IEEE ICBC'24 1570981760

How does Stake distribution influence Consensus? Analyzing Blockchain Decentralization

***Abstract*—In the PoS blockchain landscape, the challenge of achieving full decentralization is often hindered by a disproportionate concentration of staked tokens among a few validators. This study analyses this challenge by first formalizing decentralization metrics for weighted consensus mechanisms. An empirical analysis across ten permissionless blockchains uncovers significant weight concentration among validators, underscoring the need for an equitable approach. To counter this, we introduce the Square Root Stake Weight (SRSW) model, which effectively recalibrates staking weight distribution. Our examination of the SRSW model demonstrates notable improvements in the decentralization metrics: the Gini index improves by 37.16% on average, while Nakamoto coefficients for liveness and safety see mean enhancements of 101.04% and 80.09%, respectively. This research is a pivotal step toward a more fair and equitable distribution of staking weight, advancing the decentralization in blockchain consensus mechanisms.**

***Index Terms*—decentralization, consensus mechanisms, blockchains**

I. Introduction

Bitcoin shaped the field of blockchains by introducing a peer-to-peer system that operates without trusted intermediaries [70]. Its vision encapsulates the essence of *decentralization*, characterized by the elimination of single points of failure and the facilitation of collective decision-making. Our work focuses on exploring decentralization in blockchains, particularly in their consensus mechanisms. These mechanisms are critical as they establish agreement on the content and order of transactions among validators.

The problem this paper addresses is the *analysis and advancement of decentralization in consensus mechanisms*. This problem is particularly interesting because, although decentralization is fundamental to every blockchain, standardized metrics to quantify it within consensus are lacking. This gap, coupled with the technical complexity of consensus algorithms, complicates the analysis of blockchain systems in practice. Moreover, enhancing decentralization in consensus mechanisms is of significance, as it directly contributes to the trust and safety in blockchain systems.

Our approach to examining decentralization begins with a systematic classification of consensus mechanisms based on finality, as detailed in Section II. In this paper, we specifically focus on classical consensus mechanisms, leveraging their extensive research in distributed computing [16], [49]. Subsequently, we delve into the concept of weighted consensus wherein validators could have unequal influence in consensus, a framework highly relevant in Proof of Stake (PoS) and Delegated Proof of Stake (DPoS) systems. In these systems, the weighting is a function of the tokens staked by validators (or stakers) [14], [24], [76].

Drawing inspiration from quantitative decentralization metrics in decentralized autonomous organizations (DAOs) with token-based voting [8], [78], [86], our work extends these studies to consensus mechanisms in Section III. We adapt and refine these metrics to effectively measure decentralization in consensus mechanisms. Specifically, we evaluate cardinality, Gini index, and Nakamoto coefficients for safety and liveness for given set of validators.

Utilizing metrics specifically designed for evaluating decentralization in consensus mechanisms, our research carries out an empirical analysis of ten prominent blockchains, as elaborated in Section IV. This analysis encompasses Aptos [7], Axelar [9], BNB [20], Celestia [17], Celo [18], Cosmos [22], Injective [42], Osmosis [72], Polygon [74], and Sui [85]. The findings reveal a notable concentration of weight among few validators, which poses significant concerns for the security and integrity of blockchain systems. To address this challenge, we propose *the square root stake weight (SRSW)* function, outlined in Section V. Unlike solutions such as the introduction of virtual stake [63], our approach leverages existing staked tokens while redefining their weights, thereby avoiding the introduction of new security vulnerabilities. Our proposed approach, thoroughly evaluated in Section VI, demonstrates substantial potential in enhancing decentralization and, consequently, the overall reliability of blockchain systems. The paper concludes with a discussion of related work in Section VII, and identifies avenues for future research in Section VIII.

Our contributions are four-fold:

1) Adapt and formalize decentralization metrics specifically for consensus mechanisms.
2) We empirically demonstrate the challenge of weight concentration and its impact on decentralization in prominent blockchains.
3) We introduce the square root stake weight (SRSW) mechanism, to mitigate weight concentration challenge.
4) Our work pioneers the use of data-driven analysis in consensus research, offering novel insights and solutions to enhance decentralization in blockchain systems.

II. Consensus Mechanism Foundations and Classification

This section delineates the consensus mechanisms and validator set selection process, setting the stage for the empirical analysis of decentralization in blockchains.

TABLE I: Consensus mechanisms classified based on finality

	Classical consensus	Nakamoto-style
Finality	Absolute and instant	Probabilistic and eventual
Priniciple	Safety over liveness	Liveness over safety
Attestation	Quorum of validators	Only the proposer
Resources	Requires a priori knowledge	No constraints
Communication	Supports partial synchrony	Synchronous
Examples	PBFT [16], HotStuff [93], Tendermint [14], [15]	Nakamoto [70], Ouroborus [24]
In practise	Diem [10]	Bitcoin [70]

A. Classification of Consensus Mechanisms Based on Finality

A blockchain comprises a ledger that has blocks of transactions. The consensus mechanism orchestrates the process of reaching agreement on the content and order of blocks within the ledger [95]. Agreement is reached among a designated set of validators, which in different nomenclatures can be referred to as miners [70], witnesses [52], or sequencers [66]. A consensus mechanism is deemed Byzantine Fault Tolerant (BFT) if it withstands a certain proportion of validators with malicious behaviour, in addition to crash failures [49].

Two properties are guaranteed by consensus mechanisms: *safety*, ensuring all correct validators agree on the same content and order of blocks, and *liveness*, ensuring the continual production of new blocks without indefinite delays [35], [73]. Building upon the safety property, we introduce the concept of finality, also known as commitment. Finality of a block b at time t, denoted $0 \leq f(b,t) \leq 1$, indicates the probability with which the block has been appended to the ledger [6]. When $f(b,t) = 1$, it signifies *total finality*, i.e., the block b cannot be reverted or abandoned. Achieving this level of finality is essential for the immutability of the ledger. There are two distinct ways to realize finality in consensus mechanisms:

Definition II.1. ***Absolute Finality*** *is achieved when a block b is appended to the ledger at time t_0 and becomes irreversible instantly, such that $f(b,t) = 1 \quad$ for all $t > t_0$.*

Definition II.2. ***Probabilistic Finality*** *is achieved when the finality of an appended block b at time t_0 is expressed as $f(b,t_0) = 1 - \gamma$, where γ is a non-negative value less than 1 (i.e., $0 \leq \gamma < 1$) that represents the deviation from total finality. Specifically, for any two points in time t_1 and t_2 such that $t_2 > t_1$, it follows that $f(b,t_1) < f(b,t_2)$. As time progresses, $f(b,t)$ gradually converges to 1 as γ approaches zero.*

$$\lim_{\gamma \to 0} f(b,t) = 1 \tag{1}$$

Based on how consensus mechanisms achieve finality, they can be categorized into two types: Nakamoto-style and classical consensus, as shown in Table I.

The Nakamoto-style consensus embodies probabilistic finality, meaning that the system eventually approaches total finality with time [46]. This style is used in Bitcoin, where a block is considered to have reached finality after the confirmation of 6 subsequent blocks, approximately an hour [70]. Nakamoto-style consensus mechanisms prioritize liveness over safety, ensuring the continual production of new blocks; however, the ledger's order remains susceptible to forking [35], i.e., the current order of the ledger may be altered, until time t.

Conversely, classical consensus mechanisms prioritize safety over liveness. In this style, no blocks are appended to the ledger until absolute finality is achieved, rendering finality deterministic and immediate [46]. An example is the PBFT consensus [16], where a designated proposer, one of the validators, broadcasts a block and, absolute finality is achieved when a quorum of validators attests on the proposed block and the block is appended to the ledger.

A notable distinction between these styles also lies in the block generation process. In Nakamoto-style consensus, a single proposer is responsible for proposing a block. This design doesn't presuppose knowledge of resources, such as the hash power in PoW, and assumes synchronous communication, i.e., messages are broadcast within a bounded time [51]. On the other hand, classical consensus protocols assume a priori knowledge of the total available resources [14], such as the stake distribution of validators in PoS. The notion of a quorum $\mathbb{Q}$, facilitated through certificates of attestation, necessitates having finite resources, a topic explored further in the subsequent subsection.

For the scope of this work, our focus is classical consensus mechanisms for multiple reasons. Primarily, these mechanisms facilitate fast finality along with high performance in terms of throughput and latency, compared to Nakamoto-style consensus [14], [93]. Secondly, the employment of quorum $\mathbb{Q}$ certificates enables these protocols to function effectively in a partially synchronous environment, thereby tolerating indefinite periods of asynchrony [51]. Thirdly, classical consensus mechanisms have undergone rigorous examination over several decades [95], with seminal contributions such as Raft [71] and PBFT [16], finding applications in safety-critical domains such as aviation systems [79], [90].

In the subsequent sections, the discussion extends to Sybil resistance and the intricacies of weighted classical consensus.

B. Transition to Weighted Consensus

Traditional classical consensus mechanisms, such as PBFT [16], HotStuff [93], PrestigeBFT [96], and SBFT [40], are designed to be able to tolerate up to one-third of the validator set being faulty, where a faulty validator may exhibit malicious behavior or be offline. In these mechanisms, a designated block proposer is required to collect attestations from the validator set to form a quorum certificate. Let the validator set be represented as $N = \{n_1, n_2, \ldots, n_m\}$ where n_i represents a validator. A quorum certificate is formed with attestations from at least a super-majority of validators, denoted as $\mathbb{Q}$, such that:

$$\mathbb{Q} \geq \left(\frac{2}{3}\right) m, \text{ where } m = |N| \tag{2}$$

Note that while we assume the protocol can be able to tolerate up to one-third of the total validators being faulty, some

protocols may have different failure assumptions [62]. In such cases, $\mathbb{Q}$ must be adjusted accordingly.

Classical BFT consensus mechanisms were initially conceived for permissioned systems, where the identities of all validators are established. When deployed in permissionless environments with (pseudo)anonymous identities, these mechanisms become susceptible to Sybil attacks, wherein a malicious actor could create multiple validators to subvert the consensus process [31]. To mitigate this vulnerability and achieve Sybil resistance without relying on trusted intermediaries, Algorand [37], Ouroboros [24] and Tendermint [14] pioneered PoS mechanism. In PoS, validators stake the native tokens of the system as a means of establishing their identity. These tokens are subject to penalization if validators engage in malicious behavior [67]. Given that the native tokens are finite and the security of the consensus impacts the tokens' market value, validators are rationally incentivized to act correctly, thus enhancing the system's security. The development of PoS protocols, characterized by variably staked tokens, paves the way for the adoption of weighted consensus.

Weighted consensus encompasses traditional classical consensus as a subset, where traditional models are effectively a special instance with uniform weights across validators. In weighted consensus, validators have varying weights in the consensus process [94]. In practice, in PoS/DPoS blockchains such as Cosmos [14], the influence of a validator n_k in the consensus is quantified by their weight, $w_k > 0$, which is a function of their staked tokens s_k.

$$w_k = s_k \tag{3}$$

Unlike traditional classical consensus mechanisms where a quorum ceritifcate is achieved based on the absolute number of validators, in weighted consensus, a quorum necessitates garnering two-thirds of the total weight. The quorum certificate for weighted consensus for a validator set N is denoted as $\mathbb{Q}'$, is given below:

$$\mathbb{Q}' \geq \left(\frac{2}{3}\right) \sum_k w_k \quad \forall k \in N \tag{4}$$

Moreover, higher weight could also imply higher rewards or a higher probability of being selected as a block proposer [24]. The evolution from traditional to weighted consensus, underscored by PoS/DPoS, is a pivotal adaptation to suit permissionless blockchain systems. We focus on weighted consensus in the rest of this work.

C. Validator Set Selection

Classical weighted consensus assumes that resources, such as total staked tokens in PoS, are finite and known a priori. These staked tokens are used to rank candidates interested in becoming validators and to choose the validator set. Various mechanisms exist for validator set selection, including PoS [37], DPoS [76], delay towers [68], and reputation mechanisms [25]. This work does not make specific assumptions regarding the mechanism of validator set selection; instead, it focuses on the validators' engagement in the consensus mechanism.

The validator set typically remains fixed for a specified time interval, known as an *epoch*. Following each epoch, a new validator set is selected through a *reconfiguration* event [33], [68]. Reconfiguration tends to consider updated stakes and involves eliminating faulty validators.

It is also important to acknowledge that some blockchains, such as Algorand [37], use mechanisms like random sortation to randomly select a subset of candidates as validators every epoch. Our study focuses on systems where the validator set is deterministically defined, thereby excluding blockchains that employ random committee selection processes.

III. Consensus Decentralization Metrics

In consensus mechanisms, *decentralization* means reaching agreement on the contents and order of transactions without centralized control, ensuring that no single validator or group of validators dominates the process. While challenging to precisely define [44], [77], [78], decentralization is essential for consensus mechanisms, as it underpins trust in the blockchain systems.

Our discussion draws inspiration from the (m, ε, δ)-decentralization model described in "Impossibility of Full Decentralization in Permissionless Blockchains" [48]. Here, m indicates the cardinality of the validator set, and ε represents the weight disparity between the most influential (richest) and the δ-th percentile validator. The ideal case is full decentralization, expressed as $(m, 0, 0)$ for a sufficiently large m, that occurs when all validators have equal influence. While the (m, ε, δ)-model captures the essence of decentralization, it lacks quantifiable metrics for comparing the decentralization of different blockchains. Therefore, we introduce additional metrics, as shown in Table II, to effectively quantify and compare decentralization across different blockchains.

*1) **Validator Set Cardinality** (m):*

Description: Represents the number of validators ($m = |N|$) in the consensus mechanism.

Inference: A higher m suggests better decentralization, aligning with the (m, ε, δ)-model.

Limitations: In weighted consensus, m alone may not reflect true decentralization. For example, if $m = 1000$ but one validator holds 90% of the total weight, it contradicts the decentralization ideal.

*2) **Gini Coefficient** (G):*

Description: The Gini coefficient (G) measures wealth inequality, commonly used in socioeconomic studies [19], [38], [80]. In consensus mechanisms, it assesses validators' influence disparity, indicating deviation from $(m, 0, 0)$-decentralization.

G is calculated using the Lorenz curve, which graphically elucidates the weight distribution among validators [36]. The Lorenz curve plots the cumulative share of validators (sorted by their weight) on the X-axis against the cumulative share of their weight on the Y-axis. The formula for G is:

$$G = 1 - \frac{2 \times B}{A + B} \tag{5}$$

TABLE II: Decentralization metrics for consensus

Symbol	Metric	Range	Ideal
m	Validator set cardinality	$m > 0$	higher
G	Gini Index	$0 \leq G \leq 1$	lower
$\mathbb{N}_L, \rho_{\mathbb{N}_L}$	Nakamoto Coefficient for Liveness	$\mathbb{N}_L \geq 0$ $0 \leq \rho_{\mathbb{N}_L} \leq 1$	higher
$\mathbb{N}_S, \rho_{\mathbb{N}_S}$	Nakamoto Coefficient for Safety	$\mathbb{N}_S \geq 0$ $0 \leq \rho_{\mathbb{N}_S} \leq 1$	higher

where B is the area between the Line of Equality and the Lorenz Curve, and A is the area beneath the Lorenz Curve. The line of equality illustrates a hypothetical scenario of equal weight distribution, while the Lorenz curve depicts the actual distribution of weights [81]. The area between these two curves represents the extent of inequality in the weight distribution [36].

Inference: G ranges between 0 and 1, with 0 indicating equitable distribution (higher decentralization) and values closer to 1 indicating concentration of weight (lower decentralization).

Limitations: G alone may not fully capture decentralization, as it does not account for validator set cardinality m. For example, a system with a single validator ($m = 1$) would have $G = 0$, yet be highly centralized.

*3) **Nakamoto Coefficient - Liveness** ($\mathbb{N}_L, \rho_{\mathbb{N}_L}$):*

Description: The Nakamoto coefficient for liveness ($\mathbb{N}_L, \rho_{\mathbb{N}_L}$) quantifies the minimum number of validators needed to disrupt the block production or censor transactions [32], [84], [88]. In other words, $\mathbb{N}_L$ indicates the fault tolerance in weighted consensus, i.e., cardinality of the smallest subset of validators (L) whose cummulative weight is at least one-third of the total weight. The formula is:

$$\mathbb{N}_L = \min\{|L| \,|\, L \subseteq N, \sum_{i \in L} w_i \geq \frac{1}{3} \sum_{i=1}^{m} w_i\} \tag{6}$$

The normalized Nakamoto coefficient $\rho_{\mathbb{N}_L}$ is then calculated as:

$$\rho_{\mathbb{N}_L} = \frac{\mathbb{N}_L}{m} \tag{7}$$

This normalization facilitates comparison across blockchains of varying sizes. Unlike the (m, ε, δ)-decentralization model, which focuses on the richest validator, $\rho_{\mathbb{N}_L}$ considers the weight distribution across the top one-third of validators relative to the entire set, offering a broader view of the system's decentralization.

Inference: A higher $\mathbb{N}_L$ suggests better decentralization. The normalized value $\rho_{\mathbb{N}_L}$, ranging between 0 and 1. A $\rho_{\mathbb{N}_L}$ closer to 1 indicates high decentralization and resilience against censorship [32].

Limitations: $\mathbb{N}_L$ relies on correct majority of validators. Any collusion among validators may distort $\mathbb{N}_L$, rendering it an inaccurate measure of decentralization.

*4) **Nakamoto Coefficient - Safety** ($\mathbb{N}_S, \rho_{\mathbb{N}_S}$):*

Description: Safety relies on finality—ensuring once blocks are appended, they become immutable. Safety compromises have severe consequences on the ledger's integrity, such as ledger re-ordering or loss of funds [54], [83]. The Nakamoto Coefficient for Safety ($\mathbb{N}_S, \rho_{\mathbb{N}_S}$) quantifies the minimum subset of the validators (S) required to compromise safety [73], [84], i.e., $\mathbb{N}_S$ is the cardinality of the smallest subset of validator set whose combined weight can form a quorum $\mathbb{Q}'$:

$$\mathbb{N}_S = \min\{|S| \,|\, S \subseteq N, \sum_{i \in S} w_i \geq \mathbb{Q}'\} \tag{8}$$

The normalized form of $\mathbb{N}_S$, denoted by $\rho_{\mathbb{N}_S}$, is:

$$\rho_{\mathbb{N}_S} = \frac{\mathbb{N}_S}{m} \tag{9}$$

In conjunction with ($\mathbb{N}_L, \rho_{\mathbb{N}_L}$), the ($\mathbb{N}_S, \rho_{\mathbb{N}_S}$) metric complements the (m, ε, δ)-decentralization framework by quantifying the concentration of weight that affects system safety.

Inference: Higher values of $\mathbb{N}_S$ and $\rho_{\mathbb{N}_S}$ indicate a more decentralized system. Specifically, $\rho_{\mathbb{N}_S}$ close to 1, especially in systems with a large validator set (m), signifies robust decentralization.

Limitations: The assumption that validators in $\mathbb{N}_S$ calculations are non-colluding may not reflect real-world scenarios, potentially limiting its accuracy for safety evaluation. Moreover, reducing a system's safety to a single metric like $\mathbb{N}_S$ risks oversimplifying safety complexities [89].

5) Summary: In this section, we introduced various metrics to quantify decentralization in consensus mechanisms. Despite the limitations acknowledged, the synergy of these metrics holistically captures the essence of decentralization, aligning with the (m, ε, δ)-decentralization model. We leverage these metrics to quantify the decentralization of existing blockchain systems in practice in the subsequent section.

IV. Empirical Data Analysis

A. Scope and Methodology of Data Collection

In our study, we focus on permissionless blockchains that use classical consensus mechanisms, particularly those with weighted consensus as outlined in Section II. We limit our analysis to blockchains with deterministic validator set selection methods, such as PoS and DPoS. Notably, all the blockchains examined in this study employ DPoS for Sybil attack resistance.

For our empirical analysis, we selected ten blockchains, as shown in Table III, namely: Aptos, Axelar, BNB (Binance), Celestia, Celo, Cosmos, Injective, Osmosis, Polygon, and Sui. These protocols are based on BullShark [82], HotStuff [93], IstanbulBFT [64], and Tendermint [14] consensus mechanisms. These blockchains were chosen for their diverse applications, including smart contracts Layer-1 (L1) blockchains, interoperability protocols [11], Layer-2 (L2) scaling solutions [59], data availability protocols [5], and decentralized exchanges [50], ensuring the wide applicability of our findings. Our sample comprises blockchains with at least 300 million USD market capitalization, cumulatively amounting to a market capitalization of 60 billion USD as of December 14, 2023 [1].

TABLE III: Decentralization metrics for blockchains, as of 14 December 2023

	Application	**Consensus Mechanism**	m	G	$\rho_{\mathbb{N}_L}(\mathbb{N}_L)$	$\rho_{\mathbb{N}_S}(\mathbb{N}_S)$	ε **in** $(m, \varepsilon, 0)$	$(m, \varepsilon, 50)$
Aptos	L1 blockchain [7]	HotStuff/DiemBFT [26]	144	0.56	12.50 (18)	12.50 (38)	8.488454e+11	7.63
Axelar	Interoperability [9]	Tendermint [39]	75	0.41	13.33 (10)	37.33 (28)	7.796480e+03	5.01
BNB (Binance)	L1 blockchain [20]	Tendermint [21]	57	0.55	14.04 (8)	28.07 (16)	1.595114e+05	8.41
Celestia	Data availability [17]	Tendermint [27]	174	0.83	2.87 (5)	8.62 (15)	3.836768e+10	88.86
Celo	L2* (L1 blockchain) [18]	IstanbulBFT [28]	84	0.40	11.90 (10)	39.29 (33)	1.293101e+10	3.90
Cosmos	L1/interoperability [22]	Tendermint [87]	180	0.69	3.89 (7)	13.33 (24)	2.470500e+02	60.63
Injective	DeFi/interoperability [42]	Tendermint [4]	60	0.49	8.33 (5)	30.00 (18)	3.158000e+01	8.08
Osmosis	DeFi/DEX [72]	Tendermint [29]	150	0.54	6.67 (10)	28 (42)	1.080500e+02	14.52
Polygon	L2/ZK-rollup [74]	Tendermint [91]	105	0.78	3.81 (4)	10.48 (11)	3.629552e+08	69.53
Sui	L1 blockchain [85]	Narwhal/BullShark [30]	106	0.41	13.21 (14)	33.02 (35)	9.290000e+00	6.37

Data collection was automated via scripts interfacing with the blockchains' RPC endpoints to fetch active validator sets and their staked tokens. Daily snapshots were taken to account for epoch changes and the data was systematically archived in a public GitHub repository[1] to facilitate transparency and accessibility for ongoing and subsequent analyses.

B. Data Analysis

In Table III, we present the decentralization metrics for ten blockchains, derived from the validator set data snapshot on 14 December 2023. To validate the reliability of our analysis, we continuously monitored over the prior month, confirming the absence of significant deviations in the observed trends.

Upon examining the validator set cardinality (m), we note a range of 57 to 180 validators across the analysed blockchains. However, a concerning trend emerges when we consider the Nakamoto coefficients for liveness ($\mathbb{N}_L$) and safety ($\mathbb{N}_S$), which are notably low, varying from 4 to 18 and 11 to 42, respectively. This disparity implies potential vulnerabilities. For example, in the case of Polygon, merely the top 4 validators could censor an application [88], furthermore, the top 11 validators might collude to alter the ledger. Despite a high number of validators, the proportion that could compromise system liveness ($\rho_{\mathbb{N}_L}$) and safety ($\rho_{\mathbb{N}_S}$) remains worryingly small, spanning only 2.87% to 14.04% and 8.62% to 39.29%, respectively. This observation leads us to an open challenge to bolster both the liveness and safety of blockchain systems, utilizing the available validators.

Challenge 1:

Given a validator set with cardinality (m), how can we enhance the Nakamoto coefficients ($\rho_{\mathbb{N}_L}, \rho_{\mathbb{N}_S}$)?

An examination of the Gini coefficient (G) in Table III, ranging from 0.40 to 0.83, reveals a significant concentration of weight. This is indicative of a disproportionate stake distribution among a small subset of validators. The implications of this concentration are further underscored by the values of ε in the (m, ε, δ)-decentralization model. Both at $\delta = 0$ and $\delta = 50$, the ε values substantially deviate from the ideal zero value needed for $(m, 0, 0)$, i.e., full decentralization. This observation leads us to our second critical challenge in the pursuit of enhancing blockchain decentralization.

Challenge 2:

How can we achieve a more equitable weight distribution (G) among validators?

A simplistic approach to addressing these challenges might be to adopt a one-validator one-vote system with equal weight for all validators, complemented by a minimum stake threshold for participation. However, this approach shows limitations in practice in blockchains such as Ethereum. With the requirement of only 32 ETH for validator eligibility, Ethereum's network consists of over 800,000+ validators [45]. This high number necessitates random selection for consensus participation, impacting performance metrics such as time to finality. A more significant concern is operational centralization, exemplified by Lido controlling approximately 32.7% of all validators [65], effectively making the Nakamoto coefficient for liveness valued at one ($\mathbb{N}_L = 1$). Therefore, the problem lies in mitigating the risk of Sybil identities to achieve genuine decentralization, captured in the folowing challenge.

Challenge 3:

How to discourage the creation of multiple Sybil identities?

V. Advancing Decentralization: Finite SRSW Quorums

In this section, we address the identified challenges. We begin by defining primitives needed for our proposed solution. This is followed by the introduction of the SRSW (Square Root Stake Weighted) quorum.

A. Primitives and Assumptions

Validator Rewards: Validators are incentivized with rewards for their participation in the consensus mechanism. We assume validators are rational and want to maximize their rewards.

At the end of every epoch, each correct validator $n_k \in N$ receives a reward, denoted as r_{n_k}. The reward is calculated based on the system parameter α, representing the inflation

[1] masked for double-blind review

factor that determines the rate of reward distribution. The reward for each validator is given by the equation:

$$r_{n_k} = \alpha w_k, \quad \text{where} \quad \alpha > 0. \tag{10}$$

If a correct validator holds s_k native tokens at the start of an epoch, their balance of native tokens after that epoch would increase to $s_k + r_{n_k}$.

Sybil Cost: We introduce a Sybil Cost, denoted as $C > 0$, to represent the additional expenses incurred by a validator operator when choosing to run multiple validator nodes instead of one. These expenses could include operational costs, such as computational resources or the amount of staked tokens required. We assume that C is sufficiently high, thereby providing resistance against Sybil attacks.

Limit Validator Set Cardinality: We propose an upper limit for the validator set cardinality M, ensuring $m \leq M$. To implement this in practice, the validator candidates are sorted based on their staked tokens, and we select the top M candidates for the validator set, i.e., the threshold staked tokens to become a validator is the stake of the Mth validator candidate, represented by s_M. Accordingly, the rewards for a validator candidate n_k with s_k staked tokens for an epoch is as follows:

$$r_{n_k} = \begin{cases} \alpha w_k & \text{if } s_k > s_M, \\ 0 & \text{if } s_k \leq s_M. \end{cases} \tag{11}$$

Capping the validator set cardinality is justified for two reasons. Firstly, in line with classical consensus mechanisms, an increase in the number of validators tends to decrease the system scalability, measured in throughput and latency [93]. Secondly, by imposing a maximum limit on the number of validators, and a minimum capital requirement of s_M staked tokens for running a validator, the system discourages single entities from dominating the validator set, a point further explored in the following section.

This method, implemented in blockchains such as Axelar [39] and Celo [28], helps in balancing scalability and decentralization.

B. SRSW Function

Building on these primitives, we now focus on the challenge of achieving equitable influence among validators to improve the Nakamoto and Gini coefficients for a given validator set.

We propose the *Square Root Stake Weight (SRSW)* function, a novel approach that diverges from traditional linear weightings in quorum $\mathbb{Q}'$ computations. The SRSW function calculates the weight w_i^* of each validator n_i based on the square root of their staked tokens s_i, as defined by:

$$w_i^* = \sqrt{s_i} \tag{12}$$

The revised quorum $\mathbb{Q}^*$ for the validator set N is formulated as follows:

$$\mathbb{Q}^* \geq \left(\frac{2}{3}\right) \sum_i w_i^* = \left(\frac{2}{3}\right) \sum_i \sqrt{s_i} \quad \forall i \in N \tag{13}$$

Contrasting with linear models, the SRSW function aims to reduce the disproportionate influence of validators with high staked tokens. In essence, the SRSW approach diminishes the weight disparities between validators with varying stake amounts.

The validator rewards $r_{n_i}^*$ are structured to reinforce rational decisions. The reward formula is:

$$r_{n_i}^* = \alpha w_i^* = \alpha \sqrt{s_i}, \text{ if } s_i > s_M; \text{ otherwise, } 0. \tag{14}$$

This incentivizes validators to keep or increase their stakes above the threshold s_M, aligning individual gains with the system's stability. In other words, the system should satisfy the following condition.

$$r_{n_i}^* > r_{n_j}^* + r_{n_k}^* - C, \text{ where } s_i \geq s_j + s_k \tag{15}$$

This inequality implies that a validator with a combined stake s_i gains more rewards by maintaining a single identity rather than dividing into multiple validators with smaller stakes s_j and s_k.

Consider a validator with $s_i = 4$ and $s_M = 3$. The options are: split into $s_j^1 = 2, s_k^1 = 2$, or $s_j^2 = 3, s_k^2 = 1$, or not split. In the first case, $s_j^1, s_k^1 < s_M$ yield no rewards. In the second, rewards are $\alpha\sqrt{3}$ for s_j^2 only, as $s_k^2 < s_M$. Not splitting, $\alpha\sqrt{4}$, offers the highest reward. Our approach effectively deters stake fragmentation and mitigates Sybil attacks, promoting consolidated stakes as a strategically rational choice.

When both s_i and s_j exceed s_M, the inequality is adjusted in terms of weights:

$$\sqrt{s_i} > \sqrt{s_j} + \sqrt{s_k} - \frac{C}{\alpha}, \text{ where } s_i \geq s_j + s_k \text{ and } s_i, s_j > s_M \tag{16}$$

Here, our assumption of high C plays a crucial role to make the division of validator stakes non-rational, which we explore in the subsequent section.

C. Discussion

Determining M. A critical aspect of this approach is the determination of M, the maximum cardinality of the validator set. A low M might risk insufficient decentralization, while an excessively high M could impact system performance due to increased communication complexity. Although a fixed M may appear counterintuitive to decentralization, delegation in DPoS mechanisms enable individual token holders to collectively participate in consensus, thereby mitigating potential centralization concerns [76]. In this work, we do not prescribe a specific value for M, as it depends on the algorithm and implementation. In practice, we have observed around one hundred validators is the ideal number for current algorithms [2], [93].

Sybil costs. We assume that C is high. In practice, this remains an open challenge, particularly in token-based systems [60], [61]. Potential solutions include the use of proof of personhood [12], [92], limiting one validator per geospatial location [69], KYC compliance [41], or a combination of these. While these approaches might mitigate the problem to some degree, they may come at the cost of lost anonymity. Furthermore, detecting cartels among validators is challenging, especially at the protocol layer; therefore, we do not address this issue in the consensus mechanism. In conclusion, we

acknowledge that establishing Sybil costs is more a complex socio-economic challenge than a technical one and is beyond the scope of this work.

In summary, we propose the SRSW function with corresponding $\mathbb{Q}'$ and r^*, and provide considerations on M and C. We now turn our attention to evaluating this approach.

VI. Evaluation: Improved Decentralization

In this section, we demonstrate that the SRSW function achieves higher decentralization, as measured by $G, \rho_{\mathbb{N}_L}$, and $\rho_{\mathbb{N}_S}$, compared to the linear model. We then reinforce these claims with empirical evidence.

A. Decentralization Metrics Analysis

Let us analyze how the SRSW model offers a better Nakamoto coefficient than the linear model.

Theorem 1. *Given a validator set N, the SRSW model's Nakamoto coefficient for liveness, $\rho^*_{\mathbb{N}_L}$, is greater than or equal to that of the linear stake-weight model, $\rho_{\mathbb{N}_L}$.*

Proof. Consider the Nakamoto coefficient computation in linear stake weight, let K be the smallest subset such that:

$$\sum_{n_i \in K} s_i > \frac{1}{3} \sum_{n_i \in N} s_i \tag{17}$$

Similary in the SRSW model, let K^* be the smallest subset satisfying the condition:

$$\sum_{i \in K^*} \sqrt{s_i} > \frac{1}{3} \sum_{i \in N} \sqrt{s_i} \tag{18}$$

The concave nature of the square root function, as per Jensen's inequality [3], necessitates a larger K^* to fulfill this condition in the SRSW model compared to K in the linear model, thereby implying:

$$|K^*| \geq |K| \implies N^*_L \geq N_L \tag{19}$$

$$\frac{N^*_L}{m} \geq \frac{N_L}{m} \implies \rho^*_{\mathbb{N}_L} > \rho_{\mathbb{N}_L} \tag{20}$$

Hence, the relative Nakamoto coefficient for liveness is higher for SRSW compared to linear model. □

Similarly, we can prove for Nakamoto coefficient-safety.

Theorem 2. *Given N, the SRSW model's Nakamoto coefficient for safety is greater than or equal to that of the linear stake-weight model.*

Theorem 3. *Given N, the Gini indices of the SRSW and linear models, represented by G^* and G, respectively, satisfy $G^* \leq G$.*

Proof. This proof draws upon the established principles from Theorem 1 and the definitions provided in Section III.

In the SRSW model, the square root transformation applied to validator stakes results in a more uniform distribution of weights, effectively reducing relative disparities in stake sizes compared to the linear model. Consequently, this leads to a lower Gini index in the SRSW model, compared to the Gini index in the linear model.

TABLE IV: Percentage decrease in Gini and percentage increase in Nakamoto coefficients with SRSW

	G **% decrease**	$\mathbb{N}_L$**% increase**	$\mathbb{N}_S$**% increase**
Aptos	26.78	33.33	34.21
Axelar	39.02	60.0	32.14
Binance	25.45	25	25
Celestia	22.89	140	140
Celo	35	80	27.27
Cosmos	45.58	200	195.83
Injective	48.97	120	66.66
Osmosis	46.29	170	61.90
Polygon	32.05	125	163.63
Sui	48.78	57.14	54.28
mean	**37.16**	**101.04**	**80.09**

Therefore, $G^* \leq G$, indicating a more equitable distribution of validator influence under the SRSW model. □

B. Empirical Validation

In this subsection, we use the validator set data outlined in Section IV to recalculate weights as per SRSW function. We then compare decentralization metrics of the SRSW model against the linear stake weight model for specified validator sets.

1) Key Findings:

- **Improvement in Gini Index:** With SRSW function, G observed a decrease ranging from 22.89% to 48.97%, as shown in Figure 2a and Table IV. This reduction indicates a more equitable distribution of weight, enhancing the decentralization.
- **Increase in Nakamoto Coefficients:** As observed in Figure 1, the Nakamoto coefficients for SRSW are superior to the current approach. In terms of absolute numbers, as shown in Table IV, $\mathbb{N}_L$ saw an increase between 25% and 200%, while $\mathbb{N}_S$ had the increment range from 25% to 195.83%. These increases imply a stronger resistance to centralization by SRSW, requiring higher number of validators to influence the consensus.

2) Implications:

- **Rewards - Rate of Growth:** In Figure 2b, we analyze the growth rate of rewards using two annual inflation rates ($\alpha = 4.5, 9.1$), chosen based on typical values observed in current blockchain implementations [75]. This analysis underscores the benefits of the SRSW model, particularly in moderating the reward growth for validators with larger stakes. By addressing the 'rich get richer' narrative, the SRSW model promotes a fairer reward distribution, leading to more equitable weight compounding across epochs.
- **Block Generation Decentralization:** Figure 2c explores the dynamics of block proposal generation. Utilizing data from the Aptos blockchain [26], we initially demonstrate how the current block proposers are chosen based on

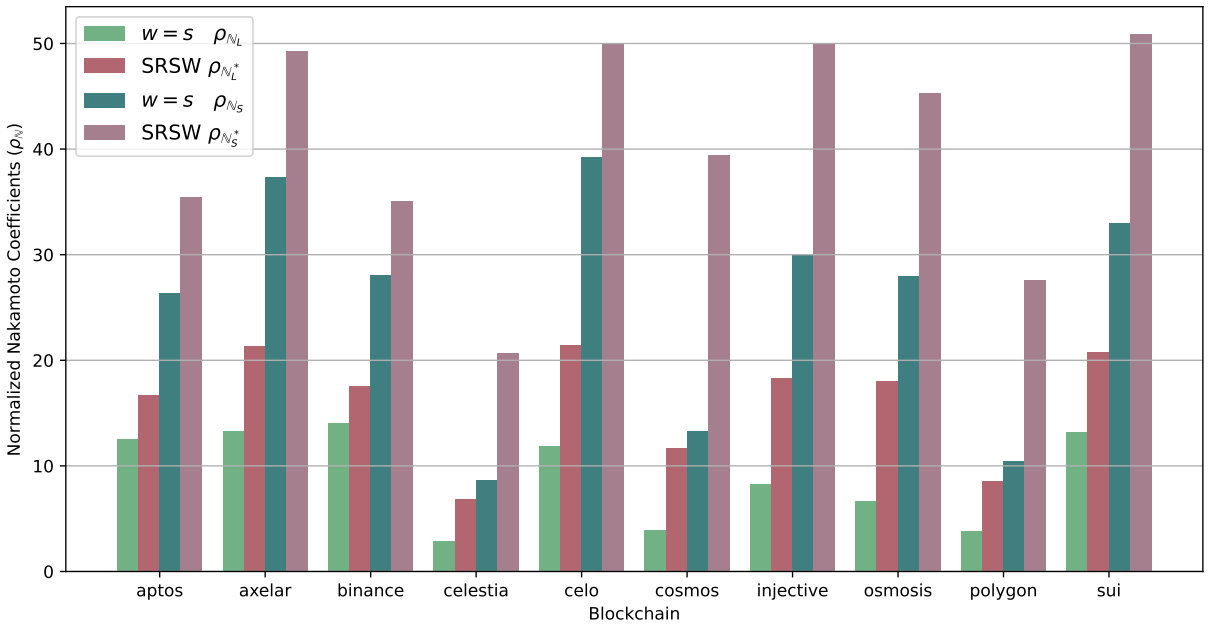
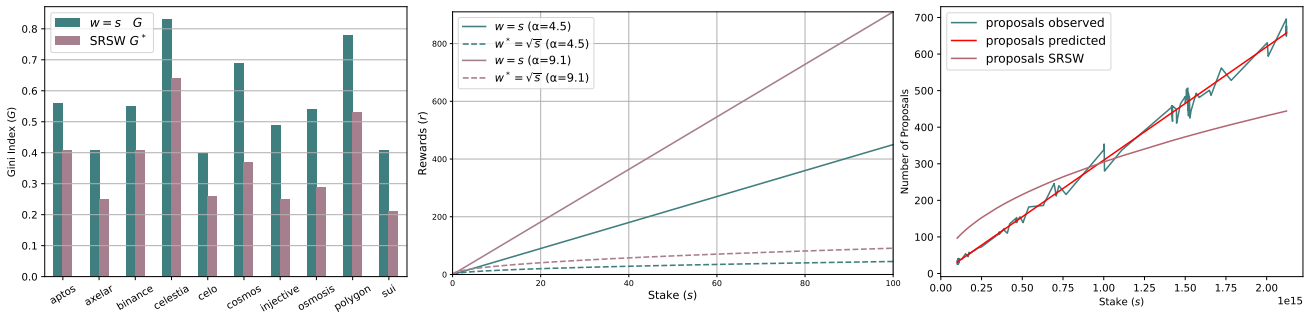


Fig. 1: Comparison of Nakamoto coefficients for safety and liveness in linear and SRSW weighting functions



(a) Comparison of Gini index (b) Reward rate with varying inflations (c) Block proposals made by validators

Fig. 2: Evaluation of SRSW against linear stake weight

their linear stake weights. Subsequently, we compare this against the predicted block proposer distribution under the SRSW model. Our findings reveal that the SRSW model leads to a more diverse array of block proposers, playing a crucial role in mitigating Miner Extractable Value (MEV) risks [23] and enhancing censorship resistance [88]. This diversification in proposers is consistent with decentralization metrics discussed in contemporary studies [52], [53], highlighting the SRSW model's contribution to decentralization.

VII. Related Work

Decentralization in blockchains, a cornerstone for blockchain efficacy, have been extensively explored, with a focus on governance [34], [44], [78], [84], [86]. Recent studies, such as those on token-based voting in DeFi protocols [60], underscore the evolving complexities in blockchain governance. Particularly, decentralization research in PoS and DPoS systems have illuminated the challenges of weight concentration in these protocols [47], [52]–[58].

These studies identify and quantify the weight concentration challenge in weighted consensus, yet solutions to this issue remain underexplored. Existing suggestions, such as capping proposals per validator [43] and introducing reward sharing in validator staking pools [13], offer only partial remedies. Latest research on introducing virtual stake based on validator performance [63] is addressing the challenge but raises potential vulnerabilities such as the 'nothing-at-stake' problem [67]. Our work diverges by enhancing decentralization directly at the consensus mechanism, without the need for new tokens or introducing associated vulnerabilities, thus improving decentralization more holistically.

VIII. Conclusions

In this study, we introduced the Square Root Stake Weight (SRSW) function to address weight concentration in permissionless blockchains, demonstrating substantial improvements in decentralization metrics such as the Gini index and Nakamoto coefficients. While acknowledging the intricacies related to Sybil cost augmentation, this paper highlights the necessity for further investigation into practical implementations and governance models. Future research directions could include exploring geospatial weight distribution and even auction-based mechanisms for validator set selection, potentially offering a means to further decentralize and economically optimize blockchain consensus mechanisms.

References

[1] https://coinmarketcap.com/. Accessed: 2023-12-14.

[2] 0L. Proof-of-fee, part 2. https://0l.network/2022/10/20/proof-of-fee-part-2-a-proposal/. Accessed: 2023-12-15.

[3] Shoshana Abramovich, Graham Jameson, and Gord Sinnamon. Refining jensen's inequality. *Bulletin mathématique de la Société des Sciences Mathématiques de Roumanie*, pages 3–14, 2004.

[4] Big Ace. Injective tendermint core: A powerful consensus engine for decentralized finance. https://medium.com/@charlesace/injective-tendermint-core-a-powerful-consensus-engine-for-decentralized-finance-a1db298b0b70. Accessed: 2023-12-14.

[5] Mustafa Al-Bassam. Lazyledger: A distributed data availability ledger with client-side smart contracts. *arXiv preprint arXiv:1905.09274*, 2019.

[6] Emmanuelle Anceaume, Antonella Pozzo, Thibault Rieutord, and Sara Tucci-Piergiovanni. On finality in blockchains. *arXiv preprint arXiv:2012.10172*, 2020.

[7] Aptos. https://aptosfoundation.org/. Accessed: 2023-10-25.

[8] James Austgen, Andrés Fábrega, Sarah Allen, Kushal Babel, Mahimna Kelkar, and Ari Juels. Dao decentralization: Voting-bloc entropy, bribery, and dark daos. *arXiv preprint arXiv:2311.03530*, 2023.

[9] Axelar. https://axelar.network/. Accessed: 2023-10-25.

[10] Mathieu Baudet, Avery Ching, Andrey Chursin, George Danezis, François Garillot, Zekun Li, Dahlia Malkhi, Oded Naor, Dmitri Perelman, and Alberto Sonnino. State machine replication in the libra blockchain. *The Libra Assn., Tech. Rep*, 7, 2019.

[11] Rafael Belchior, André Vasconcelos, Sérgio Guerreiro, and Miguel Correia. A survey on blockchain interoperability: Past, present, and future trends. *ACM Computing Surveys (CSUR)*, 54(8):1–41, 2021.

[12] Maria Borge, Eleftherios Kokoris-Kogias, Philipp Jovanovic, Linus Gasser, Nicolas Gailly, and Bryan Ford. Proof-of-personhood: Redemocratizing permissionless cryptocurrencies. In *2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 23–26. IEEE, 2017.

[13] Lars Brünjes, Aggelos Kiayias, Elias Koutsoupias, and Aikaterini-Panagiota Stouka. Reward sharing schemes for stake pools. In *2020 IEEE european symposium on security and privacy (EuroS&p)*, pages 256–275. IEEE, 2020.

[14] Ethan Buchman. *Tendermint: Byzantine fault tolerance in the age of blockchains*. PhD thesis, University of Guelph, 2016.

[15] Ethan Buchman, Jae Kwon, and Zarko Milosevic. The latest gossip on bft consensus. *arXiv preprint arXiv:1807.04938*, 2018.

[16] Miguel Castro, Barbara Liskov, et al. Practical byzantine fault tolerance. In *OsDI*, volume 99, pages 173–186, 1999.

[17] Celestia. https://celo.org/. Accessed: 2023-12-14.

[18] Celo. https://celo.org/. Accessed: 2023-12-14.

[19] Lidia Ceriani and Paolo Verme. The origins of the gini index: extracts from variabilità e mutabilità (1912) by corrado gini. *The Journal of Economic Inequality*, 10:421–443, 2012.

[20] BNB Chain. https://www.bnbchain.org/. Accessed: 2023-10-25.

[21] BNB Smart Chain. White paper. https://github.com/bnb-chain/whitepaper/blob/master/WHITEPAPER.md. Accessed: 2023-11-08.

[22] Cosmos. https://cosmos.network/. Accessed: 2023-10-25.

[23] Philip Daian, Steven Goldfeder, Tyler Kell, Yunqi Li, Xueyuan Zhao, Iddo Bentov, Lorenz Breidenbach, and Ari Juels. Flash boys 2.0: Frontrunning in decentralized exchanges, miner extractable value, and consensus instability. In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 910–927. IEEE, 2020.

[24] Bernardo David, Peter Gaži, Aggelos Kiayias, and Alexander Russell. Ouroboros praos: An adaptively-secure, semi-synchronous proof-of-stake blockchain. In *Advances in Cryptology–EUROCRYPT 2018: 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29-May 3, 2018 Proceedings, Part II 37*, pages 66–98. Springer, 2018.

[25] Stefano De Angelis, Leonardo Aniello, Roberto Baldoni, Federico Lombardi, Andrea Margheri, Vladimiro Sassone, et al. Pbft vs proof-of-authority: Applying the cap theorem to permissioned blockchain. In *CEUR workshop proceedings*, volume 2058. CEUR-WS, 2018.

[26] Aptos Dev. The aptos blockchain: Safe, scalable, and upgradeable web3 infrastructure. https://aptos.dev/aptos-white-paper/. Published:2022-08-11, v1.0.

[27] Celestia Docs. Celestia's data availability layer. https://docs.celestia.org/learn/how-celestia-works/data-availability-layer. Accessed: 2023-12-14.

[28] Celo docs. Consensus. https://docs.celo.org/protocol/consensus. Accessed: 2023-11-26.

[29] Osmosis Docs. Glossary. https://docs.osmosis.zone/overview/educate/terminology#consensus. Accessed: 2023-11-26.

[30] Sui Docs. Validator committee. https://docs.sui.io/guides/operator/validator-committee. Accessed: 2023-11-26.

[31] John R Douceur. The sybil attack. In *International workshop on peer-to-peer systems*, pages 251–260. Springer, 2002.

[32] Justin Drake and Toni Wahrstätter. Ethereum addresses added to the ofac sdn list. https://github.com/ultrasoundmoney/ofac-ethereum-addresses/. Accessed: 2023-12-17.

[33] Sisi Duan and Haibin Zhang. Foundations of dynamic bft. In *2022 IEEE Symposium on Security and Privacy (SP)*, pages 1317–1334. IEEE, 2022.

[34] Robin Fritsch, Marino Müller, and Roger Wattenhofer. Analyzing voting power in decentralized governance: Who controls daos? *arXiv preprint arXiv:2204.01176*, 2022.

[35] Juan Garay, Aggelos Kiayias, and Nikos Leonardos. The bitcoin backbone protocol: Analysis and applications. In *Annual international conference on the theory and applications of cryptographic techniques*, pages 281–310. Springer, 2015.

[36] Joseph L Gastwirth. The estimation of the lorenz curve and gini index. *The review of economics and statistics*, pages 306–316, 1972.

[37] Yossi Gilad, Rotem Hemo, Silvio Micali, Georgios Vlachos, and Nickolai Zeldovich. Algorand: Scaling byzantine agreements for cryptocurrencies. In *Proceedings of the 26th symposium on operating systems principles*, pages 51–68, 2017.

[38] Corrado Gini. Measurement of inequality of incomes. *The economic journal*, 31(121):124–125, 1921.

[39] GitHub. Axelar core. https://github.com/axelarnetwork/axelar-core/blob/main/docs/cli/axelard_tendermint_version.md. Accessed: 2023-11-26.

[40] Guy Golan Gueta, Ittai Abraham, Shelly Grossman, Dahlia Malkhi, Benny Pinkas, Michael Reiter, Dragos-Adrian Seredinschi, Orr Tamir, and Alin Tomescu. Sbft: A scalable and decentralized trust infrastructure. In *2019 49th Annual IEEE/IFIP international conference on dependable systems and networks (DSN)*, pages 568–580. IEEE, 2019.

[41] Damian Hodgson. "know your customer": marketing, governmentality and the "new consumer" of financial services. *Management Decision*, 40(4):318–328, 2002.

[42] Injective. https://injective.com/. Accessed: 2023-12-14.

[43] Seungwon Eugene Jeong. Centralized decentralization: Does voting matter? simple economics of the dpos blockchain governance. *Simple Economics of the DPoS Blockchain Governance (April 21, 2020)*, 2020.

[44] Aggelos Kiayias and Philip Lazos. Sok: blockchain governance. *arXiv preprint arXiv:2201.07188*, 2022.

[45] Christine Kim. The most pressing issue on ethereum is validator size growth. https://www.coindesk.com/consensus-magazine/2023/09/29/the-most-pressing-issue-on-ethereum-is-validator-size-growth/. Accessed: 2023-12-14.

[46] Heesang Kim and Dohoon Kim. A taxonomic hierarchy of blockchain consensus algorithms: An evolutionary phylogeny approach. *Sensors*, 23(5):2739, 2023.

[47] Minjeong Kim, Yujin Kwon, and Yongdae Kim. Is stellar as secure as you think? In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 377–385. IEEE, 2019.

[48] Yujin Kwon, Jian Liu, Minjeong Kim, Dawn Song, and Yongdae Kim. Impossibility of full decentralization in permissionless blockchains. In *Proceedings of the 1st ACM Conference on Advances in Financial Technologies*, pages 110–123, 2019.

[49] Leslie Lamport, Robert Shostak, and Marshall Pease. The byzantine generals problem. In *Concurrency: the works of leslie lamport*, pages 203–226. 2019.

[50] Alfred Lehar and Christine A Parlour. Decentralized exchanges. *Available at SSRN 3905316*, 2021.

[51] Andrew Lewis-Pye and Tim Roughgarden. How does blockchain security dictate blockchain implementation? In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, pages 1006–1019, 2021.

[52] Chao Li and Balaji Palanisamy. Comparison of decentralization in dpos and pow blockchains. In *Blockchain–ICBC 2020: Third International Conference, Held as Part of the Services Conference Federation, SCF 2020, Honolulu, HI, USA, September 18-20, 2020, Proceedings 3*, pages 18–32. Springer, 2020.

[53] Chao Li, Balaji Palanisamy, Runhua Xu, and Li Duan. Cross-consensus measurement of individual-level decentralization in blockchains. In *2023 IEEE 9th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing,(HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)*, pages 45–50. IEEE, 2023.

[54] Chao Li, Balaji Palanisamy, Runhua Xu, Li Duan, Jiqiang Liu, and Wei Wang. How hard is takeover in dpos blockchains? understanding the security of coin-based voting governance. *arXiv preprint arXiv:2310.18596*, 2023.

[55] Chao Li, Runhua Xu, and Li Duan. Liquid democracy in dpos blockchains. In *Proceedings of the 5th ACM International Symposium on Blockchain and Secure Critical Infrastructure*, pages 25–33, 2023.

[56] Qinwei Lin, Chao Li, Xifeng Zhao, and Xianhai Chen. Measuring decentralization in bitcoin and ethereum using multiple metrics and granularities. In *2021 IEEE 37th International Conference on Data Engineering Workshops (ICDEW)*, pages 80–87. IEEE, 2021.

[57] Jieli Liu, Weilin Zheng, Dingyuan Lu, Jiajing Wu, and Zibin Zheng. From decentralization to oligopoly: A data-driven analysis of decentralization evolution and voting behaviors on eosio. *IEEE Transactions on Computational Social Systems*, 2022.

[58] Jieli Liu, Weilin Zheng, Dingyuan Lu, Jiajing Wu, and Zibin Zheng. Understanding the decentralization of dpos: perspectives from data-driven analysis on eosio. *arXiv preprint arXiv:2201.06187*, 2022.

[59] Patrick McCorry, Chris Buckland, Bennet Yee, and Dawn Song. Sok: Validating bridges as a scaling solution for blockchains. *Cryptology ePrint Archive*, 2021.

[60] Johnnatan Messias, Vabuk Pahari, Balakrishnan Chandrasekaran, Krishna P Gummadi, and Patrick Loiseau. Understanding blockchain governance: Analyzing decentralized voting to amend defi smart contracts. *arXiv preprint arXiv:2305.17655*, 2023.

[61] Johnnatan Messias, Aviv Yaish, and Benjamin Livshits. Airdrops: Giving money away is harder than it seems. *arXiv preprint arXiv:2312.02752*, 2023.

[62] Andrew Miller, Yu Xia, Kyle Croman, Elaine Shi, and Dawn Song. The honey badger of bft protocols. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, pages 31–42, 2016.

[63] Jelena Mišić, Vojislav B Mišić, and Xiaolin Chang. Towards decentralization in dpos systems: election, voting and leader selection using virtual stake. *IEEE Transactions on Network and Service Management*, 2023.

[64] Henrique Moniz. The istanbul bft consensus algorithm. *arXiv preprint arXiv:2002.03613*, 2020.

[65] Nicholas Morgan. Lido dominance prompts warnings about liquid staking derivatives. https://decrypt.co/154804/lido-lsd-liquid-staking-decentralization. Accessed: 2023-11-29.

[66] Shashank Motepalli, Luciano Freitas, and Benjamin Livshits. Sok: Decentralized sequencers for rollups. *arXiv preprint arXiv:2310.03616*, 2023.

[67] Shashank Motepalli and Hans-Arno Jacobsen. Reward mechanism for blockchains using evolutionary game theory. In *2021 3rd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, pages 217–224. IEEE, 2021.

[68] Shashank Motepalli and Hans-Arno Jacobsen. Decentralizing permissioned blockchain with delay towers. *arXiv preprint arXiv:2203.09714*, 2022.

[69] Shashank Motepalli and Hans-Arno Jacobsen. Analyzing geospatial distribution in blockchains. *arXiv preprint arXiv:2305.17771*, 2023.

[70] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. *Decentralized business review*, 2008.

[71] Diego Ongaro and John Ousterhout. In search of an understandable consensus algorithm. In *2014 USENIX annual technical conference (USENIX ATC 14)*, pages 305–319, 2014.

[72] Osmosis. https://osmosis.zone/. Accessed: 2023-10-25.

[73] Rafael Pass, Lior Seeman, and Abhi Shelat. Analysis of the blockchain protocol in asynchronous networks. In *Annual international conference on the theory and applications of cryptographic techniques*, pages 643–673. Springer, 2017.

[74] Polygon. https://polygon.technology/. Accessed: 2023-10-25.

[75] Staking Rewards. Proof of stake. https://www.stakingrewards.com/assets/proof-of-stake. Accessed: 2023-12-03.

[76] Sheikh Munir Skh Saad and Raja Zahilah Raja Mohd Radzi. Comparative review of the blockchain consensus algorithm between proof of stake (pos) and delegated proof of stake (dpos). *International Journal of Innovative Computing*, 10(2), 2020.

[77] Aaron Schneider. Decentralization: Conceptualization and measurement. *Studies in comparative international development*, 38:32–56, 2003.

[78] Tanusree Sharma, Yujin Kwon, Kornrapat Pongmala, Henry Wang, Andrew Miller, Dawn Song, and Yang Wang. Unpacking how decentralized autonomous organizations (daos) work in practice. *arXiv preprint arXiv:2304.09822*, 2023.

[79] Daniel P Siewiorek and Priya Narasimhan. Fault-tolerant architectures for space and avionics applications. *NASA Ames Research http://ic. arc. nasa. gov/projects/ishem/Papers/Siewi*, 2005.

[80] Thitithep Sitthiyot and Kanyarat Holasut. A simple method for measuring inequality. *Palgrave Communications*, 6(1):1–9, 2020.

[81] Thitithep Sitthiyot and Kanyarat Holasut. A simple method for estimating the lorenz curve. *Humanities and Social Sciences Communications*, 8(1):1–9, 2021.

[82] Alexander Spiegelman, Neil Giridharan, Alberto Sonnino, and Lefteris Kokoris-Kogias. Bullshark: Dag bft protocols made practical. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, pages 2705–2718, 2022.

[83] Srivatsan Sridhar, Dionysis Zindros, and David Tse. Better safe than sorry: Recovering after adversarial majority. *arXiv preprint arXiv:2310.06338*, 2023.

[84] Balaji S. Srinivasan and Leland Lee. Quantifying decentralization. https://news.earn.com/quantifying-decentralization-e39db233c28e. Accessed: 2023-11-05.

[85] Sui. hhttps://sui.io/. Accessed: 2023-10-25.

[86] Joshua Z Tan, Tara Merk, Sarah Hubbard, Eliza R Oak, Joni Pirovich, Ellie Rennie, Rolf Hoefer, Michael Zargham, Jason Potts, Chris Berg, et al. Open problems in daos. *arXiv preprint arXiv:2310.19201*, 2023.

[87] Chjango Unchained. Tendermint explained — bringing bft-based pos to the public blockchain domain. https://blog.cosmos.network/tendermint-explained-bringing-bft-based-pos-to-the-public-blockchain-domain-f22e274a0fdb. Accessed: 2023-11-26.

[88] Toni Wahrstätter. Ethereum censorship dashboard. https://censorship.pics/. Accessed: 2023-12-17.

[89] Zeli Wang, Hai Jin, Weiqi Dai, Kim-Kwang Raymond Choo, and Deqing Zou. Ethereum smart contract security research: survey and future research opportunities. *Frontiers of Computer Science*, 15:1–18, 2021.

[90] John H Wensley, Leslie Lamport, Jack Goldberg, Milton W Green, Karl N Levitt, Po Mo Melliar-Smith, Robert E Shostak, and Charles B Weinstock. Sift: Design and analysis of a fault-tolerant computer for aircraft control. *Proceedings of the IEEE*, 66(10):1240–1255, 1978.

[91] Polygon wiki. Peppermint. https://wiki.polygon.technology/docs/pos/design/heimdall/peppermint. Accessed: 2023-11-26.

[92] Worldcoin. A new identity and financial network. https://whitepaper.worldcoin.org/#a-new-identity-and-financial-network. Accessed: 2023-12-16.

[93] Maofan Yin, Dahlia Malkhi, Michael K Reiter, Guy Golan Gueta, and Ittai Abraham. Hotstuff: Bft consensus with linearity and responsiveness. In *Proceedings of the 2019 ACM Symposium on Principles of Distributed Computing*, pages 347–356, 2019.

[94] Gengrui Zhang. *Towards More Efficient and Scalable Consensus Algorithms*. PhD thesis, University of Toronto, 2023.

[95] Gengrui Zhang, Fei Pan, Michael Dang'ana, Yunhao Mao, Shashank Motepalli, Shiquan Zhang, and Hans-Arno Jacobsen. Reaching consensus in the byzantine empire: A comprehensive review of bft consensus algorithms. *arXiv preprint arXiv:2204.03181*, 2022.

[96] Gengrui Zhang, Fei Pan, Sofia Tijanic, and Hans-Arno Jacobsen. Prestigebft: Revolutionizing view changes in bft consensus algorithms with reputation mechanisms. *arXiv preprint arXiv:2307.08154*, 2023.