Washington Journal of Law, Technology & Arts

Volume 18 | Issue 4 Article 2

6-11-2023

CONSENSUS'S CONSOLIDATION CONUNDRUM

James J. Bernstein
Georgetown University Law Center

CONSENSUS'S CONSOLIDATION CONUNDRUM

Cover Page Footnote

J.D. Georgetown University Law Center (2024), B.A. Columbia College (2020); My immeasurable gratitude to Professor Christopher Brummer who catalyzed this project. My thanks as well to my friends and classmates Mike Nisper and Connor Reese. These three made this paper possible.

WASHINGTON JOURNAL OF LAW, TECHNOLOGY & ARTS
VOLUME 18, ISSUE 4 — SUMMER 2023

CONSENSUS'S CONSOLIDATION CONUNDRUM

James J. Bernstein[*]

TABLE OF CONTENTS

[*]J.D. Georgetown University Law Center (2024), B.A. Columbia College (2020); My immeasurable gratitude to Professor Christopher Brummer who catalyzed this project. My thanks as well to my friends and classmates Mike Nisper and Connor Reese. These three made this paper possible.

INTRODUCTION

The Merge started on September 6, 2022, just before noon.[1] The mission was clear: take Ethereum, a Web3, blockchain-based network, from one consensus mechanism to another.[2] Within a week, programmers and developers successfully completed the transition.[3] The basis for the switch, contentious though it was among some in the blockchain community,[4] was rooted in a desire to advance the Ethereum network while cognizant of the harm to the environment that travels with widespread use of computing power.[5] The Ethereum Foundation believes that this switch will reduce consumption by nearly 100%, from 112 terawatt-hours per year to 0.01.[6] Additionally, going from a proof of work to a proof of stake validating methodology would solve many of the collective action problems associated with a community-focused network like Ethereum.[7] In particular, proof of stake ensures that validators are "invested" in the worth of their position within the network.[8]

To understand the importance of this decision to switch, consider the foundational backdrop of a blockchain system: to expand the network and ensure the accuracy of all transactions, blockchains require a consensus mechanism with individuals known as validators deciding on whether to add new blocks;[9] these validators can assert their power by either solving a complex math problem ("proof of work")[10] or through a collateral system where one possesses voting power proportional with the amount of money one offers up ("proof of stake").[11] While the former is more "democratic" (after all, anyone can solve the problem),[12] it also requires tremendously more computing power to solve the problems as more computers join the network.[13]

---

[1] *The Ethereum Merge is Finally Here!*, Coinbase (2022), coinbase.com/ethereum-merge.

[2] Arijit Sarkar, *The Merge Brings Down Ethereum Network Power Consumption by 99.9%*, Cointelegraph (Oct. 29, 2022), cointelegraph.com/news/the-merge-brings-down-ethereum-s-network-power-consumption-by-over-99-9.

[3] Sam Kessler, *The Ethereum Merge is Done, Opening New Era for Second-Biggest Blockchain,* Coindesk (Sept. 15, 2022), coindesk.com/tech/2022/09/15/the-ethereum-merge-is-done-did-it-work/.

[4] Nitish Pahwa, *The Merge is Upon Us! Wait, What's the Merge?*, Slate (Sept. 14, 2022), slate.com/technology/2022/09/ethereum-merge-what-to-know.html.

[5] Ezra Kaplan, *Cryptocurrency Goes Green: Could "proof of stake" offer a solution to energy concerns*, NBC News (May 25, 2021), nbcnews.com/tech/tech-news/cryptocurrency-goes-green-proof-stake-offer-solution-energy-concerns-rcna1030.

[6] Zack Hale, *Ethereum's 99% Cut in Energy Use Will Curb Crypto's Climate Footprint*, S&P GLOBAL (Sept. 16, 2022), spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/ethereum-s-99-cut-in-energy-use-will-curb-crypto-s-climate-footprint-72145342.

[7] Olga Kharif and David Pan, *The Ethereum Merge Ups the Stakes - and Reshapes the Crypto Universe,* BLOOMBERG (Sept. 13, 2022), bloomberg.com/news/articles/2022-09-13/what-s-ethereum-eth-merge-proof-of-stake-differs-from-bitcoin-btc.

[8] *Id.*

[9] *Consensus Algorithms in Blockchain*, GEEKSFORGEEKS (June 29, 2022), geeksforgeeks.org/consensus-algorithms-in-blockchain/#:~:text=A%20consensus%20algorithm%20is%20a,state%20of%20the%20distributed%20ledger.

[10] Amanda Reaume, *Proof of Work vs. Proof of State: Explained*, SEEKING ALPHA (June 16, 2022), seekingalpha.com/article/4468656-proof-of-work-vs-proof-of-stake.

[11] Jake Frankenfield, *What Does Proof of Stake (PoS) Mean in Crypto?*, INVESTOPEDIA (Sept. 27, 2022), investopedia.com/terms/p/proof-stake-pos.asp.

[12] Yoan Hermstrüwer, *Blockchain Democracy: Digital Governance in the EU and the US*, STANFORD UNIVERSITY LAW SCHOOL, law.stanford.edu/projects/blockchain-democracy-digital-governance-in-the-eu-and-the-us/.

[13] Mike Antolin, *Proof-of-Work vs. Proof-of-Stake: What's the Difference?*, Coindesk (Nov. 7, 2022), coindesk.com/learn/proof-of-work-vs-proof-of-stake-what-is-the-difference/.

Bitcoin currently uses a proof of work validating procedure which "adjusts the difficulty of the mathematical puzzle depending on the number of miners of the Bitcoin network playing the proof of work game."[14] But all this computer energy is not without cost, especially as more computers join the Bitcoin stratosphere: a chief criticism of blockchains generally is that they will adversely contribute to climate change.[15] Proof of work networks also risk having a high preponderance of disinterested users and can more easily fall victim to a 51% attack, or a majority stakeholder's manipulation of a blockchain network.

Enter proof of stake: though this system favors users with both time and money to validate blocks, it requires significantly less computing power to let the network grow.[16] Therefore, as compared to proof of work, proof of stake "requires much less energy and no specialized equipment…[so] it is considered a more environmentally-friendly alternative to proof of work."[17] Further, because validators risk losing their "staked" cash if a validation goes awry, proof of stake ensures that validators are aimed towards one of the larger ends of the network - namely, scaling the blockchain.[18]

But the proof of stake consensus mechanism is not without critical, if not fatal, drawbacks: indeed, many worry that proof of stake, a consensus mechanism implicitly rooted in financial might, does little to overhaul many of the shortcomings of the current internet.[19] Detractors of this internet ("Web2") are loath to characterize it as anything but a world in which a few companies dominate the many legions of users.[20] Repeating the present version of the internet's dynamics cuts at the heart of Web3. Specifically, blockchain programmers desire to curb, if not stop, the consolidation that characterizes Web2.[21] With any luck, these programmers will instead guide a new internet towards one of potentially several decentralized systems.

To this end, the current conception of proof of stake does nothing to satiate the concerns that Web3 will just be Web2 by a different name.[22] Plainly, proof of stake allows for a system in which wealthy validators can corner large percentages of the market.[23] As a result, these individuals could act as *de facto* gatekeepers of the network as they choose and reject which blocks to validate. Presently, an internet company like Facebook "serves…over a key channel of distribution…[and in] controlling access to markets, [this giant] can pick winners and losers throughout our economy."[24] Proof of stake may result in a similar kind of structure in which only those who can pay to be validators do so - and in turn blockchains oriented around proof of stake would not really improve on some of the centralization criticisms of Web2. Ultimately, future

---

[14] Primavera De Filippi & Aaron Wright, *Blockchain and the Law: The Rule of Code* (2018).
[15] Hermstrüwer, *supra* note 12.
[16] *Proof-of-Stake: Will the Ethereum Merge Really Lead to A Rally?*, FORBES (Sept. 27, 2022), forbes.com/sites/qai/2022/09/27/proof-of-stake-will-the-ethereum-merge-really-lead-to-a-rally/?sh=27b3b60223de.
[17] Miranda Marquit *Proof of Work vs. Proof of Stake: Why the Difference Matters for Ethereum Investors*, TIME (Sept. 16, 2022), time.com/nextadvisor/investing/cryptocurrency/proof-of-work-vs-proof-of-stake/.
[18] CertiK, *The Blockchain Trilemma: Decentralized, Scalable, and Secure?*, MEDIUM(Oct. 4, 2019), medium.com/certik/the-blockchain-trilemma-decentralized-scalable-and-secure-e9d8c41a87b3
[19] Moxie Marlinspike, *My First Impressions of Web3* (Jan 7, 2022), moxie.org/2022/01/07/web3-first-impressions.html.
[20] Chris Dixon (@cdixon), TWITTER(Jan 23, 2022), twitter.com/cdixon/status/1485303920419299331
[21] Rebecca Searles, *Web3 101: A Beginner's Guide*, MEDIUM (Jan. 6, 2022), medium.com/@beccabigwords/web3-101-a5631d244fe4 ("decentralized data puts more power back in the hands of users").
[22] Sarwar Saheed & Hector Marco-Gisbert, *Assessing Blockchain Consensus and Security Mechanisms against the 51% Attack*, APPL. SCI. (2019).
[23] *Id.*
[24] H.R. REP. NO. 47-832, at 6 (2020), judiciary.house.gov/uploadedfiles/competition_in_digital_markets.pdf?utm_campaign=4493-519.

Web3 proof of stake validators may hold significant authority to the point they may pick "winners and losers."

Thus, in order to avoid repeating the consolidation pitfalls of the internet's predecessor forms, it is necessary to change the underlying architecture of a proof of stake system. This piece focuses exclusively on proof of stake because of Ethereum's decision to switch, highlighting a possible trend that other blockchain systems may soon follow suit. Moreover, typical forces for change – namely, laws and the market – fail to adequately regulate blockchain systems. Regardless, proof of stake is preferable given its built-in security and requirement of the commitment of validators. For simplicity, this piece uses Lawrence Lessig's "New Chicago School" theory to orient how the regulation of proof of stake networks may take place. According to Lessig, networks can marshal one of four possible forces to best align incentives or change behavior: laws, norms, the market, or altering the underlying architecture.[25] These four regulatory forces do not represent an exhaustive list; however, these four offer a clear conceptual framework which helps to introduce this piece's proposed change. Indeed, this paper argues that programmers must augment the underlying network architecture by introducing a new, restrictive protocol which increases the price of each successive token a validator can buy. This would make it difficult for even the wealthiest of individuals to possess sizable shares of the voting bloc. Importantly, "proof of stake" itself is an architectural phenomenon. Changing the architecture goes to the heart of the problem directly rather than relying on another force directing the necessary changes. Economic incentives dictate that non-linear costs of tokens will make it both harder to acquire more voting power and also less desirable with highly punitive costs.

To this end, in Part I, this piece will highlight the history, basis, and justifications for blockchain systems over the present version of the internet. This section helps to frame where consensus mechanisms may undermine Web3's core premise. Part II will describe the fundamentals of consensus mechanisms. Thereafter, in Part III this piece will demonstrate the pitfalls of each system - and why proof of stake is not necessarily better at fighting off some of the risks associated with consensus mechanisms. Finally, in Part IV this article offers an architectural solution: introducing a series of new protocols which would increase the cost of each successive token that one purchases to serve as a validator. Ideally, this new architectural shift will undercut some possible risks associated with the present model.

I. THE BASIS FOR BLOCKCHAIN

As the internet has moved from its initial infancy ("Web1") to its present version ("Web2"), it began consolidating around a handful of companies.[26] Users and laypeople know their names: Facebook, Google, Apple, and Amazon to name several examples. These companies dominate the internet of today.[27] This version features applications sitting atop a thin layer of "fat protocols," or the underlying computing architecture which helps drive these applications.[28] In this version, competition is increasingly more difficult because of issues associated with information asymmetry and barriers to entry.[29] This level of central control harms consumers as it allows a few

[25] Lawrence Lessig, *The New Chicago School*, 27 J. OF LEG. STUDIES 661, 662-63 (1998).
[26] CertiK, *supra* note 18.
[27] *Id*.
[28] Joel Monegro, *Fat Protocols*, UNION SQUARE VENTURES (Aug. 8, 2016), www.usv.com/writing/2016/08/fat-protocols/.
[29] *Id*.

companies to drive decision-making, prop up barriers to entry for startups, and control much, if not most, of user's digital data.

To this point, Web3 flips this script: instead of applications commandeering much of the space, it is the computing architecture that has, up to now, sat in the background which will feature more heavily.[30] When these underlying protocols - rather than the applications - dominate, it reduces "the barriers to entry for new players and [creates] a more vibrant and competitive ecosystem of products and services on top."[31] Accordingly, emergent companies which seek to dance with existing players may do so with ease because both kinds of companies "have equal and free access to the underlying data [of] blockchain transactions."[32] As a general matter, Web3 therefore takes power away from the internet companies of old and instead returns it to both users and programmers. This technological maneuver may mean very little to the common user in terms of how, say, he or she views one's social media "feed"; however, giving protocols greater weight actually facilitates easier and freer competition among prospective and present companies. In turn, the most bullish of Web3 programmers believe that "by pooling bandwidth and storage resources…they will gain a leg up on existing online services. Instead of building an online application by renting space from a traditional cloud service…blockchains and these new decentralized protocols may underpin an entirely new Internet architecture."[33]

Generally, what Web3 drives at is a dispersed network in which users dictate decision-making. In order to achieve this, and to add a technological dimension to the framework for Web3, what undergirds this new internet infrastructure is a "decentralized" network known as a blockchain. At its core, the blockchain is a publicly available ledger which records transactions.[34] These transactions can be for tangible goods or even the transfer of intangible things like intellectual property rights. The possible purchase and sale agreements on a blockchain are governed by "smart contracts" - or computer code which "immediately executes all or parts of an agreement and is stored on a blockchain based platform."[35] Much like the overall aims of the blockchain, smart contracts themselves act as a transaction away from intermediaries (like "banks") and they place control with the users of the blockchain.[36]

Furthermore, given that it is public information, the ledger provides users or parties interested in a transaction a freely available summary of who exchanges what. Here, all users may readily be privy to the communications or commercial transactions that occur on the grand thoroughfare of the chain. Consequently, this ledger reduces a significant benefit that the current internet confers to companies: the ability to hoard information. If a ledger is public, it takes away the powerful bargaining chip of data. Unlike the typical corporation which is highly centralized and able to command large swaths of data, the blockchain is politically and architecturally decentralized - but logically centralized.[37] Simply put, the blockchain does not have one person

---

[30] *Id.*
[31] *Id.*
[32] *Id.*
[33] *See supra* note 13, at30-31.
[34] *What is Blockchain Techology?* Ibm, www.ibm.com/topics/what-is-blockchain.
[35] Stuart Levi &Alex B. Lipton, *An Introduction to Smart Contracts and their Potential and Inherent Limitations*, HARVARD LAW SCHOOL FORUM ON CORPORATE GOVERNANCE (May 26, 2018), corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/.
[36] *Id.*
[37] Vitalik Buterin, *The Meaning of Decentralization*, MEDIUM (Feb. 6, 2017), medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274

that controls it, but the system is still able to operate as one whole unit.[38] Thus, users may choose how to assign or manipulate information for their own ends; however, the central ledger provides for universal access.[39] There is no intermediary who grants access to the ledger.

Significantly, the reasoning for a blockchain finds several other justifications. Take the most fundamental basis for broad decentralization: Friedrich Hayek writes that "the economic problem of society is mainly one of rapid adaptation …[thus] the ultimate decisions must be left to the people who are familiar with these circumstances…this problem [cannot] be solved by first communicating all this knowledge to a central board…[it must be solved] by some form of decentralization."[40] Put another way, solutions are best found not through a centralized authority and sent out; rather, they are best communicated inwardly from the outermost layer. The decentralized infrastructure of Web3 seeks to amplify this fundamental principle: it places decision making in many people, empowering those most "familiar" with the issues.

Moreover, blockchains are borne out of a desire to limit entities that typically exert centralized control. It appears to be no accident that Satoshi Nakamoto created Bitcoin, the most popular and widely known cryptocurrency, during the "peak" of distrust of governments and banks because of the Great Recession in 2009.[41] At bottom, blockchains try to act as a replacement - rather than a supplement - to things like fiat currency so as to enable individuals to take power that is ordinarily reserved for central actors and spread control out among more individuals.[42] The corporate dominance of the internet is not immune to these criticisms either: presently, only a few companies control sizable chunks of the internet space and use their respective market dominance to stamp out competition. The vast size of these commercial giants matters significantly as they "[use their] gatekeeper position to maintain [their] market power…and have ultimately bought out, copied, or cut off their competitive threats."[43] Antitrust implications aside, the basis for future blockchain-based networks seeks to avoid this type of corporate capture with a new version of the internet. Independent, then, of whether the target of one's chagrin is a government or corporation, what a decentralized system seeks to achieve is taking the levers of power from one individual and putting them into the hands of many possible users.

Additionally, decentralized networks also have a security dimension which invites their use beyond the political features that Nakamoto and Hayek allude to in their respective writings. Indeed, decentralized systems, compared especially with their centralized counterparts, are delivered with their security infrastructure baked in.[44] These systems protect against widespread failure, collusion, and even attacks. In the words of Vitalkin Buterin, these systems have high levels of "fault tolerance [and] attack resistance [and] collusion resistance."[45] With fault tolerance think of the outcomes of a virus which attacks one computer versus hundreds.[46] While, yes, one facet of a multi-headed network may go down, it need not doom the entire community of users. By contrast, when there is only one, conceivably weakly guarded, node on which the whole system

---

[38] *Id.*
[39] Hermstrüwer, *supra* note 12.
[40] Friedrich A. Hayek, *The Use of Knowledge in Society*, 35 Am. Econ. Rev. 519 (1945)
[41] Wayne Duggan, *The History of Bitcoin, the First Cryptocurrency*, U.S. NEWS (Aug. 31, 2022), money.usnews.com/investing/articles/the-history-of-bitcoin#:~:text=Bitcoin%20was%20created%20in%202009,of%20the%20entire%20cryptocurrency%20market.
[42] *Id.*
[43] *See supra* note 8.
[44] *See supra* note 21.
[45] *Id.*
[46] *Id.*

turns, this virus can knock out large functional chunks quite quickly.[47] As a result, a decentralized network is a relatively safer network insofar as it allows for greater overall security in the face of attacks, both internal and external alike. To this end, decentralized systems increase the costs of undermining the entire network. They are highly immune to attacks in that taking out all the possible computers on the network requires greater amounts of capital. And, just the same, because there are simply so many computers, it makes coordination far harder.[48] So, while decision-making on blockchains is comparatively harder because many individuals must reach a consensus rather than one person, this is something of a goal: decentralized networks aim at a more democratic structure to both secure the network and provide some appeal.

All told, blockchain's appeal comes from the fact that one may achieve similar ends on a decentralized network as one would on its centralized counterparts - just without cumbersome intermediaries. Not only is the system more resistant to attacks of various sorts, blockchains also - best of all! - spread authority out among the users on the network. This kind of decentralization allows those that are most familiar with the transactions, i.e. the users themselves, to dictate decision-making without sacrificing any of the kinds of transactions that may occur in the presence of a central authority.

II. CONSENSUS MECHANISMS

In order to continue expanding the decentralized system, it may be seemingly necessary to include some form of centralization. Simply, how can a network which functions on many users continue to expand and add new blocks to the chain of the network? Even the Merge seemed to include some elements of centralization to corral user support.[49] In fact, the answer to this problem comes in the form of an aptly named pseudo-democratic process called "consensus."[50] Broadly speaking, consensus is the process by which the blockchain is capable of reporting transactions as "true," or that the transaction actually took place.[51] Since no one party controls the public ledger, consensus ensures that each add-on to the blockchain records something that actually happened. If someone purchases a car using bitcoin or ethereum, users themselves on the network verify the resulting smart contract. Consensus is an essential element in both the function of the blockchain as well as the more intangible political aims of Web3 decentralization. The aspirations – and even bases – for seeking to fundamentally change the internet's structure require diffuse centers of control which reach a common goal. In short, consensus is the direct means by which a new internet may develop as well as a critical component in the overall mission of Web3 to disperse authority online.

Consensus, to date, takes two different forms: "proof of work" and "proof of stake." These two are worthy of independent exploration. Proof of work comes in the form of broad, uninhibited competition. This is, importantly, the validating system that Bitcoin currently uses. Nakamoto's brainchild "makes it difficult to add information to the blockchain" because "Bitcoin protocol establishes a strict procedure for adding new blocks to the shared database, and all blocks are

---

[47] *Id.*
[48] *Id.*
[49] Best Owie, *Ethereum Merge Puts Spotlight on Potential Centralization Issues*, BITCOINIST (Sept. 2022), bitcoinist.com/ethereum-merge-puts-spotlight-on-potential-centralization-issues/.
[50] Brooke Becher, *What is A Consensus Mechanism?*, BuiltIn (Mar. 23, 2023), builtin.com/blockchain/consensus-mechanism
[51] *Id.*

verified to ensure that they contain valid transactions and a valid hash."[52] The basics of this validating process are that "cryptocurrency miners compete against each other to solve complex problems using high-powered computers. Those first to do so are given the authority to add the new block of transactions and then rewarded with digital currency for their work. When a block is authenticated, it's added to the *blockchain*."[53] The system privileges something akin to a perfect equality among miners in that no one individual is favored from the outset relative to the others - it relies solely on who can solve a problem first. However, this system also requires those with access to the computing power necessary to "compete" to join the game.

Incidentally, "[this] blockchain is less environmentally friendly than other systems" because of the use of energy-consuming computers that are required to solve these equations.[54] The reason for this is found in the fact that the equation is proportionally difficult to the amount of computers that could solve the problem.[55] So, as more computers join the network, the problem is harder to solve, which increases the amount of energy these computers consume. This is due to the fact that the incentives of this system are such that individuals will try to acquire the best possible computing power to solve these mathematical mysteries - which drains environmental resources.[56] At present, the energy these computers consume is concerning enough - this is to say nothing of what a highly scaled, widely-used version of the blockchain may look like wherein many millions of computers go online.[57] In this way, the mass adoption of a proof of work framed blockchain accelerates the depletion of finite natural resources.

But, climate change is not alone among the issues that proof of work presents. Of note, three other immediate problems come to the fore: (1) the ability of a proof of work network to exacerbate centralization problems; (2) proof of work may have too many disinterested validators; and, (3) there are security risks associated with proof of work. For the first, since those with the most resources can acquire these kinds of computers, "a small number of mining pools control the blockchain [which is functionally like] de-facto centralization."[58] Therefore, while proof of work offers an ostensibly decentralized system in that all are nominally allowed to participate, in reality only those with access to the kinds of computers required to solve these equations are capable of participating.

And, concerningly, proof of work does nothing to quell issues related to validator involvement. The blockchain turns on validators not only acting in the best interest of the network, it mandates that validators act to enable its expansion. But proof of work plays no favorites as to who gets the token necessary to act as a validator. Instead, all computers have, at least theoretically speaking, the same odds of solving the equation necessary to receive a token. Even those with the least interest in acquiring one may have the chance to act as a validator. Simply put, proof of work risks giving individuals with the least interest in the blockchain a stake just because he or she

---

[52] *See* Antolin, *supra* note 13.
[53] *See* Coinbase, *supra* note 1.
[54] *See* Kessler, *supra* note 3.
[55] *See* Antolin, *supra* note 13.
[56] Paul Kim, *What are the environmental impacts of cryptocurrency?* BUSINESS INSIDER (Mar. 17, 2022), businessinsider.com/personal-finance/cryptocurrency-environmental-impact
[57] *Fact Sheet: Climate and Energy Implications of Crypto-Assets in the United States*, THE WHITE HOUSE (Sept. 8, 2022), whitehouse.gov/ostp/news-updates/2022/09/08/fact-sheet-climate-and-energy-implications-of-crypto-assets-in-the-united-states/ ("The United States currently hosts the world's largest Bitcoin mining industry, totaling more than 38% of global Bitcoin activity, up from 3.5% in 2020. Despite the potential for rapid growth, future electricity demand from crypto-asset operations is uncertain, demonstrating the need for better data to understand and monitor electricity usage from crypto-assets.").
[58] *See supra* note 3

"mined" the right solution.[59] This can result in a collective action problem of sorts in that proof of work risks having validators with no real commitment to the ideals of the blockchain, especially as fewer coins come available.[60] If too many disinterested individuals came to possess validating authority, the blockchain's gestational progress could insurmountably stall.

Finally, another problem arises in the security of proof of stake networks – or lack thereof. Consider the following issue which typically arises with proof of work: the so-called Sybil attack.[61] The name of this maneuver comes from a story of a woman of the same name who could assume multiple personalities.[62] The principle of multiple individual identities is borrowed on the blockchain: here, one individual uses aliases to control multiple computers which solve the aforementioned equations.[63] As these computers slowly aggregate more validating power, this actor is able to control more individual authority on the network. If the process is ultimately successful, it can result in a 51% attack.[64] With this, one individual would be able to dictate the validation process by themselves. By controlling a majority of the voting power, one person could out-vote the "honest" nodes on the network.[65] Accordingly, this individual could "override the consensus mechanism of the network." In turn, one user having 51% of the consensus power could also allow them to "modify" transactions or, in the most extreme case, stop mining altogether ("mining monopoly").[66] The possibility for a network to fall victim to a Sybil attack is one of the general fears associated with proof of work: presently there is no security system that wholly prevents this kind of attack. Proof of work's central technical failing is that it is susceptible to both internal and external threats. Alternative consensus mechanisms are therefore worth considering.

As an alternative, proof of stake does away with many of the shortcomings associated with proof of work. Here, "blocks are verified using the machines of coin owners, so there doesn't need to be as much computational work done."[67] Instead, in this version of consensus, individuals offer up collateral as a way of validating blocks. This helps to solve the security issues related to proof of work because validators offer cash as individuals. Therefore, it is harder to assume multiple personalities. But that's not all: this system also tries to overcome the collective action problems associated with proof of work because those who are acting as validators offer their own money as a statement of their interest in the maintenance of the system. Plainly, "if a validator adds an inaccurate block, they lose some of their staked crypto."[68] There are real consequences, then, for not adhering to the role of validators. This aims at solving the issue of validator involvement. On this point, too, the consequences for a mis-validated block help to promote blockchain security on proof of stake networks. Finally, and critically, proof of stake's main achievement comes in the form of overcoming some of the environmental concerns associated with mining.[69] Take Ethereum's switch: in going from a proof of work to a proof of stake model, "the Ethereum

---

[59] Jesus Rodriguez, *Proof of Work or Proof of Stake? How About Both?*, MEDIUM (May 3, 2018), medium.com/coinmonks/proof-of-work-or-proof-of-stake-how-about-both-27ff19b73f51.
[60] Toby Hazlewood, *Proof-of-Stake versus Proof-of-Work Blockchains*, LEVEL UP CODING (Mar. 23, 2021) levelup.gitconnected.com/proof-of-stake-versus-proof-of-work-blockchains-c0dc1b2bc43f.
[61] *Sybil Attacks Explained*, BINANCE ACADEMY, academy.binance.com/en/articles/sybil-attacks-explained.
[62] *Id.*
[63] *Id.*
[64] *51% Attack*, BINANCE ACADEMY, academy.binance.com/en/glossary/51-percent-attack.
[65] *Id.*
[66] *Id.*
[67] *See supra* note 2.
[68] *See supra* note 4.
[69] Vitalik Buterin, *Why Proof of Stake* (Nov. 6, 2020), vitalik.ca/general/2020/11/06/pos2020.html.

Foundation has claimed that the transition reduced Ethereum's energy consumption by 99.95%."[70] This switch was not for naught, or at least not without real positive developments in a practical sense. On balance, then, proof of stake offers solutions to four principal problems as compared with a proof of work network.

III. SHORTCOMINGS OF STAKING

However, proof of stake can lead to a more naked kind of centralization. Indeed, "[in] staking a large portion of wealth consistently, *a participant becomes a powerful entity within the network and also able to influence the well-being of the network*." (emphasis added).[71] This should not be the case, though. Again, proof of stake offers a supposed solution to many of the central failings of proof of work – including those around consolidation. Take the 51% attack: supposedly, incentives are such that the "most affluent users [are] unlikely to perform the [51%] attack."[72] The argument goes some like this: because affluent users would not *want* to undermine the network, they have contributed capital to, these wealthy validators will act in the best interest of the network lest they lose their collateral. Whoever may claim coin-based voting power in a proof of stake network does not want to lose their collateral.[73] This forces honest voting, i.e. the fear of losing collateral is a powerful enough force to counteract against a bad actor's vote.[74] As a result, the network itself seems to have tools which prevent a malicious majority from even attempting to mis-validate blocks.

But, this proves to be specious analysis. For one, validators may still benefit from a 51% attack using a technique known as short-selling.[75] More fundamentally, this argument does not acknowledge that validators can control portions of the network *and* promote its existence. It is not a zero-sum game: wealthy individuals may "stake" large portions of the network without dooming the whole system. After all, this is more or less what the present version of the internet looks like. A handful of companies "vote" to promote and maintain their individual power among the commercial giants.[76] It would not be functionally indistinguishable to have a handful of individuals control all the future validating power - like a Boggis, Bunce, and Bean of cryptocurrency[77] - as compared with a handful of companies controlling the movement of capital on the internet today. Given that Web2 doesn't have any one company possessing a 51% ownership right now does not mean it represents the kind of broad participation and democratic structure that Web3 seeks to achieve. More to the point, just a few companies possessing a 51% ownership may operate as if only one owns that much.

This is the paradox, then, of having wealth dictate which users may act as validators: while they may not try to have a majority of the voting power, having only a few wealthy validators

---

[70] *See supra* note 4.
[71] *See* Hale, *supra* note 6.
[72] *Understanding a 51% Attack on the Blockchain*, Section.io (Dec. 15, 2021), section.io/engineering-education/understanding-the-51-attack-on-blockchain/#:~:text=To%20avoid%20the%20risk%20of,unlikely%20to%20perform%20the%20attack.
[73] *Id.*
[74] *Id.*
[75] Suhyeon Lee & Seungjoo Kim, *Short Selling Attack: A Self-Destructive but Profitable 51% Attack on PoS Blockchains*, eprint.iacr.org/2020/019.pdf.
[76] *Federal Trade Commission v. Facebook, Inc.*, No. 20-3590 (2021), ftc.gov/system/files/documents/cases/073_2021.06.28_mtd_order_memo.pdf ("Facebook…[leveraged] its power to foreclose and forestall the rise of new competitors").
[77] Roald Dahl, *Fantastic Mr. Fox* (1974)

undermines the goal of near-perfect decentralization. While Vitalik Buterin writes that "it is much harder for participants in decentralized systems to collude to act in ways that benefit them at the expense of other participants" unlike how "the leaderships of corporations and governments collude in ways that benefit themselves" that should not imply that it is impossible.[78] Designing a network infrastructure that privileges wealth when it comes to general decision making resembles many of the criticisms of Web2 centralization like creating *de facto* barriers to entry in the form of access to capital.

Such is the story with much of Web3 in its present version.[79] Proof of stake does not help bring Web3 back to the path of a decentralized orbit. Because proof of stake allows for individuals to scramble in perpetuity as they try to collect more and more validating tokens, Web3 may be destined to repeat many of Web2's shortcomings.[80] In brief, the present version of the proof of stake system, not entirely unlike the proof of work consensus model, still risks control by the few at the expense of the many.[81] Coincidentally, a year prior to the Merge, Buterin wrote about the possibility of coin-voting undercutting decentralization infrastructure.[82] With the coin-voting that comes with any kind of consensus mechanism, "small groups of wealthy participants are better at successfully executing decisions than large groups of small-holders…[because] each small-holder has only an insignificant influence on the outcome."[83] It should come as no surprise, then, that individuals seek to acquire more voting power in order to exert greater influence by executing particular decisions.

Thus, proof of stake's benefits arrive clad in the proverbial sheep's clothing: while this system makes it significantly more difficult to make decisions by one individual (it is incredibly costly, for one), proof of stake still provides for the possibility of a great degree of centralization.[84] Ethereum, principal catalyst of the proof of stake transition, is failing to distinguish itself from Web2. History seems to be repeating itself as "ethereum [has] been built with many of the same implicit trappings as web1. To make these technologies usable, the space is consolidating around… platforms. Again."[85] So, while all users on the network exist in a state of initial equality, some users (the validators and even corporations who seek to take advantage of the current cache of buying into blockchains) have the opportunity and motive to control greater slices of the network.

In short order, tokens will likely accumulate with the few individuals who can afford them. Given that the environmental, security, and participation concerns associated with proof of work appear very real,[86] proof of stake offers the clearest, cleanest path towards a Web3 future. Of the two choices, proof of stake provides a legitimate chance to catalyze a shift towards

---

[78] *See supra* note 21.
[79] Tomio Geron &Benjamin Pimental, *OpenSea puts Web's Decentralized Nature to the Test*, PROTOCOL (Jan. 7, 2022), protocol.com/newsletters/protocol-fintech/opensea-nft-frozen?rebelltitem=1#rebelltitem1 ("Web3 may be decentralized in theory, but not in practice. OpenSea, [for example], has run away with the NFT market, commanding an estimated 97% share. [Similarly,] Coinbase had more than half of the bitcoin trading market.").
[80] Bryan Daugherty, *Proof-of-Stake Is Proof of Misunderstanding*, COINDESK (Sept. 22, 2022), coingeek.com/proof-of-stake-is-proof-of-misunderstanding/.
[81] *Id.*
[82] Vitalik Buterin, *Moving Beyond Coin Voting Governance* (Aug. 16, 2021), vitalik.ca/general/2021/08/16/voting3.html
[83] *Id.*
[84] Stacy Elliot, *Has Proof of Stake Made Ethereum More Centralized?*, Decrypt (Oct. 9, 2022), decrypt.co/111485/has-proof-of-stake-made-ethereum-more-centralized
[85] *See supra* note 10
[86] Duggan, *supra* note 41

decentralization. But, without any changes to the consensus mechanism, the new internet just may not be that different from the one that exists now.

IV. ARCHITECTUAL CHANGE

Criticisms aside, this Article does not seek to paint an entirely bleak picture of the future of Web3 in general nor the use of a proof of stake consensus mechanism in particular. But it is necessary to implement some important changes to the underlying architecture of proof of stake to ensure that Web3 does not enhance the substantial inequalities found on Web2. While proof of stake is not *all* of Web3, consensus mechanisms drive so much of the development seen on this new internet that the two are inextricably linked. After all, consensus undergirds the allegedly decentralized power structure of Web3. Moreover, changing proof of stake's architecture is preferable to changing, say, proof of work's architecture, considering the fact that the latter provides for a greater number of disinterested users. This is not to say that there are no disinterested users on a proof of stake network. There is, however, a greater number on a proof of work network. Independent of consolidation concerns, proof of stake's advantages are fundamental: this consensus mechanism better handles the issue of the apathetic validator and other shortcomings found on proof of work networks.

For the purposes of this conversation, this piece borrows from Lawrence Lessig's "New Chicago School" theory.[87] At the center of this theory is a dot, which represents any regulated entity.[88] Four forces influence and constrain it: laws, norms, the market, and the architecture.[89] (The diagram also helps explain why this theory is called the "Pathetic Dot" model too.[90]) Lessig concedes that these forces "do not regulate the same way."[91] Indeed, it is for precisely this reason that this Article identifies architecture as the agent for change: the independent forces that the three other engines may apply is simply too weak to overcome the compromised consensus mechanisms of Web3.

Take laws, for example: statutory initiatives fail to adequately regulate quick-changing industries. Plainly, the blockchain is difficult to regulate.[92] Regulating end-users, for example, is "burdensome and time-consuming."[93] But, even more so, laws regulate "after the fact": they develop in response to events that have already happened.[94] Highly dynamic industries are particularly difficult to regulate. Laws generally help regulate "stable" industries unlike the fast-paced technology world.[95] Given the changing nature of the blockchain, laws may too frequently lag behind whatever the consensus mechanism *du jour* is. Existing laws do not adequately capture the complexities of relatively stable corporations, let alone proof of stake. Moreover, the structure of the blockchain networks themselves struggle to fit within an ordinary legal framework.[96]

---

[87] Lessig, *supra* note 24
[88] *Id.*
[89] *Id.*
[90] *Id.*
[91] *Id.*
[92] Primavera, *supra* note 13
[93] *Id.*
[94] Lessig, *supra* note 24
[95] Tom Wheeler, Phil Verveer, & Gene Kimmelman, *The Need for Regulation of Big Tech Beyond Antitrust,* Brookings Institution (Sept. 23, 2020), brookings.edu/blog/techtank/2020/09/23/the-need-for-regulation-of-big-tech-beyond-antitrust/
[96] Nathan Fulmer, *Exploring the Legal Issues of Blockchain Applications*, 52 Akron L. Rev. 1 (2019) at 182. ("The law surrounding cryptocurrencies will undergo rigorous testing and interpreting as new fact scenarios are analyzed.

Typical concentration measurements like the Herfindahl-Hirschman Index (HHI) already fail to capture some of the intrinsic issues related to current businesses[97], and blockchain companies are no ordinary business.[98] Proof of stake networks would not situate well within maybe even otherwise helpful measures of consolidation. This Article does not argue that *no* legal remedy suffices to counteract the adverse consequences of a proof of stake consensus mechanism. But it does acknowledge that no present legal intervention is sufficient.

Second, norms are similarly unhelpful in turning Web3's proof of stake away from past versions of the internet. Central to Web3 is a common goal of designing an enterprise in the blockchain that helps to completely decentralize authority.[99] These norms help to drive dispersed and diverse groups of programmers towards this common goal.[100] Slowly but surely, though, without guardrails these norms are subject to change. Controlling validators may even be capable of stamping out dissent irrespective of differing or developing norms.[101] Putting aside the fact that proof of stake may similarly create a network in which validators are "more equal than others,"[102] changes to the norms of a community may transpire which cut at its ideals. Norms are by their nature fickle and subject to change.[103] Relying on norms to affect change assumes they will not tack towards more moderate positions, including a willingness to grant more power to a central authority through proof of stake.[104] Hoping for norms to remain true may be a quixotic fantasy for it does nothing to permanently prevent consolidation by proof of stake.

Third, the market no doubt plays a critical role in helping to direct proof of stake. But market forces do not assuage concerns related to proof of stake. The market can help diminish the

---

However, courts have little experience with the newest blockchain capability: smart contracting."); *see also* Michael Kades and Fiona Scott Morton, *Interoperability as a Competition Remedy for Digital Networks*, Washington Center for Equitable Growth (Sept. 2020equitablegrowth.org/wp-content/uploads/2020/09/092320-WP-Interoperability-as-a-competition-remedy-for-digital-networks-Kades-and-Scott-Morton.pdf ("Digital markets, however, also pose challenges for antitrust enforcement. They combine economies of scale, economies of scope, and network effects."

[97] William A. Galston and Clara Hendrickson, *A Policy at Peace with Itself: Antitrust Remedies for our Concentrated, Uncompetitive Economy*, Brookings Institution (Jan. 5, 2018), brookings.edu/research/a-policy-at-peace-with-itself-antitrust-remedies-for-our-concentrated-uncompetitive-economy/ ("The problem may not lie in documented HHI levels failing to breach the point at which antitrust scrutiny is triggered, but in a threshold insufficiently concerned with the threat posed by concentration levels below those identified by current agency guidelines.")

[98] Wulf A. Kaal, *Blockchain-Based Corporate Governance*, Stan. J. Blockchain L. & Pol'y (Jan. 4, 2021), stanford-jblp.pubpub.org/pub/blockchain-corporate-governance/release/1 ("Blockchain-based corporate governance offers dynamic regulatory features that are partially incompatible with the rule-based traditional legal environment with which traditional limited liability entities are required to comply.")

[99] *See* Primavera, *supra* note 32.

[100] *Id*.

[101] Maria Konnikova, *How Norms Change*, The New Yorker (Oct 11, 2017), newyorker.com/science/maria-konnikova/how-norms-change ("The voice of authority speaks not for the one but for the many; authority figures have a strong and rapid effect on social norms in part because they change our assumptions about what other people think.")

[102] George Orwell, *Animal Farm* (1945)

[103] Milenko Martinovich, *Changing behaviors may be easier when people see norms changing, Stanford research finds*, Stanford News Service (Oct. 6, 2017), news.stanford.edu/press-releases/2017/10/06/change-behaviorserception-normal/

[104] As an example of a fringe representative of what is actually a more moderate voting bloc, consider the typical libertarian voter with a platform or candidates who espouse ideals like protecting citizens from a government that will instruct them on how to "make toast in your own damn toaster." *See Political scientist finds disconnect in Libertarian Party platform, voters*, University of Dayton (May 1, 2020), udayton.edu/news/articles/2020/05/libertarian_party.php; *See also A License to Make Toast in Your Own Damn Toaster*, C-Span (May, 29, 2016), c-span.org/video/?c4713898/user-clip-licence-make-toast-damn-toaster

power that some gain through proof of stake through increased competition.[105] Presently it is too costly to participate in the proof of stake system.[106] Proof of stake privileges the ability to spend on tokens to serve as a validator. This is an option only for those with both the time and the financial resources to spend disposable cash on tokens. As a result, those who actually compete for voting influence turn out to be the wealthiest among the users. This is not to say that the market is for naught; rather, just like laws, it does not address underlying inequality *vis à vis* proof of stake.

Therefore, in hopes of regulating Web3's proof of stake consensus mechanism away from its present trendline, the network's architecture is the most useful both by default but also for the reasons set forth here. According to Lessig, "architecture" is a synonym for "nature" - that is, it is "the world as [we] find it."[107] As an example, Lessig shows that changing the "architecture" of a "cigarette" would alter its addictive quality.[108] Much the same, Web3 may change the "nature" of how proof of stake operates. Unlike norms, architecture has more staying power; and unlike laws and the market, it frees these decentralized systems from outside actors attempting to either retrofit inadequate frameworks or not overcoming some of the underlying causes for the change respectively. In order to achieve this, it will require a programming initiative that models the Merge as it will require many of the users to help catalyze this change. The Merge shows that a fundamental change to the "nature" of a blockchain system is possible.[109]

This new architectural system will work as follows: a proof of stake network introduces a new protocol that doubles the cost of successive validating tokens. Like the Merge, this would require programmers to unite to ensure that this modification of the coin-cost system would take root in the underlying architecture of the network. And, also like the Merge, it would require two protocols: one to prepare the network to change how staking may work and one to complete the change.[110] Significantly, bitcoin's proof of work system also offers a useful guide: the mathematical problems that users solve to validate blocks increases with difficulty as more users join.[111] The same may be true with the purchase of tokens in this revised version of proof of stake. The current system on Ethereum works by allowing individuals to purchase tokens to act as validators at uniform costs.[112] This reduces barriers to acquiring more tokens because the cost of

---

[105] Today, one ether costs north of $1,500 dollars - or nearly $50,000 to buy one validating stake. *See* ethereum.org/en/get-eth/

[106] Mason Marcobello, *Top Questions About Proof-of-Stake and Staking Answered*, COINDESK (Aug. 19, 2022) ("A common argument amongst proponents of proof-of-work is that proof-of-stake favors the rich and reduces the rewards for those with less ether.").

[107] Lessig, *supra* note 24.

[108] *Id.*

[109] Sam Kessler and Sage D. Young, *Ethereum Merge: What You Need to Know*, COINDESK (Sept. 7, 2022) coindesk.com/tech/2022/09/07/ethereum-merge-what-you-need-to-know/ ("If the Merge succeeds, it will represent a massive feat of engineering and human coordination.").

[110] COINBASE, *supra* note 1 ("The Merge actually happens in a two-step process, which have been named the Bellatrix & Paris upgrades. The Merge was officially kicked off by Bellatrix, which took place on Sept 6th 2022 at 11:34:47am UTC. Bellatrix is a network upgrade on the consensus layer. Bellatrix will be followed up by Paris, which will be the execution layer that will transition Ethereum from proof-of-work to proof-of-stake.); *see also Ethereum's Bellatrix & Paris Upgrades to Bring ETH Merge Home*, CYBAVO (Sept. 6, 2022), cybavo.com/blog/eth-merge-bellatrix-paris-upgrades/ ("The next big item on the agenda for the Ethereum developers is the Bellatrix upgrade. In this update, the Beacon Chain will be readied for the Merge.").

[111] Primavera, *supra* note 14.

[112] *See Staking with Ethereum*, ethereum.org/en/staking/.

each is the same per unit.[113] But think of the alternative: one validating token presently costs thirty-two ether (Ethereum's currency) whereas the cost to purchase a second token could be twice the cost of the first. In this scenario, the total cost to purchase these two tokens is ninety-six ether rather than sixty-four.[114] The cost of this cryptocurrency is distinct from the cost of purchasing it on the market for it serves the sole purpose of acting as a validator.[115] (On Ethereum, validators stake capital that is beholden to a smart contract. This capital can exist separately from the network.[116])

Borrowing from proof of work's constructions and encouraged by the Merge's protocol developments, proof of stake networks may change their architecture to "tax" a growing voting bloc. While consolidation remains a concern, to be sure, this proposed architecture helps to slow down consolidation concerns because it would be increasingly too expensive to play a nefarious game on the network. Most of all, this sort of modest change to the network's architecture does not reduce the benefits of proof of stake. For one, this change does not harm the network's internal security, nor does it cut at involvement or scalability. This is because this change does not foreclose active – but perhaps limited – involvement from more validators. In other words, changing the architecture of a proof of stake network retains the benefits while addressing the potential harms that an unfettered network may levy upon users.

CONCLUSION

Supreme Court Justice Louis Brandeis said, "We can have a democracy…or we can have great wealth concentrated in the hands of the few, but we can't have both."[117] The same tradeoff appears true on Web3: the networks on the blockchain may exist in a state of more equal, democratic rule or risk a few companies capturing much of the interface. Regrettably, proof of stake, in its present form, drags the blockchain towards the latter. Though this consensus mechanism overcomes many of the environmental concerns, risk of falling victim to a 51% attack, and issues related to validator involvement compared with proof of work, proof of stake in its current form leaves much to be desired. Basic concerns over consolidation undermine many of the gains that proof of stake offers. But they do not need to. Changes to the underlying architecture of proof of stake - namely, increasing the cost of successive validating tokens - can ensure that blockchains remain closer to their participatory goals. Unlike laws, norms, and the market, an architectural change can nip issues associated with consolidation and proof of stake in the bud. An

---

[113] Patrick Collins, *Eth 2.0 Staking - How to stake for all levels*, Medium (Dec. 11, 2020), medium.com/coinmonks/eth-2-0-staking-how-to-stake-for-all-levels-77e6440cd39a ("You can stake multiples of 32.").

[114] As a practical example of how these increased costs may operate, it may look similar to the luxury tax threshold in Major League Baseball. As with this tax, scaling the cost of currency like this is not a "hard cap" - that is, it's not as if it's impossible to continue acquiring more validating tokens - but the cost is so punitive that few cross the threshold if ever. The purported purpose of the luxury tax in Major Baseball is at least two-fold but, of particular note, it is designed to "discourage" owners from crossing these financial ceilings. *See* Will Calandra, *The MLB Has a Competitive Balance Issue, and it's Related to Money and Payroll Inequalities*, Georgetown Voice (Feb. 18, 2020), https://georgetownvoice.com/2020/02/18/the-mlb-has-a-competitive-balance-issue-and-its-related-to-money-and-payroll-inequalities/.

[115] *See What is Solo Staking?*, Ethereum, ethereum.org/en/staking/solo/ (explaining that the 32 ether is used to "activate a validator, giving [users] the ability to participate in network consensus."); *see also* Marcobello, *supra* note 110 (explaining that staking ether serves the sole purpose of acting as a validator.).

[116] *See Staking with Ethereum*, *supra* note 112.

[117] Irving Dilliard, *Mr. Justice Brandeis: Great American*, at 42-45 (1941).

architectural overhaul is not a panacea, but this modest change may lead to untold benefits for the promotion of a new internet.