. Instead, miners typically use expensive, specialized devices called "mining rigs", which use high-end graphics cards to provide the computing power required for mining.

What this means is that participation in governance on a Proof-of-Work blockchain has become a pay-to-play affair, with real-world capital expenditure required to have a say in how the blockchain operates. Complicating matters is the fact that many Bitcoin miners operate as part of "mining pools", through which they combine their computing resources and share the profits of mining. Most of these pools are owned by centralized, private companies. According to one estimate, one such company, F2Pool, controls about 25 percent of the total compute resources on the Ethereum blockchain (Cindx, 2018). Control is only slightly less centralized on the Bitcoin

blockchain, where the top five mining pools each account for about ten percent of the total mining operations performed on the network (Hashrate Distribution).

The Proof-of-Work consensus system also creates a technical-political liability for blockchains that use it in the form of so-called 51 percent attacks. In the event that a malicious actor were able to take control of more than half the mining power on a Proof-of-Work blockchain, even if only temporarily, that actor would be able to make unilateral decisions about the network's governance. Among other things, this means that the actor could rewrite or delete data that was previously verified and added to the blockchain. Because it is now possible to purchase temporary access to cloud-based mining rigs over the Internet and connect them to almost any blockchain, 51 percent attacks have become relatively easy to execute for individuals or groups who can amass enough capital to rent mining rigs running in the cloud. Large blockchains like Bitcoin and Ethereum have not proven susceptible to such attacks in recent years, but several smaller blockchains, which are easier to co-opt via a 51 percent attack because they have less total mining power, have been compromised in this way (Canellis, 2018).

5. Mining democratization: alternative Proof-of-Work solutions

Due to the ways in which Proof-of-Work privileges individuals and groups who enjoy an advantage in resources compared to their peers, blockchain governance based on Proof-of-Work would appear not to challenge liberal-democratic institutions in the way Bitcoin's creator apparently hoped as much as to embody their shortcomings. Although in theory anyone who chooses to join a Proof-of-Work blockchain can participate in its governance process, in practice the ability to do so is contingent upon access to real-world financial and material resources. This architecture allows powerful, centralized interests to co-opt what on the surface functions as a decentralized consensus technique.

This limitation has helped spur efforts to modify Proof-of-Work consensus models to make them less prone to co-optation by powerful parties. Equihash, a solution described by a professor and Ph.D. student at the University of Luxembourg in 2017 (Biryukov), has proven the most influential, having enjoyed adoption by some notable blockchains, including Zcash and Horizen. In place of the compute-intensive cryptographic puzzles used by the Nakamoto Proof-of-Work architecture, the Equihash model requires miner nodes to solve puzzles that require significant computer memory, or RAM. Because RAM, unlike compute resources, is relatively inexpensive and cannot be obtained in large quantities through specialized mining rigs, the Equihash model theoretically makes it harder for financially powerful parties to centralize control over a blockchain, while also mitigating the risk of a 51 percent attack.

Equihash's designers were concerned first and foremost with solving the technical limitations of Proof-of-Work models that require significant computing power. However, Equihash's popularity has been driven in part by perceptions that it is "intended to achieve mining democratization" (Asolo, 2018), and to avoid the "centralized mining" of compute-intensive consensus mechanisms (Zcash). Rob Viglione, a co-founder of the Horizen project, emphasized the ideological ambitions behind the project's governance model even more forcefully, telling me in a February 2018 interview that the project's

goal is to create "a fully competitive, open governance framework". He added, "My wildest dream is for our voting system to become a proof of concept for a small nation to create cleaner, fairer governance".

Beyond Equihash, several other significant Proof-of-Work consensus solutions have emerged in recent years that reflect efforts to address the perceived lack of fairness in Nakamoto Proof-of-Work. Notable examples include Scrypt, NeoScrypt and CryptoNight. The algorithms behind these consensus mechanisms either use memory-intensive cryptographic puzzles, like Equihash does, or attempt to require compute-intensive mining operations to be performed by traditional CPUs, rather than high-end graphics cards.

It is thus clear that concerns over the undemocratic, less-than-decentralized nature of the original blockchain consensus solution have spawned a number of efforts to implement a seemingly fairer solution. Yet the alternative Proof-of-Work methods have not satisfied all blockchain enthusiasts. As a result, several alternative consensus solutions exist that discard the Proof-of-Work approach entirely in favor of other methods that their designers view as more genuinely democratic.

6. Proof-of-stake

To date, the most popular alternative to Proof-of-Work is what is known as Proof-of-Stake. First conceived in 2012, a Proof-of-Stake consensus model selects nodes more or less randomly to verify that data added to the blockchain is valid. The nodes do not have to perform complex cryptographic operations to verify data; they simply accept or reject the data's validity. In return for their work, they earn transaction fees, paid in the form of cryptocurrency.

By choosing nodes at random instead of allowing nodes to participate actively in the consensus process as miners (as would happen under Proof-of-Work), Proof-of-Stake theoretically prevents nodes or groups of nodes that possess extensive computer-hardware resources to enjoy greater influence over the consensus process than the rest of the network. It also does not require substantial expenditures of electricity, since there is no mining process to perform or cryptographic puzzles that nodes must solve.

In order to ensure that nodes participating in consensus have a "stake" in the blockchain (and are therefore incentivized to very data transactions accurately), Proof-of-Stake requires nodes that verify data to possess cryptocurrency whose transaction records are stored on the blockchain in question. The more cryptocurrency a node possesses, the higher its chances of being selected to verify data transactions and participate in governance.

The technical and political merits of Proof-of-Stake have generated extensive debate in the blockchain ecosystem, especially because of signs that Ethereum, one of the most influential public blockchains, might switch from Proof-of-Work to Proof-of-Stake (Beedham, 2019). Proof-of-Stake's critics contend that the solution could "compromise security or democracy" because a node's ability to participate in governance is proportional to the cryptocurrency it controls (Lindsey, 2018). In this sense, Proof-of-Stake is subject to the same criticisms as Proof-of-Work regarding the creation of a "pay-to-play" governance framework wherein "the rich get richer" (Nasgo). On the other hand, Proof-of-Stake has been applauded as a way to solve

the environmental sustainability problems associated with Proof-of-Work ("Proof-of-Stake is the Future").

Some blockchain communities have attempted to improve upon Proof-of-Stake by linking governance participation not to cryptocurrency owned, but to some other measure of participation in the network, such as how much storage space a node consumes. These approaches, which are known as Proof-of-Weight, remain relatively obscure and little-used. Most of the "weights" that they prioritize are proxies for material wealth, and Proof-of-Weight can therefore be subjected to the same political and social criticisms as Proof-of-Stake.

7. Delegated Proof-of-Stake

These weaknesses of Proof-of-Stake have spurred the development of an alternative variant called Delegated Proof-of-Stake. Under Delegated Proof-of-Stake, any individual or group who owns cryptocurrency stored on a blockchain can vote to designate which nodes will serve to verify data transactions. The more cryptocurrency voters own on the blockchain (and by extension, the higher their "stake" in the network), the greater their voting power. The nodes selected to verify data transactions through this process are called delegates, and they receive cryptocurrency as a reward for the work they perform in maintaining consensus.

The delegates themselves must have some stake on the blockchain in the form of cryptocurrency, but their ability to be selected as delegates does not necessarily increase with the more cryptocurrency that they own. Instead, delegates are theoretically selected based on the decentralized network's faith in their ability to maintain consensus effectively. Voting for delegates typically takes place continuously and in real time, with the result that delegates deemed to be malicious or ineffective by a majority of the network will quickly lose their delegate status.

Delegated Proof-of-Stake has been compared by some observers to corporate governance models in which shareholders elect board members through a process in which voting power is proportional to shares owned (Jenks). From this perspective, Delegated Proof-of-Stake may not seem especially innovative in a liberal-democratic world.

However, other advocates of Delegated Proof-of-Stake place greater faith in the model's unique ability to achieve a form of democratic governance that is truly decentralized and that does not reward wealthy stakeholders disproportionately. Delegated Proof-of-Stake has "more democratic features" than traditional Proof-of-Stake and other conventional consensus mechanisms, according to one explanation of the architecture (Miah, 2019). It functions as a "form of digital democracy", according to another ("What is Delegated Proof of Stake?"). One blockchain project, NASGO, which has adopted Delegated Proof-of-Stake to maintain consensus calls its entire platform a "decentralized democracy".

Whether Delegated Proof-of-Stake truly offers a digital democratic governance solution that resolves the shortcomings of modern liberal democracy by breaking down the relationship between wealth and power depends on one's perspective. The system does not prevent parties who hold large amounts of cryptocurrency on a given blockchain from centralizing control in their hands in the event that a majority of the

network elects those parties as delegates; it only removes the direct link between control over resources and participation in governance.

Moreover, in one sense, a blockchain that operates using a Delegated Proof-of-Stake model has a rational incentive to elect wealthy nodes as delegates. The more cryptocurrency a node controls on the network, the greater that node's incentive to maintain transaction records accurately. If records are not accurately maintained, the cryptocurrency stored on the blockchain risks losing its value. Less wealthy nodes are thus incentivized to place governance power in the hands of wealthy nodes because the latter have more to lose should they fail to govern effectively.

That said, supporters of Delegated Proof-of-Stake might point out that in most real-world liberal democracies, those elected to perform governmental functions might sometimes have more to gain personally from failing to govern effectively. For example, a corrupt politician might have greater incentive to maintain broken institutions that line his own pockets with bribes than to fix those institutions in a way that benefits his society as a whole.

This type of self-interested poor governance is harder to envisage within a Delegated Proof-of-Stake framework. Short of an outsider managing to gain designation as a delegate and then destroying a blockchain entirely in order to scuttle the value of its cryptocurrency – an act that in most cases would not reap significant material rewards for the intruder, but might be ideologically motivated – there are very few scenarios in which wealthy nodes within a digital blockchain community that maintains consensus via Delegated Proof-of-Stake would have a rational reason to govern ineffectively.

In short, Delegated Proof-of-Stake reflects a novel way of limiting the ability of financially or materially powerful parties to co-opt democratic governance. Whether it will succeed in practice in its goal of enabling a "more democratic" consensus solution than standard Proof-of-Stake or Proof-of-Work, however, is a matter of debate is not yet clear.

8. Proof-of-Burn

Whereas Delegated Proof-of-Stake seeks to avoid giving disproportional governance power to wealthy parties by unraveling the direct link between governance participation and the control of resources, Proof-of-Burn, a lesser-known consensus model developed in 2014 ("Slimcoin"), links cryptocurrency wealth explicitly to governance. However, it does so in such a way that individuals or groups wishing to participate actively in governance must surrender some of their wealth in order to do so.

Under the Proof-of-Burn model, nodes seeking to verify data transactions on a blockchain must "burn" cryptocurrency in order to claim that right. To do this, they typically send cryptocurrency to a special recipient node that discards the cryptocurrency permanently. Thus, there is a direct and proportional cost associated with executing governance rights on the blockchain.

Proof-of-Burn is similar to Proof-of-Stake in that both require nodes to possess cryptocurrency on a given blockchain in order to participate in that blockchain's governance process. However, whereas governing nodes in Proof-of-Stake not only keep their cryptocurrency, but earn more cryptocurrency by verifying data transactions, Proof-of-Burn deprives nodes of cryptocurrency the longer they govern.

Further, in order to prevent nodes from gaining an advantage by "buying" governance rights early in a blockchain's history and then enjoying those rights in perpetuity, the Proof-of-Burn architecture continually decreases the governance rights obtained by burning cryptocurrency ("Slimcoin"). As a result, nodes wishing to exercise governance functions must pay constantly for that privilege.

Like Proof-of-Stake and Delegated Proof-of-Stake, Proof-of-Burn offers an ecological advantage as well. Because the "burning" of cryptocurrency does not require the solving of cryptographic puzzles, it consumes negligible amounts of compute resources and electricity.

From a political perspective, the chief innovation of Proof-of-Burn is that it forces nodes to choose between participating in governance and maximizing their accumulation of cryptocurrency. It thus ensures that nodes cannot be excessively wealthy (in terms of cryptocurrency owned) while also exercising disproportionate control over the blockchain.

Placed within the context of modern liberal democracy, Proof-of-Burn may be interpreted as radically egalitarian or radically inegalitarian. In one sense, it is the equivalent of requiring politicians to surrender their personal wealth in order to earn the right govern. On the other hand, because Proof-of-Burn requires nodes to possess cryptocurrency that they can afford to "burn" in order to govern, the strategy could be read as the embodiment of everything that is wrong about liberal-democratic societies in which personal wealth, and the ability to finance one's own political campaigns, are prerequisites for gaining governance powers.

Perhaps because of the ambiguity surrounding the political and social implications of Proof-of-Burn, relatively few blockchains have implemented consensus mechanisms founded upon the Proof-of-Burn concept. Slimcoin, a blockchain and cryptocurrency created in 2014 with a focus on avoiding the environmental sustainability problems of Proof-of-Work, is the notable exception. Slimcoin uses a consensus solution that combines Proof-of-Burn with Proof-of-Stake and Proof-of-Work.

9. Practical Byzantine fault tolerance

The final politically and socially significant blockchain consensus strategy developed to date is the model known as Practical Byzantine Fault Tolerance. This consensus solution predates the introduction of blockchain technology by about a decade (Casto, 2002), and it is based on research by computer scientists on the so-called Byzantine Generals Problem that originated in the 1980s (Lamport, 1982). This problem refers to the difficulty of ensuring that all members of a decentralized network communicate with one another effectively and honestly, even if some of their communications pass through other nodes and therefore run the risk of being manipulated in transit. (The computer scientists who coined the term *Byzantine Generals Problem* likened the challenge to a group of Byzantine generals leading independent armies who needed to coordinate their attack on a city, but who lacked assurance that they could trust each other.)

On a blockchain that uses Practical Byzantine Fault Tolerance consensus, certain nodes are selected to serve as leaders, and leadership status rotates between nodes at random. When one node on the blockchain seeks to record data, it asks the leader node to forward the request to other nodes on the blockchain. These nodes decide,

based on majority consensus, whether to approve or reject the data transaction in question. If the leader fails to forward the request in a timely fashion, a new leader will be chosen. Leadership is not contingent upon solving cryptographic puzzles or owning cryptocurrency.

From a technical perspective, Practical Byzantine Fault Tolerance's main advantages are that, because no complex cryptographic operations are required, transactions can be processed quickly and with minimal expenditure of electricity.

The trade-off for this efficiency is higher susceptibility to attack than other consensus methods. On a Practical Byzantine Fault Tolerance blockchain, only one-third of the nodes on a blockchain need to be malicious in order for consensus to break down, as compared to one-half on blockchains that use Proof-of-Work. Further, Practical Byzantine Fault Tolerance consensus algorithms are susceptible to so-called sybil attacks, in which one node pretends to be multiple nodes in order to increase its influence over decision-making on the network. Sybil attacks can be prevented by incorporating elements of Proof-of-Work into Practical Byzantine Fault Tolerance, but doing so slows transaction throughput. Because of these limitations, Practical Byzantine Fault Tolerance has seen little adoption to date within public blockchains; most use cases for the architecture involve blockchains where membership is not open to the public at large, and where the risk of an attack by malicious nodes is therefore smaller.

Despite its technical shortcomings, Practical Byzantine Fault Tolerance is perhaps the best example of efforts by blockchain communities to innovate within the realm of governance. In several key ways, it diverges sharply from the norms of conventional liberal democracy of the kind with which Fukuyama concerned himself. First, by totally eliminating the connection between material power and the ability to govern, Practical Byzantine Fault Tolerance provides for a fully decentralized and egalitarian network. Second, it empowers – indeed requires – every member of the network to participate in governance as a "leader". It is analogous to classical direct democracy.

Of course, it is worth emphasizing that, as noted above, Practical Byzantine Fault Tolerance was not invented by blockchain enthusiasts. It was the work of academic computer scientists, and has simply been borrowed by blockchain developers as an alternative to other consensus solutions.

10. Conclusion

Given the diversity of consensus strategies within blockchain communities, and their various technical and political limitations, the most obvious lesson to be drawn is that building a completely fair and democratic governance framework within a decentralized community is inherently subjective and perhaps not fully possible. Blockchain has been idealized by some of its proponents as a way to build political and social modes of organization that are fairer than those that exist in non-digital democratic realms; however, the various blockchain consensus protocols developed to date show that fairness and egalitarianism can be elusive even in digital communities that have no central governing authorities.

This does not mean, however, that progressing toward fairer forms of decentralized, democratic consensus is not possible. In many key respects, as I have shown above, some of the newer blockchain consensus solutions, such as Delegated Proof-of-Stake and Practical Byzantine Fault Tolerance, are more genuinely democratic, in

the sense that they mitigate the political advantages conferred by material wealth, than earlier consensus solutions, namely Proof-of-Work.

Moreover, however imperfect existing blockchain consensus solutions may be for enabling truly democratic decision-making, they remain significant for their role in challenging the conventional liberal-democratic order. Nakamoto Proof-of-Work may reproduce in a digital context many of the same offline political and social inequalities that Bitcoin's creator seemed to want to remediate, but this limitation does not erase the fact that Bitcoin aims, at least in spirit, to challenge what its creators saw as deep flaws with the liberal-democratic order. Other consensus solutions arguably go further in demonstrating that more authentically democratic forms of decision-making and social-political organization are possible than those proffered by Fukuyaman liberal democracy.

If the liberal-democratic order eventually collapses, blockchain consensus protocols will probably not be the primary cause. But they are helping to chip away at the political, economic and social norms established at the end of the Cold War. From the perspective of the blockchain ecosystem, it is clear that history has hardly come to an end.

11. References

An Abridged History of Bitcoin. (2013, October 30). Retrieved from https://archive.nytimes.com/www.nytimes.com/interactive/technology/bitcoin-timeline.html

Asolo, B. (2018, November 01). Zcash Algorithm Explained. Retrieved from https://www.mycryptopedia.com/zcash-algorithm-explained/

Beedham, M. (2019, April 21). 4 things that concern Vitalik Buterin about moving Ethereum to Proof-of-Stake. Retrieved from https://thenextweb.com/hardfork/2019/03/28/vitalik-buterin-concerns-ethereum-proof-of-stake/

Biryukov, Alex and Dmitry Khovratovich. Equihash: Asymmetric Proof-of-Work Based on the Generalized Birthday Problem. Ledger Journal 2 (2017)

Bitcoin is NOT a democracy. Retrieved from https://www.reddit.com/r/btc/comments/97axoy/bitcoin_is_not_a_democracy/

Blockchain speeds & the scalability debate. (2018, March 07). Retrieved from https://blocksplain.com/2018/02/28/transaction-speeds/

Canellis, D. (2018, October 23). Report: Cryptocurrency hackers earned $20M with 51-percent attacks in 2018. Retrieved from https://thenextweb.com/hardfork/2018/10/23/cryptocurrency-51-percent-attack

Castro, M. and Liskov, B. (2002). "Practical Byzantine Fault Tolerance and Proactive Recovery". ACM Transactions on Computer Systems

Changelog. Retrieved from https://en.bitcoin.it/wiki/Changelog

Cindx. (2018, September 01). Top-5 largest Bitcoin mining firms in the world. Retrieved from https://medium.com/@cindx/top-5-largest-bitcoin-mining-firms-in-the-world-bb98a1537aad

Fukuyama, Francis. (1989). The End of History? National Interest 16 (Summer 1989), pp. 3-18

Galea, A. (2018, March 30). Bitcoin development: Who can change the core protocol? Retrieved from https://medium.com/@galea/bitcoin-development-who-can-change-the-core-protocol-478b8ac5fe43

Hashrate Distribution. (n.d.). Retrieved from https://www.blockchain.com/en/pools

Hugo, Kristin (2018, October 29). "If Bitcoin Continues to Take So Much Energy, 'It Will Kill the Planet.'" Independent.

Jenks, T. (n.d.). Pros and Cons of the Delegated Proof-of-Stake Consensus Model. Retrieved from https://www.verypossible.com/blog/pros-and-cons-of-the-delegated-proof-of-stake-consensus-model

Kharpal, A. (2018, August 7). Bitcoin market share is at the level it was just after it hit its near-$20,000 record high. Retrieved from https://www.cnbc.com/2018/08/07/bitcoin-market-share-near-level-when-price-hit-record-high.html

Lamport, L., Shostak, R. and Pease, M. The Byzantine Generals Problem. ACM Transactions on Programming Languages and Systems 4 (July 1982), pp.382-401.

Lindsey, B. (2018, November 11). Proof of Stake (PoS): What Is It and How Does It Work? Retrieved from https://blocklr.com/guides/proof-of-stake-pos/

Miah, S. (2019, January 03). Comparison of PoW, PoS And DPoS Governance Models. Retrieved from https://medium.com/@salmanmiah/comparison-of-pow-pos-and-dpos-governance-models-dcea481140f8

Proof of Work is several orders of magnitude better than democracy as a consensus mechanism. Retrieved from https://www.reddit.com/r/btc/comments/9wg6zq/proof_of_work_is_several_orders_of_magnitude/

Slimcoin. A Peer-to-Peer Crypto-Currency with Proof-of-Burn. Retrieved from http://www.doc.ic.ac.uk/~ids/realdotdot/crypto_papers_etc_worth_reading/proof_of_burn/slimcoin_whitepaper.pdf

Study claims Bitcoin uses as much energy as Ireland. Not so fast, experts say. (n.d.). Retrieved from https://www.nbcnews.com/tech/tech-news/study-claims-bitcoin-uses-much-energy-ireland-not-so-fast-n875211

Tharoor, Ishaan. (2017, February 9). "The man who declared the 'end of history' fears for democracy's future". Washington Post.

The Nasgo Decentralized Democracy. (n.d.). Retrieved from https://nasgo.com/launch/the-nasgo-decentralized-democracy/

Vries, Alex de. Bitcoin's Growing Energy Problem. Joule 2 (May 2018), pp. 801-805

What is Delegated Proof of Stake? (n.d.). Retrieved from https://lisk.io/academy/blockchain-basics/how-does-blockchain-work/delegated-proof-of-stake

Why Proof-of-Stake is the Future of Blockchain Technology. (2018, January 19) Retrieved from https://hackernoon.com/why-proof-of-stake-is-the-future-of-blockchain-technology-b1ae997d79a8

Zcash (Equihash) FPGA implementation. (2016, November 16). Retrieved from https://forum.zcashcommunity.com/t/zcash-equihash-fpga-implementation/8509/3