On-Chain Analysis of Network Decentralization in Cardano Post-k Adjustment

Junya Yamada*, Kentaroh Toyoda†, Takanori Hara*,
Yu Nakahata*, Christopher Wiraatmaja*, Shoji Kasahara*
*Nara Institute of Science and Technology, Ikoma, Nara, Japan
Emails: yamada.junya.yj9@naist.ac.jp, hara@ieee.org, yu.nakahata@is.naist.jp,
wiraatmaja.christopher@naist.ac.jp, kasahara@ieee.org
† Keio University, Yokohama, Kanagawa, Japan Email: kentaroh.toyoda@ieee.org

***Abstract*—Cardano, a major Proof-of-Stake (PoS) blockchain, aims to achieve decentralization through its reward distribution mechanism governed by the protocol parameter k, which defines the ideal number of reward-receiving stake pools. While k plays a critical role in shaping network dynamics, its current value is statically determined and lacks a formal theoretical basis.**

In this study, we conduct an empirical analysis of Cardano's on-chain data to evaluate the effects of changing k on decentralization metrics such as the number of active pools, stake distribution, and the Nakamoto coefficient. Our findings show that while increasing k initially enhances decentralization, the long-term effects are limited due to dynamic shifts in pool performance and stake concentration.

Based on these insights, we propose the foundation for a dynamic optimization framework that determines the appropriate value of k by integrating decentralization, operational cost, and behavioral factors. This work contributes to the development of sustainable and fair PoS governance through data-driven parameter tuning.

***Index Terms*—Blockchain Governance, Cardano, Proof of Stake, On-chain Analysis**

I. Introduction

Blockchain technology, leveraging the characteristics of decentralized systems, has attracted attention as a highly reliable infrastructure across various domains. Among these, blockchains that adopt the Proof of Stake (PoS) consensus mechanism have been widely adopted in recent years due to their high energy efficiency and flexibility in economic incentive design (e.g., [1]–[3]). One such example is Cardano, which aims to enhance network decentralization through its reward design.

The reward distribution mechanism in Cardano has been theoretically formalized as a Reward Sharing Scheme (RSS) for stake pools, proposed by Brünjes et al. [4]. This model elaborates on the reward calculation method for stake pools and the incentive effects it has on participants' economic behavior. In this context, the parameter k, which represents the ideal number of pools, is a central design element that directly affects network decentralization. However, the current value of k (e.g., 500) has been statically determined based on practical considerations rather than a clear theoretical foundation. Under such a setting, there is no guarantee that the current k remains optimal when the network size or stake distribution changes.

In this regard, the study by Ovezik et al. [5] quantitatively evaluates the behavior of decentralization and stake concentration under the RSS model through simulations with a fixed k. However, the present study does not take into account the effects of time-dependent variations in the parameter k, nor does it investigate the impact of parameter tuning.

This study empirically analyzes changes in network decentralization (e.g., stake distribution, Nakamoto coefficient) using on-chain data, focusing on the effects of network stability after k was adjusted. Based on this analysis, we explore methods to dynamically and theoretically derive an optimal value for k.

Based on our findings, we propose defining a social welfare function that incorporates utility based on decentralization level and operational costs, aiming to derive the value of k that maximizes this function. Furthermore, assuming that both stake pool operators and delegators are human agents, we incorporate behavioral economic perspectives, such as prospect theory [6], [7], to account for cognitive biases in decision-making, thereby proposing a more realistic methodology for setting the parameter k.

The remainder of this paper is organized as follows: Section II introduces the foundational concepts of Cardano's network structure, its reward mechanism, and decentralization metrics. Section III reviews prior theoretical and empirical research on Proof-of-Stake decentralization, with a focus on Cardano and its reward design. Section IV describes our data collection methodology and the on-chain metrics analyzed. Section V discusses the implications and outlines a framework for dynamic protocol parameter tuning. Finally, Section VI concludes the paper.

II. Preliminaries

This section explains the foundational concepts necessary to understand this study, including the basic structure of Cardano, its reward distribution design, decentralization metrics, and delegation mechanism.

A. *Overview of Cardano and Proof-of-Stake*

Cardano is a third-generation blockchain platform that employs a PoS consensus mechanism based on the Ouroboros protocol [2]. In PoS, validators (stake pool operators) gain the right to produce blocks in proportion to the amount of ADA they hold or have been delegated by others. This mechanism enables better energy efficiency compared to Proof-of-Work (PoW), while aligning network security with economic incentives.

Users can participate in network operation either by running their own pools or by delegating their stake to existing ones. This design reflects Cardano's goal of achieving a decentralized and sustainable network.

B. Reward Sharing Scheme (RSS) in Cardano

To enhance decentralization and encourage honest behavior among participants, Cardano implements a reward distribution mechanism called the RSS [4]. In this scheme, rewards are distributed to both stake pool operators and delegators. The distribution amount depends on multiple factors, including the pool's performance, its relative position in the network, and parameters set by the operator.

The reward function includes the parameter k, which is the focus of this study, and is expressed as follows:

$$r_k(\sigma, \lambda) = \frac{R}{1+\alpha} \cdot \left[\sigma' + \lambda' \cdot \alpha \cdot \frac{\sigma' - \lambda' \cdot (1 - \sigma'/\beta)}{\beta} \right]. \quad (1)$$

The parameters used in the reward function $r_k(\sigma, \lambda)$ are summarized in Table I.

TABLE I: Parameters used in the reward function $r_k(\sigma, \lambda)$.

Symbol	Description
$\sigma \in [0,1]$	Total stake in the pool
$\lambda \in (0,1)$	Pool leader's own stake
$\sigma' = \min\{\sigma, \beta\}$	Capped pool stake
$\lambda' = \min\{\lambda, \beta\}$	Capped leader stake
$\beta = 1/k$	Target pool size
$R \in \mathbb{R}$	Total available reward
$\alpha \in [0, \infty)$	Sybil resistance parameter
$k \in \mathbb{N}$	Target number of pools

These factors include the amount of stake attracted to a pool and its level of concentration. Although the reward calculation is complex and defined by the protocol, its core aim is to promote sustainable decentralization that does not rely solely on the size of the stake.

A key parameter in the RSS is k, which represents the ideal number of stake pools. This value significantly influences stake distribution and delegation behavior within the network. A small k leads to stake concentration in a few pools, risking centralization. Conversely, if k is too large, individual pools may struggle to earn sufficient rewards, undermining sustainability and network efficiency.

C. Nakamoto Coefficient

In relation to this reward design, the Nakamoto coefficient is used as a quantitative metric to assess overall network decentralization [8].

The Nakamoto coefficient indicates the minimum number of entities required to control over 50% of the stake or computing power in the network. In PoS networks like Cardano, it serves as a measure of stake distribution. A higher Nakamoto coefficient implies a greater number of independent entities involved in decision-making, thus reflecting a healthier level of decentralization.

D. Delegation and Saturation

The delegation and saturation mechanisms are closely related to the aforementioned reward structure. Each stake pool has a saturation point, calculated based on the parameter k and the total stake across the network, as shown in Eq. 1. When a pool exceeds its saturation point, no additional rewards are granted for the stake beyond that threshold—the total rewards for the pool become capped. As a result, delegators are incentivized to choose smaller pools to maximize their rewards, thereby promoting stake distribution.

In this way, the design of the reward system, delegation behavior, and the setting of k are closely interrelated and exert significant influence on overall network decentralization.

III. Related Work

A substantial body of theoretical and empirical research has been conducted on reward design and decentralization assessment in PoS blockchains. This section provides an overview of mathematical models related to Cardano's reward scheme, quantitative evaluations of fairness and decentralization in PoS systems, and empirical studies using on-chain data, thereby clarifying the position of this study.

Brünjes et al. [4] mathematically formulated the stake pool reward design in Cardano and proposed it as the RSS. This model defines reward allocation based on several variables, including stake amount and operator delegation fees, and analyzes participants' strategic equilibria from a game-theoretic perspective. Notably, the parameter k, which indicates the ideal number of pools, plays a central role in balancing network decentralization and economic incentives.

Ovezik et al. [5] quantitatively evaluated stake concentration trends and behavioral shifts of participants through simulations based on the RSS model. They demonstrated how network size and reward settings affect decentralization under a fixed k. However, their study did not address temporal changes in k or analyses based on real on-chain data, thus overlooking the need for flexible parameter tuning in real-world network environments.

Fanti et al. [9] theoretically demonstrated that the compounding effect of capital in PoS can lead to long-term wealth concentration, warning of a loss of fairness due to the "rich-get-richer" phenomenon. They pointed out the structural issue that certain actors could maintain long-term dominance through reward restaking, and emphasized the importance of redistribution mechanisms in reward design.

Almasi et al. [10] collected and analyzed multi-year on-chain data from four major PoS blockchains, such as Tezos, Polkadot, Cardano, and Casper, using quantitative metrics such as the Gini coefficient and Nakamoto coefficient to compare decentralization and fairness. They also introduced the concepts of "Expectational Fairness," which measures alignment with theoretical rewards based on stake, and "Robust Fairness," which measures the distributional deviation between actual and theoretically fair rewards. Their findings suggest that even in relatively mature networks like Cardano, the reward structure may inherently favor centralization.

In addition, Niya et al. [11] and Chegenizadeh et al. [12] empirically analyzed macro-level structural characteristics such as stake pool distribution, delegator behavior, reward allocation, and wealth concentration in the Cardano network. While these studies provide valuable insights into the real-world implications of Cardano's economic design, they do not offer proposals for optimizing or dynamically adjusting protocol parameters—particularly the k parameter.

Brown-Cohen et al. [13] theoretically analyzed the limitations of longest-chain PoS protocols, identifying fundamental challenges such as grinding attacks and selection biases. Their work provides a formal basis for understanding protocol-level vulnerabilities, which indirectly underscores the importance of robust parameterization—such as that of the k parameter—in maintaining network resilience and decentralization.

Building upon these prior works, this study analyzes the practical impact of k adjustment using Cardano's on-chain data. Furthermore, it aims to contribute a novel perspective by developing a future framework for dynamic optimization of k that integrates decentralization, operational costs, and behavioral economic factors.

IV. On-Chain Analysis and Findings

As we have reviewed above, none of the papers have analyzed how k impacted network stability, such as the number of active pools, stake distribution, and the Nakamoto coefficient, and this is the objective of our paper. Our approach builds on prior studies that analyzed Cardano's macro-level network behavior and economic structure [11], [12]. We focus on the event that k was increased from 150 to 500 at epoch 234 in December 2020. This change aimed to enhance network decentralization by increasing the upper limit of the ideal number of stake pools, thereby allowing a larger number of pools to receive (but smaller) rewards.

Table II lists the data collection environment and on-chain metrics that we analyzed.

TABLE II: Experimental Setup and On-Chain Metrics.

(a) Experimental Setup.

Item	Value
CPU	Intel Xeon Gold 6326 @ 2.90GHz
Memory	105.6 GB
Collection Tool	Cardano DB-Sync [14]
Actual DB Size	525 GB
Epoch Range	0 to 547 (Sep 23, 2017 – Mar 20, 2025)
Scope	Restored snapshots only

(b) Metrics Analyzed.

Metric	Description
Active Pools	Pools with nonzero stake
Rewarded Pools	Pools that received rewards
Stake Per Pool	Stake held by each pool
Total Stake	Total amount of staked ADA
Nakamoto Coefficient	Pools needed to control 50% of stake
Normalized Nakamoto	Nakamoto coefficient divided by k

A. Analytical Results

1) Number of Pools: The number of pools involved in staking is a critical indicator of decentralization and competition within the network. We consider both active pools (those with nonzero stake) and reward-receiving pools.

Figure 1(a) shows the number of active stake pools per epoch. A sharp increase in the number of active pools is observed immediately following the change to k at epoch 234 (December 2020). The count peaks between epochs 300 and 350, then gradually declines. This suggests that the change to k initially promoted pool diversification, but over time, market competition led to the elimination of less competitive pools and a trend toward reconsolidation.

Figure 1(b) shows the number of pools receiving rewards per epoch. While a similar increasing trend is observed post-epoch 234, the number stabilizes more quickly than the active pool count.

Comparing Figures 1(a) and 1(b), it is evident that not all active pools receive rewards. This phenomenon is primarily due to insufficient stake and a lack of delegation. Pools with low stake have a lower probability of being selected as slot leaders, which results in no block production and, consequently, no rewards. Furthermore, pools that rely solely on self-stake without meaningful external delegation lack the competitiveness needed to succeed in the network, making it even more difficult for them to earn rewards.

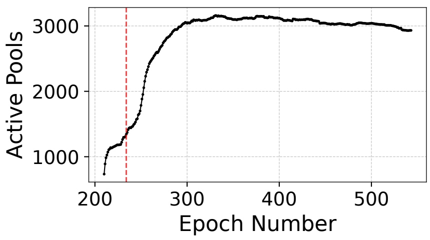
2) Stake Amounts per Pool: Figure 1(c) illustrates the temporal transition of the total stake amount (in ADA) per pool. A substantial decrease in stake per pool is observed immediately after epoch 234, followed by stabilization around epoch 250 for most pools. This trend reflects the protocol update at epoch 234, in which the ideal number of pools k was increased from 150 to 500, thereby reducing the saturation threshold for each pool.

Additionally, the sharp fluctuations observed in the graph suggest temporary movements of large stake amounts. These anomalies may be attributed to misconfigurations or unintended actions by large stakeholders.

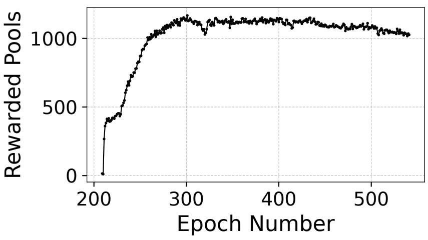
3) Total Network Stake Over Time: Figure 1(d) presents the total staked ADA in the network per epoch. From epoch 200 onward, total stake remains relatively stable between 20 billion and 25 billion ADA. This reflects a generally stable staking foundation across the network.

Despite temporary fluctuations in some epochs, the long-term trend indicates consistent participation, suggesting effective incentive mechanisms and user trust.

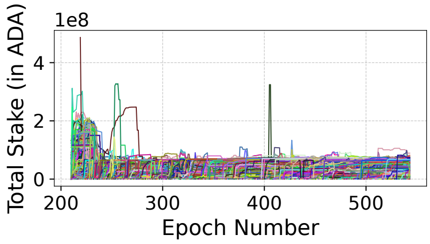
Moreover, although overall stake volume remains steady, the variability seen in Figure 1(c) shows that stake distribution continues to shift between pools, even while aggregate totals remain stable.



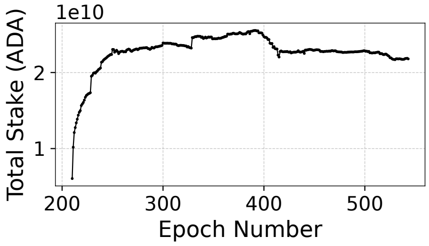
(a) Active stake pools per epoch. The red dashed line indicates the change of parameter k from 150 to 500 at epoch 234.



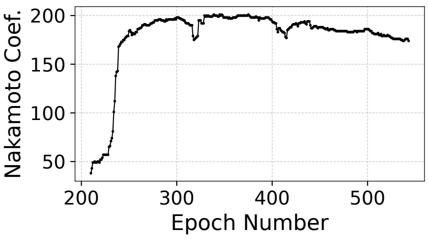
(b) Reward-receiving pools per epoch.



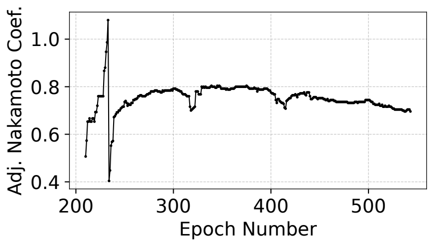
(c) Stake amount per pool over time (in ADA).



(d) Total staked ADA per epoch.



(e) Nakamoto coefficient per epoch.



(f) Normalized Nakamoto coefficient (adjusted by ideal pool count k).

Fig. 1: Stake pool dynamics, reward participation, stake distribution, and decentralization indicators over time.

4) Nakamoto Coefficient: Figure 1(e) shows the Nakamoto coefficient over epochs, which indicates the minimum number of entities required to control over 50% of the total stake [8]. This metric is formally defined as follows [15]:

$$\mathrm{NC} = \min \left\{ k \in [1, \ldots, n] \mid \sum_{i=1}^{k} s_i > 0.5 \right\}. \tag{2}$$

Here, s_i denotes the share of stake held by the i-th entity in descending order of stake ownership, and n is the total number of entities holding a non-zero amount of stake.

A steep rise is observed after epoch 234, with the coefficient increasing from around 50 to approximately 180. This sharp change likely reflects improved stake distribution following the k adjustment. From epoch 250 onward, the coefficient remains at a high level (175–200), indicating sustained decentralization.

Figure 1(f) displays the Nakamoto coefficient normalized by the ideal number of pools k. This adjustment provides a consistent basis for evaluating decentralization regardless of k changes.

To formalize this, we define the normalized Nakamoto coefficient for epoch e as:

$$\mathrm{NormalizedNC}_e = \frac{\mathrm{NC}_e}{k_e}. \tag{3}$$

Here, NC_e denotes the Nakamoto coefficient at epoch e, and k_e represents the protocol parameter for the ideal number of pools at that time.

Around epoch 234, the normalized Nakamoto coefficient fluctuated significantly. However, before and after that period, it remained roughly within the range of 0.7 to 0.8. This suggests that prior to the change in the ideal number of pools k, users were preparing for the adjustment by increasing the number of pools, and after the change, delegators quickly shifted to new pools. This noticeable fluctuation can be largely attributed to the sudden increase of k from 150 to 500. Because not all stakeholders adjusted their allocations immediately, a temporary imbalance would appear before delegation patterns gradually stabilized.

A slight downward trend in later epochs may indicate gradual stake centralization or widening performance gaps among pools. Nevertheless, the coefficient stays above 0.7, suggesting that the network retains a healthy degree of decentralization.

Using this normalized metric enables more nuanced and fair comparisons of decentralization under different k configurations.

V. Future Direction

The current configuration of $k = 500$ in Cardano has no rigorous theoretical foundation and was chosen based on practical and empirical considerations. However, as the network continues to evolve, its structural conditions, including the number of nodes, stake distribution, and propagation delays, are expected to change over time. A static value of k may fail to accommodate such dynamic conditions, potentially leading to inefficiencies or suboptimal levels of decentralization. We therefore assert that k should be adaptively adjusted according to network state. To enable this, a formal evaluation framework for k is essential, along with an optimization model that integrates relevant on-chain metrics.

To address the static nature of the ideal pool number k, we plan to develop a formal evaluation framework that captures key network characteristics. This includes metrics such as decentralization level (e.g., Nakamoto coefficient), operational costs for pool operators, and block propagation delays. These metrics will serve as components of an objective function to guide the optimization of k.

Based on this formulation, we will construct an optimization framework that determines the most suitable value of k given current network conditions. Our long-term goal is to design a dynamic control mechanism for k that continuously adapts to on-chain observations.

Furthermore, to ensure the robustness and social acceptability of the optimized k, future models will also incorporate factors such as user behavior, economic incentives, and possible cognitive biases. Through this approach, we aim to contribute to the development of sustainable, fair, and decentralized PoS blockchain architectures.

VI. Conclusion

This study empirically examined the impact of Cardano's protocol parameter k, which determines the ideal number of reward-receiving stake pools. By analyzing longitudinal on-chain data, we observed that the increase in k from 150 to 500 led to an immediate rise in the number of active pools and the Nakamoto coefficient, indicating improved decentralization. However, these effects gradually tapered off, suggesting that a static k may be insufficient to sustain decentralization over time.

Our findings highlight the importance of a dynamic, data-driven approach to protocol parameter tuning. In particular, k should be adaptively optimized in response to changes in stake distribution, pool competitiveness, and broader network conditions. To this end, we proposed a framework that incorporates social welfare considerations, operational costs, and behavioral economics.

Through this approach, we aim to contribute toward the design of more resilient and equitable Proof-of-Stake ecosystems. Future work will formalize this optimization framework and evaluate its applicability using real-time network data.

Acknowledgment

This work was supported in part by the Japan Society for the Promotion of Science (JSPS) KAKENHI (B) under Grant 24K02931, Japan.

References

[1] F. Saleh, "Blockchain without waste: Proof-of-stake," *The Review of Financial Studies*, vol. 34, no. 3, pp. 1156–1190, 2021.

[2] A. Kiayias, A. Russell, B. David, and R. Oliynykov, "Ouroboros: A provably secure proof-of-stake blockchain protocol," in *Proc. of Annual International Cryptology Conference (CRYPTO)*. Springer, 2017, pp. 357–388.

[3] V. Bagaria, A. Dembo, S. Kannan, S. Oh, D. Tse, P. Viswanath, X. Wang, and O. Zeitouni, "Proof-of-stake longest chain protocols: Security vs predictability," in *Proc. of ACM Workshop on Developments in Consensus*, 2022, pp. 29–42.

[4] L. Brünjes, A. Kiayias, E. Koutsoupias, and A. P. Stouka, "Reward sharing schemes for stake pools," in *Proc. of IEEE European Symposium on Security and Privacy (EuroS&P)*, Sep. 2020, pp. 256–275.

[5] C. Ovezik and A. Kiayias, "Decentralization analysis of pooling behavior in Cardano proof of stake," in *Proc. of International Conference on AI in Finance (AIF)*, Nov. 2022, pp. 18–26.

[6] D. Kahneman, A. Tversky *et al.*, "Prospect theory: An analysis of decision under risk," *Econometrica*, vol. 47, no. 2, pp. 363–391, 1979.

[7] A. Tversky and D. Kahneman, "Advances in prospect theory: Cumulative representation of uncertainty," *Journal of Risk and Uncertainty*, vol. 5, no. 4, pp. 297–323, 1992.

[8] Q. Lin, C. Li, X. Zhao, and X. Chen, "Measuring decentralization in bitcoin and ethereum using multiple metrics and granularities," in *Proc. of IEEE International Conference on Data Engineering Workshops (ICDEW)*. IEEE, 2021, pp. 80–87.

[9] G. Fanti, L. Kogan, S. Oh, K. Ruan, P. Viswanath, and G. Wang, "Compounding of wealth in proof-of-stake cryptocurrencies," in *Proc. of International Conference on Financial Cryptography and Data Security (FC)*, Feb. 2019, pp. 42–61.

[10] S.-N. Li, F. Spychiger, and C. J. Tessone, "Reward distribution in proof-of-stake protocols: A trade-off between inclusion and fairness," *IEEE Access*, vol. 11, pp. 134 136–134 145, Nov. 2023.

[11] S. R. Niya, I. Mesić, G. Anagnostou, G. Brunini, and C. J. Tessone, "A first analytics approach to cardano," in *Proc. of IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. IEEE, 2023, pp. 1–5.

[12] M. Chegenizadeh, S.-N. Li, and C. J. Tessone, "Towards a deeper understanding of the cardano macro-economics," in *Proc. of IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. IEEE, 2024, pp. 585–593.

[13] J. Brown-Cohen, A. Narayanan, A. Psomas, and S. M. Weinberg, "Formal barriers to longest-chain proof-of-stake protocols," in *Proc. of ACM Conference on Economics and Computation (EC)*, 2019, pp. 459–473.

[14] Intersect MBO, "Cardano DB-Sync," https://github.com/IntersectMBO/cardano-db-sync, 2024, accessed: Jul. 29, 2025.

[15] C. Ovezik, D. Karakostas, M. Milad, D. W. Woods, and A. Kiayias, "Sok: measuring blockchain decentralization," in *International Conference on Applied Cryptography and Network Security*. Springer, 2025, pp. 184–214.