Decentralization in PoS Blockchain Consensus: Quantification and Advancement

Gangryun Kwon

Feb. 27, 2026

INFONET Journal Club Presentation

Paper information

Paper Title: Decentralization in PoS Blockchain Consensus: Quantification and Advancement

Venue : IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT

Author: Shashank Motepalli, Hans-Arno Jacobsen

Affiliation: University of Toronto

Date: 19th April 2025

Decentralization in PoS Blockchain Consensus: Quantification and Advancement

Shashank Motepalli and Hans-Arno Jacobsen, *Fellow, IEEE*

***Abstract*—Decentralization is a foundational principle of permissionless blockchains, with consensus mechanisms serving a critical role in its realization. This study quantifies the decentralization of consensus mechanisms in proof-of-stake (PoS) blockchains using a comprehensive set of metrics, including Nakamoto coefficients, Gini, Herfindahl-Hirschman Index (HHI), Shapley values, and Zipf's coefficient. Our empirical analysis across ten prominent blockchains reveals significant concentration of stake among a few validators, posing challenges to fair consensus. To address this, we introduce two alternative weighting models for PoS consensus: Square Root Stake Weight (SRSW) and Logarithmic Stake Weight (LSW), which adjust validator influence through non-linear transformations. Results demonstrate that SRSW and LSW models improve decentralization metrics by an average of 51% and 132%, respectively, supporting more equitable and resilient blockchain systems.**

***Index Terms*—Blockchains, decentralized applications, decentralized applications.**

I. Introduction

BITCOIN shaped the field of blockchains by introducing a peer-to-peer system that operates without trusted intermediaries [71]. Its vision encapsulates *decentralization*, characterized by the elimination of single points of failure. 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.

To address the challenge of decentralization in proof-of-stake (PoS) blockchains, we analyze how a validator's stake influences their voting power in weighted consensus mechanisms. Drawing inspiration from quantitative decentralization metrics originally developed for decentralized autonomous organizations (DAOs) with token-based voting [7], [81], [88], we extend these frameworks to measure decentralization within consensus mechanisms. Specifically, we adapt metrics such as the Gini index and Nakamoto coefficients for both safety and liveness to assess validator influence [70]. Our empirical analysis spans ten major blockchains: Aptos [6], Axelar [8], BNB [21], Celestia [18], Celo [19], Cosmos [24], Injective [42], Osmosis [74], Polygon [77], and Sui [87]. Findings reveal a concentration of voting power among a small subset of validators, raising critical concerns for blockchain security and integrity. To address this, we propose the Square Root Stake Weight (SRSW) function, demonstrating its effectiveness through extensive evaluation [70].

This paper extends our previous work [70] across four main dimensions. First, we broaden the analysis of decentralization by adapting four new interdisciplinary metrics, including the Shapley value from cooperative game theory to capture coalition influence, along with the Herfindahl-Hirschman Index and Zipf's law coefficient. Second, we introduce the Logarithmic Stake Weight (LSW) model to further decentralize consensus mechanisms, showing that LSW consistently outperforms SRSW and current PoS models by an average of 51% and 132% across all metrics, respectively. Third, we provide empirical assessments for both SRSW and LSW models and extending the formal analysis with rigorous proofs that justify the observed results. Lastly, we broaden the scope of our empirical analysis by incorporating additional metrics across our blockchain set, using the latest available data to ensure relevance.

Our contributions are four-fold:

1) Adapt and formalize decentralization metrics specifically for evaluating 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) and Logarithmic Stake Weight (LSW) as mechanisms to address the weight concentration challenge.
4) Our work pioneers a data-driven approach to consensus research, offering novel insights and solutions to enhance decentralization in blockchain systems.

This paper is organized as follows. We begin with a classification of consensus mechanisms, based on finality, in the following section. After adapting metrics to capture

Received 27 November 2024; revised 28 March 2025; accepted 6 April 2025. Date of publication 15 April 2025; date of current version 7 August 2025. This work has been supported in part by NSERC, ORF, and the Sui Foundation. The associate editor coordinating the review of this article and approving it for publication was S. Kanhere. *(Corresponding author: Shashank Motepalli.)*

The authors are with the Department of Electrical and Computer Engineering, University of Toronto, Toronto, ON M5S 1A1, Canada (e-mail: shashank.motepalli@mail.utoronto.ca).

Digital Object Identifier 10.1109/TNSM.2025.3561098

contribution

- 1) Adapt and formalize decentralization metrics specifically for evaluating consensus mechanisms.
- 2) Empirically demonstrate the challenge of weight concentration and its impact on decentralization in prominent blockchains.
- 3) Introduce the Square Root Stake Weight (SRSW) and Logarithmic Stake Weight (LSW) as mechanisms to address the weight concentration challenge.
- 4) Pioneer a data-driven approach to consensus research, offering novel insights and solutions to enhance decentralization in blockchain systems.

PoS Blockchain consensus

- PoS is a consensus mechanism where validators are selected proportionally to their staked tokens.

- Each validator has weight proportional to the number of coin staked.
  - $\mathbf{w_k = s_k}$
- Total weight W
  - $\mathbf{W = \sum_{k}^{m} w_k \quad \forall k \in N}$
- Condition for Quorum Q
  - $\mathbb{Q} \geqslant \frac{2}{3}\mathbf{W}$

Metrics

(m,ε,δ) decentralization model

m: indicates the cardinality of the validator set

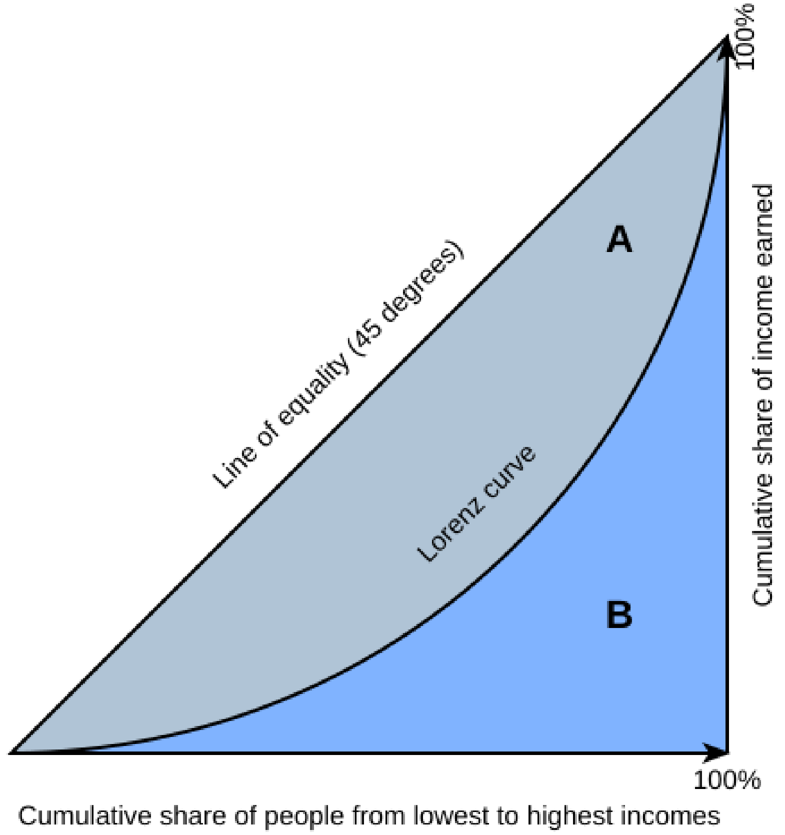
ε: represents the weight disparity between the most influential (richest) and the δ-th percentile validator.

Gini Coefficient(G)

Gini coefficient quantifies how unevenly a resource is distributed

0 under perfect equality and approaches
1 as influence becomes concentrated in a small minority.

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



Metrics

Nakamoto coefficient – Liveness $\rho_{\mathbb{N}_L}$

minimum fraction of validators whose coordinated disruption can halt block production and prevent the chain from making progress.

$$\mathbb{N}_L = \min\{|L| \mid L \subseteq N, \sum_{i \in L} w_i \geq \frac{1}{3} W\}$$

$$\rho_{\mathbb{N}_L} = \frac{\mathbb{N}_L}{m} \times 100$$

Nakamoto coefficient – Safety $\rho_{\mathbb{N}_S}$

minimum fraction of validators whose coordinated behavior can violate consistency by finalizing conflicting histories.

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

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

Metrics

Herfindahl-Hirschman Index (HHI)

the sum of the squared shares of each validator’s stake or voting weight

measure how concentrated consensus power is.

$$HHI = \sum_{k=1}^{m} (w'_k)^2, \text{ where } w'_k = \frac{w_k}{\sum_{k=1}^{m} w_k}$$

Zipf’s Law Coefficient(Z)

exponent (α) in the rank–size power-law fit (weight ∝ rank^−α)

indicate how heavy-tailed and skewed the validator power distribution is.

$$w_r \propto r^{-Z}$$

Metrics

The Shapley value is the expected contribution of a player, averaged over all possible permutations of coalition formation.

Shapley Value for liveness and Gini analysis

$$\varphi_k^L = \sum_{S \subseteq N \setminus \{k\}} \frac{|S|!\,(m-|S|-1)!}{m!}\left(v(S \cup \{k\}) - v(S)\right)$$

$$v(S) = \begin{cases} 1, & \text{if} \sum_{i \in S} w_i > 0.33 \times W \\ 0, & \text{otherwise} \end{cases}$$

G_{φ^L} is Gini coefficient over distribution of φ_K^L

Shapley Value for Safety and Gini analysis

$$\varphi_k^L = \sum_{S \subseteq N \setminus \{k\}} \frac{|S|!\,(m-|S|-1)!}{m!}\left(v(S \cup \{k\}) - v(S)\right)$$

$$v(S) = \begin{cases} 1, & \text{if} \sum_{i \in S} w_i > 0.66 \times W \\ 0, & \text{otherwise} \end{cases}$$

G_{φ^S} is Gini coefficient over distribution of φ_K^S

DECENTRALIZATION METRICS FOR PERMISSIONLESS BLOCKCHAINS

TABLE III
DECENTRALIZATION METRICS FOR PERMISSIONLESS BLOCKCHAINS

	Application	m	G	$\rho_{\mathbb{N}_L}$	$\rho_{\mathbb{N}_S}$	HHI	G_{φ^L}	G_{φ^S}	$\mathcal{Z}$	ε in $(m, \varepsilon, 0)$	$(m, \varepsilon, 50)$
Aptos	L1 blockchain [6]	191	0.55	11.52	27.23	0.011	0.561	0.559	3.135	1127805207331	7.99
Axelar	Interoperability [8]	75	0.37	16	41.33	0.02	0.375	0.373	0.928	591.9	2.83
BNB (Binance)	L1 blockchain [21]	57	0.55	14.04	28.07	0.036	0.556	0.558	2.316	159511.43	8.41
Celestia	Data availability [18]	239	0.8	2.93	11.3	0.026	0.797	0.803	5.679	4468193447.12	4940.77
Celo	L2* (L1 blockchain) [19]	86	0.42	13.95	38.37	0.019	0.426	0.425	1.517	8805762239.16	2.85
Cosmos	L1/interoperability [24]	200	0.72	3.5	12	0.029	0.73	0.731	1.573	23841.39	72.73
Injective	DeFi/interoperability [42]	60	0.4	11.67	38.33	0.033	0.409	0.414	0.72	26.62	8.96
Osmosis	DeFi/DEX [74]	150	0.54	6.67	28	0.02	0.554	0.557	1.022	108.05	14.52
Polygon	L2/ZK-rollup [77]	105	0.79	3.81	11.43	0.051	0.8	0.8	2.057	35677.03	114.84
Sui	L1 blockchain [87]	108	0.35	15.74	39.81	0.014	0.351	0.358	0.63	10.37	3.0

DECENTRALIZATION METRICS FOR PERMISSIONLESS BLOCKCHAINS

Gini coefficient: 0.35~ 0.8 $(\approx \boldsymbol{G_{\varphi^L}, G_{\varphi^S}})$

(Gini coefficient of America money income: ~0.48 /South Korea money income: ~0.32)

Nakamoto coefficient: $\rho_{\mathbb{N}_L}$:2.93~16% $\rho_{\mathbb{N}_S}$:11.3~41.3%

	Application	m	G	ρ_{NL}	ρ_{NS}	**HHI**	$G_{\varphi L}$	$G_{\varphi S}$	z	ε **in** $(m, \varepsilon, 0)$	$(m, \varepsilon, 50)$
Polygon	L2/ZK-rollup [77]	105	0.79	3.81	11.43	0.051	0.8	0.8	2.057	35677.03	114.84

On Polygon, top 4 validators could halt block production, top 12 validators could alter the ledger.

HHI: $\leq \mathbf{0.051}$

No single dominant validator

Ziph coefficient:0.63~5.67

these results suggest that decentralization remains limited in many PoS-based networks.

SRSW and LSW

SRSW(Square root stake weight)

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

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

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

Sybil-resistance condition

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

LSW(Log Stake weight)

$$w_i^\phi = \log s_i$$

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

$$r_{n_i}^\phi = \alpha w_i^\phi = \alpha \log s_i, \quad \text{if } s_i > s_M; \text{otherwise, } 0.$$

Sybil-resistance condition

$$r_{n_i}^\phi > r_{n_j}^\phi + r_{n_k}^\phi - C, where \ s_i \geq s_j + s_k$$

Concave stake weighting compresses large stakes and reduces marginal dominance.

SRSW and LSW

- **Lemma1**
  Given a validator set N, the SRSW model's Nakamoto coefficients, $\rho^*_{N_L}$ and $\rho^*_{N_S}$, are greater than or equal to that of the linear stake-weight model, represented as ρ_{N_L} and ρ_{N_L} , respectively.
- **Lemma2**
  Given N, the Gini of SRSW and linear models, represented by G^* and G, respectively, satisfy $G^* \leq G$.
- **Theorem1**
  Given a validator set N, the SRSW model achieves a degree of decentralization, across key metrics, that is greater than or equal to that of the linear stake-weight model.
- **Theorem 2**
  Given a validator set N, the LSW model achieves a higher degree of decentralization across key metrics than the SRSW model.
- **Collorary 1**
  the LSW model achieves a higher degree of decentralization than the linear stake-weight model across all metrics.

the paper shows that LSW > SRSW > Linear in terms of decentralization across all evaluation metrics.

Empirical validaton

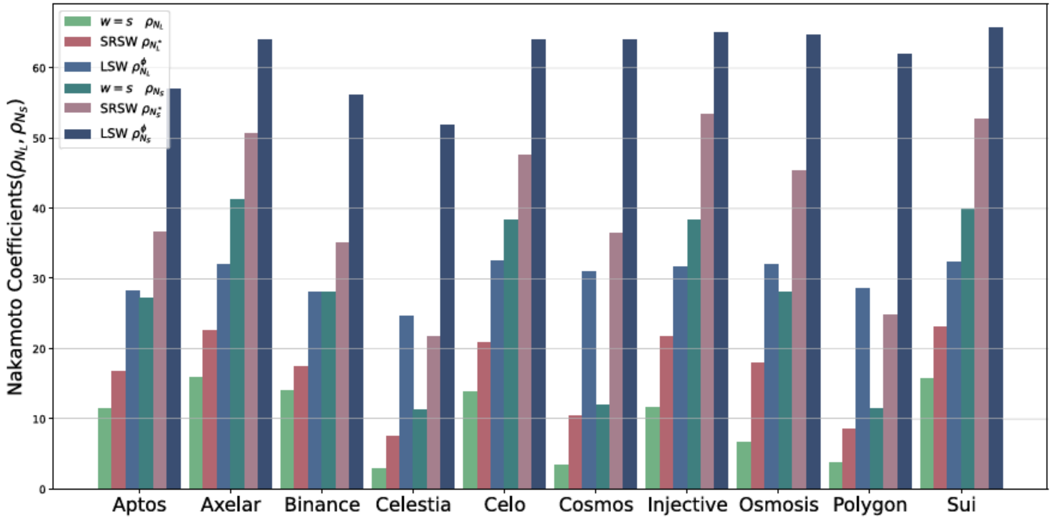


Fig. 1. Comparison of Nakamoto coefficients for safety and liveness in linear, SRSW and LSW weighting functions.

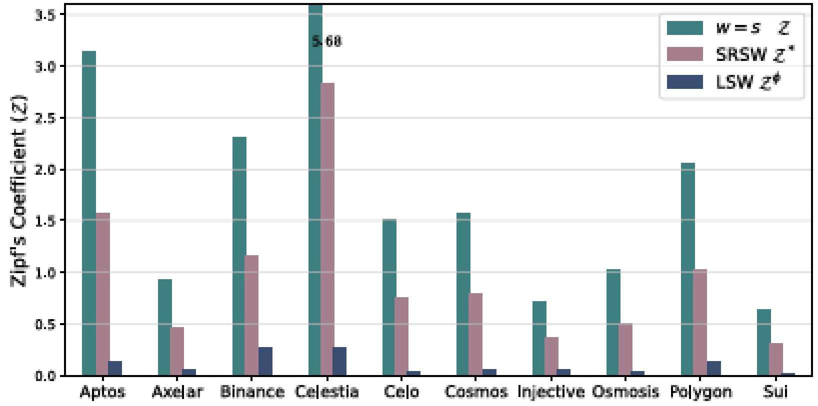


Fig. 3. Comparison of Zipf's law coefficient.

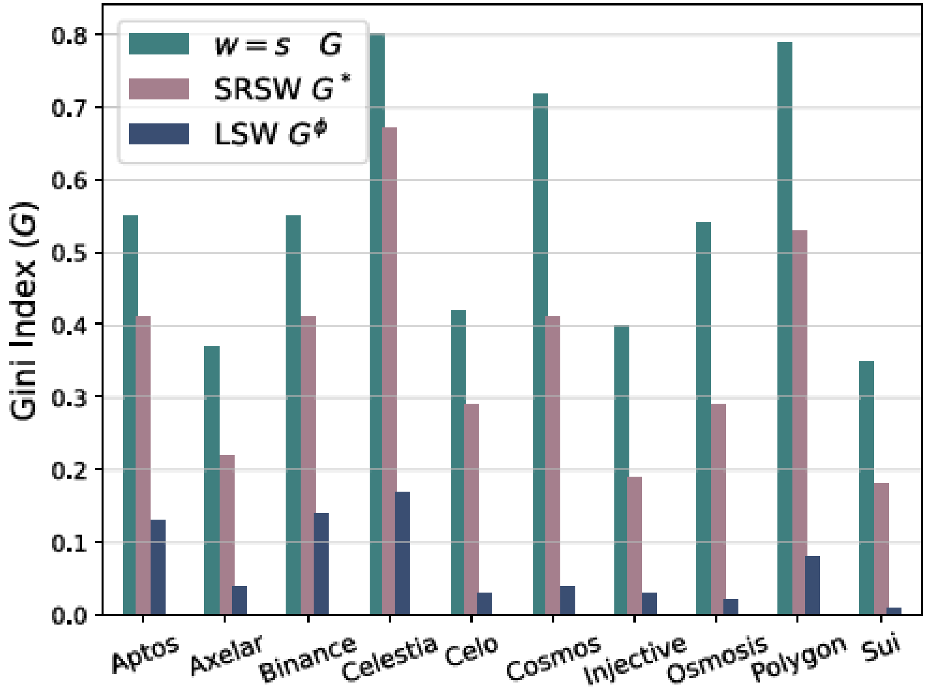


Fig. 2. Comparison of Gini index.

GIST

Empirical validaton

TABLE IV

PERCENTAGE IMPROVEMENTS OF SRSW AND LSW OVER LINEAR TOKEN WEIGHTS FOR VARIOUS DECENTRALIZATION METRICS

Blockchain	ρ_{N_L} (%)	ρ_{N_S} (%)	G (%)	HHI (%)	$G_{\varphi L}$ (%)	$G_{\varphi L}$(%)	$\mathcal{Z}$ (%)
Aptos	45.4 / 145.4	34.59 / 109.59	25.45 / 76.36	27.27 / 45.45	26.56 / 72.19	25.76 / 70.84	49.98 / 95.92
Axelar	41.69 / 100	22.6 / 54.85	40.54 / 89.19	25 / 35	38.93 / 84.53	40.75 / 87.94	50 / 93.32
Binance	24.93 / 99.93	25.01 / 100	25.45 / 74.55	25 / 47.22	24.64 / 73.92	25.45 / 73.84	50 / 88.51
Celestia	157 / 742.66	92.57 / 359.12	16.25 / 78.75	53.85 / 80.77	15.56 / 76.54	16.44 / 77.33	49.99 / 95.33
Celo	50.04 / 133.41	24.24 / 66.67	30.95 / 92.86	21.05 / 36.84	30.05 / 83.1	31.29 / 86.59	50.03 / 98.09
Cosmos	200 / 785.71	204.17 / 433.33	43.06 / 94.44	68.97 / 82.76	42.05 / 91.37	42.41 / 90.15	50.03 / 96.25
Injective	85.69 / 171.38	39.13 / 69.58	52.5 / 92.5	42.42 / 48.48	53.3 / 89.73	50.48 / 92.51	50 / 92.78
Osmosis	169.87 / 379.76	61.89 / 130.96	46.3 / 96.3	55 / 65	47.29 / 91.7	45.52 / 87.2	50 / 96.48
Polygon	124.93 / 649.87	116.62 / 441.56	32.91 / 89.87	56.86 / 80.39	32.13 / 89	32.5 / 89	50.02 / 93.68
Sui	47.08 / 105.91	32.58 / 65.13	48.57 / 97.14	28.57 / 35.71	46.72/ 89.74	45.53 / 88.55	50 / 97.46
Average	94.66 / 331.40	65.34 / 183.08	36.20 / 88.20	40.39 / 55.76	35.72 / 84.18	35.61 / 84.4	50.01 / 95.62

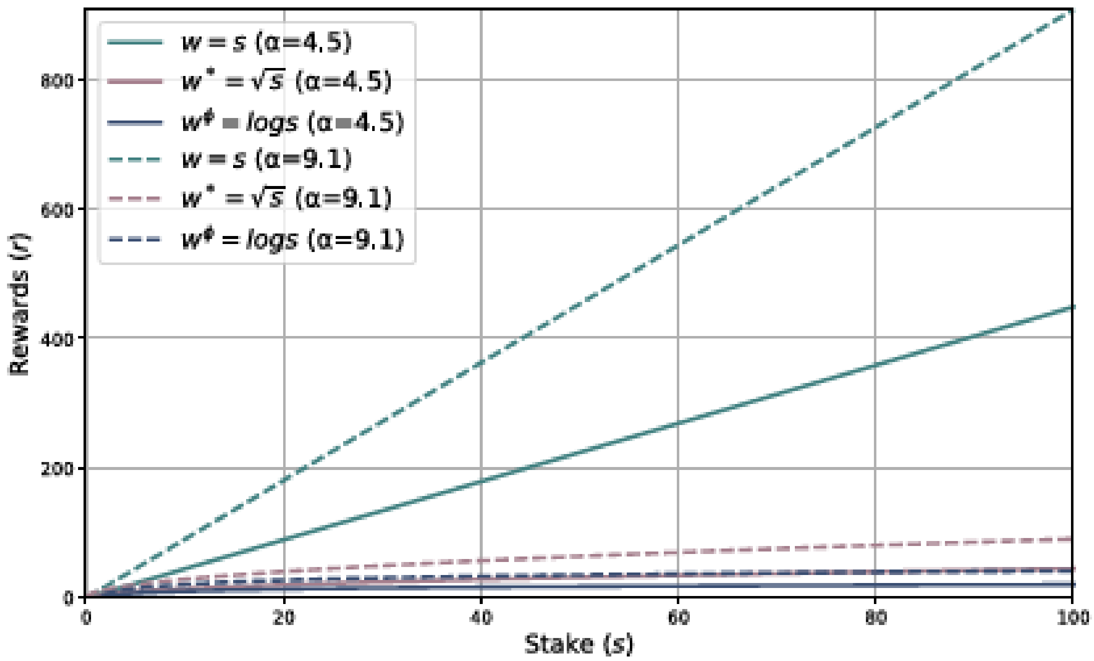
Empirical validation

- **Nakamoto Coefficients (ρNL, ρNS)**
  - vs. linear: **ρNL ↑ 24.93–169.87% (SRSW)**, **↑ 100–785.71% (LSW)**
  - **ρNS (avg.) ↑ 65.34% (SRSW)**, **↑ 183.01% (LSW)**
  - Interpretation: **more validators needed to influence consensus → higher centralization resistance**
- **Gini Index (weights inequality)**
  - **SRSW: ↓ 16.25–48.57%**
  - **LSW: ↓ 74.55–97.14%**
  - Interpretation: **stake-weight distribution becomes much more equal → higher decentralization**
- **HHI (concentration)**
  - **SRSW (avg.): ↓ 40.39%**
  - **LSW (avg.): ↓ 55.76%**
  - Interpretation: **even with no monopoly already, concentration drops further vs. linear**

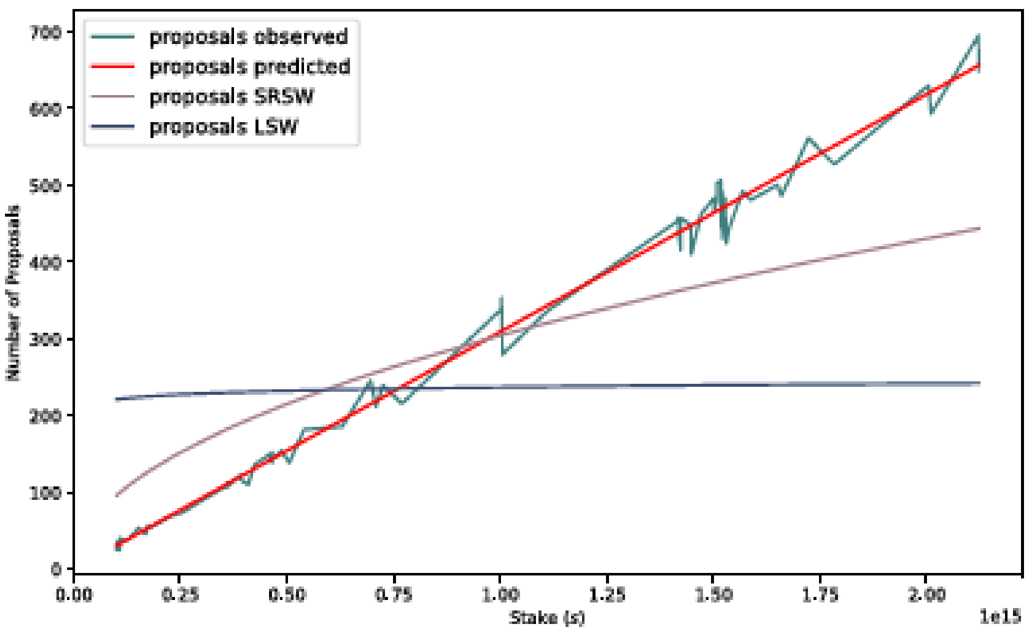
Empirical validation

- **Shapley Values (influence inequality)**
  - Shapley-Gini (liveness & safety) follows weight-Gini trends
  - **Mean correlation: 0.96** (percentage improvements)
  - Interpretation: **weight equalization ≈ influence equalization**
- **Zipf's Coefficient (heavy-tail / power-law skew)**
  - **Substantial improvement**, especially under **LSW**
  - Interpretation: **weaker heavy-tail → more decentralized distribution**

Secondary effects



(a) Reward rate with varying inflations



(b) Block proposals made by validators

Concluson

- The paper introduces Square Root Stake Weight (SRSW) and Log Stake Weight (LSW) to mitigate stake concentration in permissionless blockchains, reporting strong improvements across decentralization metrics.
- It also notes that practical Sybil resistance and governance remain challenging, and points to future directions such as geospatial weighting and auction-based validator selection to further improve decentralization and economic efficiency.

Thank you