Proof-of-Stake Cryptoeconomics Design: A General Framework of Modeling and Evaluation

Sheng-Nan Li[a,b], Jiahua Xu[c,d], Paolo Tasca[c,d], Claudio J. Tessone[a,b]

[a]Blockchain and Distributed Ledger Technologies Group, University of Zurich, Switzerland
[b]UZH Blockchain Center, University of Zurich, Switzerland.
shengnan.li@uzh.ch, claudio.tessone@uzh.ch
[c]Centre for Blockchain Technologies, University College London, UK.
jiahua.xu@ucl.ac.uk, p.tasca@ucl.ac.uk
[d]Exponential Science Foundation.

December 26, 2024

Abstract

Proof-of-Stake (PoS) has gained huge traction in the past years due to its energy-saving advantage compared to the older Proof-of-Work mechanism. By its "plutocratic" nature, it requires a more intricate economic design to ensure its resilience and safety. In this paper, we establish a generalizable, transferable PoS framework that encompasses the interactions and relationships between protocol reserves, treasury, reward pot and transaction fees and staking rewards. With appropriate specifications and configurations, we are able to apply the model to two major PoS protocols: Hedera and Cardano. The dynamic model can inform us of protocol trajectories, including the evolution of the treasury and reserve balances as well as the level of decentralization. Our framework serves as a handbook to investigate the staking behaviors and reward dynamics with the concomitant effects on the crypto economics of various PoS-based systems.

Funding: This research was supported by Exponential Science Foundation, and Cardano Foundation.

Keywords: Proof-of-Stake, Cryptoeconomics, Agent-based Modeling, Incentives Design, Decentralization

1 Introduction

With the rising adoption of blockchain technologies, Proof-of-Stake (PoS) consensus mechanisms have gained increasing attention as an energy-saving alternative to Proof-of-Work (PoW) (Tasca and Tessone 2019, Spychiger et al. 2021, Dimitri 2021). While PoW remains one of the oldest and most straightforward consensus mechanisms, PoS introduces a more nuanced and sophisticated approach. In PoW systems, miners compete to solve computationally intensive puzzles, and the first to successfully propose a block is rewarded with cryptocurrency. This process is inherently simple in its economic design: work is directly tied to reward. In contrast, PoS mechanisms rely on stakeholders locking a certain amount of cryptocurrency as a signal of their commitment to the network. This foundational concept has given rise to a wide spectrum of variations—each with distinct roles, incentives, and validation processes—such as pure Proof-of-Stake (e.g. Algorand) (Gilad et al. 2017), Delegated Proof-of-Stake (DPoS) (e.g. EOS, Cardano) (Kiayias et al. 2017), Liquid Proof-of-Stake (e.g., Tezos) (Goodman 2014), and Nominated Proof-of-Stake (NPoS) (e.g., Polkadot) (Nguyen et al. 2019). Each variant entails unique roles, such as validators, attestants, delegators, stakers, and nominators, forming a complex web of interactions and incentives.

The security and sustainability of PoS protocols depend on various factors, among which the incentive mechanism is vital. On the one hand, the reward scheme must incentivise consensus participation by rewarding block proposers and related validators (Luu et al. 2015). To avoid the operational cost of always being online, some variants of PoS, like DPoS and NPoS, mimic parliamentary democracy systems, where users (delegators or nominators) can delegate their "vote" using their tokens for a set of validator candidates, thereby increasing a candidate's chances of validating a block and receiving rewards. Generally, PoS incentive mechanisms are designed to ensure that the protocol properly outweighs the economic gains from malicious behavior (Xiao et al. 2020).

The inherent flexibility and degrees of freedom in PoS designs present both opportunities and challenges. While the diversity allows for tailored solutions that optimize for scalability, security, or decentralization, it also increases the complexity of understanding, comparing, and evaluating different systems. Unlike PoW, where the relationship between effort and reward is linear and easily understood, PoS mechanisms require a detailed analysis

of economic incentives Cong et al. (2023), participant behaviors, and the interplay between roles and rewards. Each PoS protocol typically includes a set of parameters, such as profit margin, fee, saturation, and inflation rate, which can impact various aspects of the protocol, including Annual Percentage Yield (APY), decentralization, and inequality (Roşu and Saleh 2020, Wang et al. 2020).

However, the extent to which each parameter affects various aspects of PoS cryptoeconomics remains underexplored, with limited causal and quantitative insights available in existing research. To address this gap, this paper proposes a general modeling framework designed to provide a more detailed understanding of the cryptoeconomic dynamics in PoS networks. Our approach begins by identifying the core components that characterize PoS cryptoeconomics, creating a foundation for evaluating key protocol elements. We illustrate this framework using Cardano and Hedera as case studies, showcasing how specific PoS protocols can be modeled and evaluating essential aspects such as monetary dynamics and inequality in reward distribution.

Cardano employs the Ouroboros protocol (Kiayias et al. 2017), which is based on a rigorous academic foundation and emphasizes energy efficiency, provable security, and decentralization. Its mechanism is designed to balance validator selection, stakeholder engagement, and reward distribution. Hedera, on the other hand, utilizes the Hashgraph consensus, a novel approach that combines weighted stake-based voting with a gossip-about-gossip protocol (Baird et al. 2018). This design prioritizes high throughput and fairness while maintaining low-latency consensus. By analyzing these two systems, we highlight the diversity in PoS mechanisms and demonstrate the utility of a unified framework for understanding their cryptoeconomic structures.

The framework we present offers a systematic approach to understanding the intricate relationships among protocol parameters, guiding the design of these elements, and revealing the behavior patterns of network participants. By facilitating an evaluation of the interconnected effects of protocol parameters, this work provides a robust foundation for assessing the performance of blockchain systems, ultimately contributing to more informed and effective PoS protocol design.

2 Literature

The PoS consensus mechanism has significantly addressed inefficiencies inherent in the original PoW model, as discussed by Nguyen et al. (2019). Because it is competition-based, PoW is exposed to a variety of departures

from conformant behavior (Eyal and Sirer 2018, Gans and Halaburda 2024). Li et al. (2024) further underscored vulnerabilities of PoW in its mechanism, demonstrating that majority attacks can be profitable and have been identified in the real world. Buterin and Griffith (2017) introduced a PoS-based finality system, "Casper", to ensure finality and provide greater protection against long-range attacks. Dimitri (2021) delved into the PoS monetary dynamics, illustrating that the aggregate demand and supply of currency may not always align, raising concerns about long-term stability and wealth distribution within PoS systems.

In this context, inequalities in reward distribution have been critically examined. Li et al. (2023) analyzed PoS platforms such as Tezos, Polkadot, Cardano Casper, as well as Ethereum 2.0 (Yan et al. 2024) revealing that these systems face wealth centralization - except for Polkadot. Their analysis also examined from the stake-reward fairness perspective, concluding that the implementation approach of PoS significantly influences such fairness. Additionally, Wang et al. (2020) explored the concept of incentive compatibility within PoS protocols, emphasizing how system design influences participant motivation. Schwarz-Schilling et al. (2023) further advanced this argument by demonstrating that optimized reward mechanisms can simultaneously enhance equitability and incentive compatibility. This insights align closely with the broader need to understand participant behavior within PoS ecosystems.

A thorough review of blockchain consensus protocols by Xiao et al. (2020) highlighted differences in fault tolerance, scalability, and suitable application scenarios using a five-component framework. Scaling challenges, particularly in high-throughput environments, were addressed by Gilad et al. (2017), who demonstrated how the new Byzantine Agreement (BA) protocol and Verifiable Random Functions can improve transaction throughput and scalability. Similarly, the work of Luu et al. (2015) focused on overcoming the verifier's dilemma and shed light on incentives required for correct computation validation in PoS networks.

Expanding on these technical concerns in PoS, Roşu and Saleh (2020), Kiayias et al. (2017) delved into cryptoeconomic aspects, specifically examining whether wealth centralization is inevitable in PoS networks. Their finding revealed that, in the absence of trading, wealth distribution tends to stabilize over time, contradicting the common notion that the rich always get richer. These studies underscore the importance of considering both economic stability and fairness in PoS systems alongside technical challenges like scalability and security.

Proof-of-Stake (PoS) offers a wide range of design choices, particularly in how rewards are distributed. These design choices do not merely deter-

mine short-term performance, but also reshape the macro-properties of the system's economy, influencing participant incentives and ultimately determining the platform's long-term viability and fairness. Building on these insights, it becomes clear that the design of PoS systems must address not only technical scalability and security but also economic behavioral factors. While earlier work has explored solutions to specific challenges like transaction throughput, wealth distribution, and validator incentives, a broader perspective is required to address the interplay of these factors effectively.

To address these interconnected challenges, we propose a modeling framework to examine various dimensions of cryptoeconomics, focusing on monetary dynamics and reward distribution inequalities. By quantitatively assessing the interactions among protocol factors, this framework aims to contribute to the development of more sustainable and equitable PoS networks.

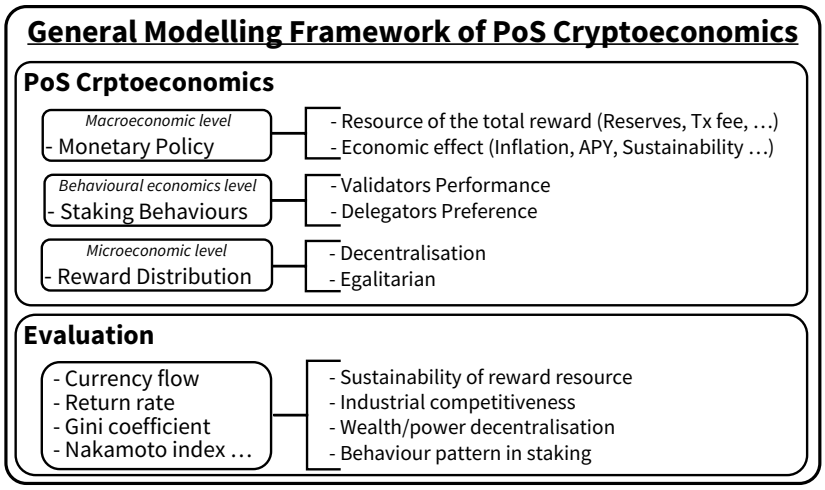


Figure 1: General PoS modeling framework

3 Mutiple aspects of proof-of-stake cryptoeconomics

As shown in the Figure 1, in our framework, we split the PoS cryptoeconomics into three main parts:

- **Monetary policy (macroeconomic level):** Monetary policy governs the issuance rate of new tokens, directly influencing the inflation rate, currency stability, token liquidity, and market expansion. This level shapes the staking incentives that drive network participation.

Depending on the specific monetary policy, the total rewards per period can be structured around various parameters: expected annual percentage yield on staked tokens, a fixed inflation rate on the circulating supply, or amount of reward sources such as transaction fees.

- **Staking Behavior (behavioral economics level):** We focus on modeling participants' rational behavior patterns to assess their impacts on network security and decentralization. Staking behavior involves two primary types of actions. First is the performance of validators, which varies based on individual strategies, participation rate, reward returns, etc. Second, we consider the preferences of delegators, who base their staking choices on the "trust" they place in specific validators. This trust may be influenced by validators' track records, perceived reliability, and reputation within the network. Together, these behaviors play a critical role in fostering network resilience and decentralization by affecting both the distribution of staked assets and overall participant engagement.

4 Main measurements of Proof-of-Stake cryptoeconomics

Our framework enables the measurement of key metrics that characterize the PoS system's economic and security dynamics. Specifically, it assesses currency flow, return rate, and the distribution of stake and rewards using the Gini index to gauge equality within the system. Additionally, it evaluates the decentralization of power through the Nakamoto Coefficient. Together, these metrics provide valuable insights into the stability and sustainability of the network, highlighting potential vulnerabilities and guiding improvements in protocol design.

4.1 Currency Flow

The currency flow within a PoS system is usually governed by the dynamics between Reserve and Treasury, structured in alignment with the protocol's monetary policy design. The reserve serves as the primary source of reward, issuing new tokens into the system based on predefined issuance rates. This steady issuance supports transaction activity and staking rewards while incentivising ongoing participation in the network and maintaining token value.

The Treasury plays a dual role within the system. First, it acts as an adjuster to help regulate inflation by controlling the rate of token distribu-

tion and maintaining a stable economic environment. Second, it serves as a buffer, allowing the system to set aside reserves for future development, anticipated growth, and unforeseen risks. This buffering capacity is essential for sustaining the network, as it provides the resources necessary for handling unforeseen risks and supporting long-term sustainability.

4.2 Reward rate

The reward rate acts as a common market signal, enabling stakeholders to compare the attractiveness of different networks. This comparison is essential for guiding investment decisions, as it provides insights into the potential returns and relative stability of each network. However, the reward rate is never the higher the better. While a high reward rate can attract investors by promising greater returns, it also carries inherent risks. An elevated reward rate can lead to increased token issuance, which, if not carefully managed, may drive inflation and reduce the token's value over time. This inflationary pressure can erode the purchasing power of rewards, diminishing the long-term value for stakeholders. Additionally, a high reward rate may encourage speculative participation rather than a genuine, long-term commitment to the network, potentially increasing volatility and reducing network stability. If reward rates outpace sustainable economic growth, the network may struggle to maintain token value and attract dedicated participants, ultimately compromising its resilience and security.

4.3 Inequality: Gini index

The Gini index is the most frequently used inequality index of income or wealth distribution among a nation's residents Dalton (1920). Therefore, we borrow this convention to analyze the equality for wealth distributions of cryptocurrencies under the influences of specific reward mechanisms. The Gini index can theoretically range from 0 (complete equality) to 1 (complete inequality), and is given by,

$$G = \frac{\sum_{i=1}^{N} \sum_{j=1}^{N} |x_i - x_j|}{2N \sum_{i=1}^{N} x_i} \tag{1}$$

where x_i is the wealth or income of an agent i, and there are N agents.

4.4 Decentralization: Nakamoto Coefficient

The Nakamoto coefficient (Lin et al. 2021) is defined as the minimum number of entities required to collude for gathering over 50% of the overall mining

power p to compromise a blockchain system, which could be computed via:

$$N = \min \left\{ k \in [1, 2, ..., K] : \sum_{i=1}^{k} p_i \geq 0.51 \right\} \tag{2}$$

We use this approach to calculate the Nakamoto coefficient based on the 50% threshold of stake controlled by a minimum amount of validators. A higher Nakamoto coefficient indicates greater decentralization, as it suggests that control is distributed among a larger number of entities.

5 Use cases

The framework can be applied to various blockchains. In this section, we examine its applicability in particular to Cardano and Hedera.

5.1 Cardano

Cardano (Kiayias et al. 2017), whose native cryptocurrency is ADA (*ada*), implements delegated PoS via stake pools. Stake pools are operated by so-called pool operators who act as validators. Then delegators can add their stake to a stake pool of their choice. Cardano divides times into epochs, where each epoch consists of 432,000 slots (5 days). The algorithm then randomly selects zero or multiple validators from all stake pools that can add the next blocks to the blockchain. This selection is proportional to the staked coins in the stake pools. According to the protocol design, there is no slashing in Cardano. The system rewards the stake pools (validators) based on their activity and participation, not only on a block basis. Besides block-specific transaction fees, stake pools are rewarded by funds from the ADA-reserve (a certain percentage is allocated as a reward in each epoch). These funds are distributed among the stake pools and its delegators, that participated in slots, proportionally to their stakes. To counteract large stake pools, the protocol defines a saturation threshold for the maximal stake. Above this threshold, the rewards are decoupled from the stake and remain constant.

5.2 Hedera

Hedera, whose native cryptocurrency is hbar ($\hbar$), is a permissioned network that uses a directed acyclic graph (DAG)-based data structure to store the transaction history and applies PoS. The network has its consensus nodes run solely by its council members at the moment, with the plan to open

up to permissionless nodes in the future. That's why better simulating the system's PoS protocol design is more beneficial to the governance decision to warn the risk earlier and update the parameters efficiently, However, it is possible to do proxy staking to a council node, which receives rewards and then share them with the delegators. Rewards diminish with the size of the total stake if a node has a total stake that exceeds a cap maximum parameter. And the rewards are distributed on a daily (24-hour) basis.

6 Modeling

The details of the modeling framework are illustrated in Figure 2. In alignment with multiple aspects of proof-of-stake cryptoeconomics, our model encompasses all the key components mentioned above in section 3. First, monetary policy governs the planning of total rewards for each reward period. Second, staking behavior captures the dynamic selection relationships between validators and delegators, modeling how these roles interact within the network. Third, reward distribution allocates rewards according to the system's predefined policies, ensuring that incentives align with network goals.

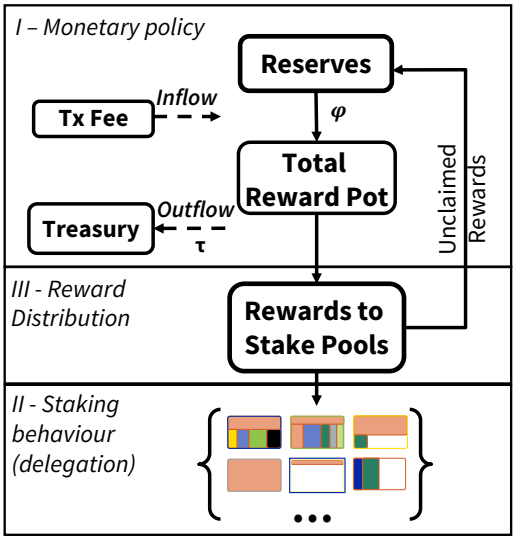


Figure 2: Modeling Process

6.1 Generalization of monetary policy

In designing a monetary policy for any new PoS-based protocol or dissecting it for the existing system, it is helpful to structure the reward plan around

two main components: Inflow and outflow of the total reward pot. The inflow generally consists of transaction fees collected from network participants and tokens released from the system's reserve, which together contribute to the reward pot available for distribution. On the other hand, outflow typically includes allocations to the Treasury, where a portion of rewards is set aside for future development, operational costs, and contingency planning.

This general approach provides a flexible framework that can be adapted to various PoS protocols, allowing protocol designers to balance immediate rewards with long-term sustainability. For instance, in Figure 3, we compare the specific inflow and outflow structures of Hedera and Cardano, illustrating how each protocol implements distinct approaches to managing their monetary policy and reward distribution. In the Hedera system, the current allocation of fees is that $\tau = 90\%$ flows to the treasury (account, 0.0.900), and the other 10% flows to the staking account, which acts the same as a reserve (account, 0.0.800). The daily money issuance rate φ is determined by a few variables including the amount of active stake for reward as well as the current balance of reserve relative to a target balance (85 million $\hbar$). The actual is basically as follows,

$$\varphi(\pi, \sigma) = \frac{2.5\%}{365} \times \frac{\sigma_0}{\max(\sigma_0, \sum \sigma)} \times \pi \times (2 - \pi) \tag{3}$$

where 2.5% is the base reward rate multiplied by $\pi = \frac{\min(r_t, r')}{r'}$. r_t is the current reserve balance, and $r' = 85$ million $\hbar$ is the target reserve balance for the base reward rate. $\sum \sigma$ is the actual active stake, and $\sigma_0 = 6.5$ billion $\hbar$ the minimum threshold of reward stake. Thus, the amount of token outflow from a reserve used to pay the reward equal $\varphi(\pi, \sigma) \times \sum \sigma$.

In the Cardano system, the monetary policy is simpler, because both the φ and τ are set as fixed parameters. (More details about the value of parameters in the model are shown in the following Table 1.)

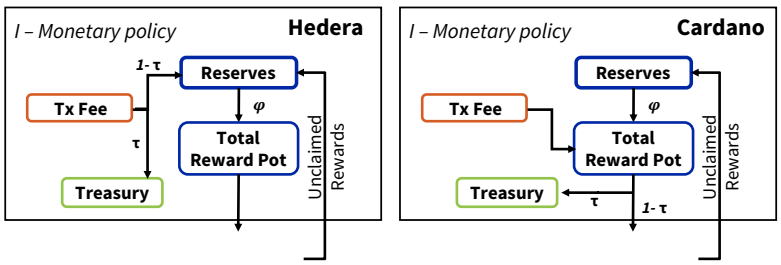


Figure 3: Modeling of the monetary policy of Cardano and Hedera

6.2 Staking Selection between Validators and Delegators

6.2.1 Validators' Performance and Saturation

The security of the PoS staking ensures the most power is controlled by the honest participants. Casper (Buterin and Griffith 2017) is proven to be secure as long as 2/3 of the voting power is controlled by honest validators in a partially synchronous network. Algorand (Gilad et al. 2017) is proven to be safe as long as 51% of the total stake is controlled by honest participants because the committee votes to finalize every block, i.e., there is no fork. Therefore, the PoS protocol should always encourage the stake flows to validators with good behavior which could be defined as the *participation level*. From the modeling language, at the end of every reward period, the validators with good enough behaviors are those who have met the threshold of the *participation level*. They will be able to receive the reward. The participation threshold $\rho \in (0, 1)$ is an exogenous parameter set to be `constant` over time. $\rho(v)_t$ is the specific participation level of each validator $v \in \mathcal{V}$ in the t-round reward period. The validators v can be involved in the reward distribution at time t, if

$$\rho(v)_t \geq \rho \tag{4}$$

We reasonably assume that the participation level of validator v is positively affected by the quality level of the specific technology chosen. (In the current version of the manuscript, for the sake of simplicity, we assume the technology quality of certain validator's computing device is constant over time.)

It is worth noting that to ensure the security and decentralization platforms always use different parameters to avoid that stake centralisation in certain nodes, like the maximum cap or saturation threshold of the total receiving stake, as well as the oversubscribed number of delegators and so on. Using the maximum cap as a representation, it means the delegator's reward might be diluted if the validator of his pool received too much stake that excess the maximum cap, the more the validator excess the maximum cap, the more his delegator's reward will be diluted. Thus, the delegators (stakers) might have the incentive to choose the validator with higher `reward rate` for stakers, $r(v)_t$. These incentives can be captured by the following

equation:

$$r(v)_t = \begin{cases} 0 & \text{if } b(v)_t < C(v)_t^{\text{MIN}} \\ 1 & \text{if } C(v)_t^{\text{MIN}} \leq b(v)_t \leq C(v)_t^{\text{MAX}} \\ \dfrac{C(v)_t^{\text{MAX}}}{b(v)_t} & \text{if } b(v)_t > C(v)_t^{\text{MAX}} \end{cases} \tag{5}$$

where $b(v)_t$ is the total receiving stake of validator v at period t. C_t^{MIN} and C_t^{MAX} are separately the **minimum threshold** and **maximum cap** of the total stake. If the total staked amount is below the minimum threshold, then they get no reward. And if the total stake exceeds the maximum cap the reward will be diluted.

6.2.2 Delegators' Preference

In each reward period, delegators decide on which nodes to stake their balance. In most real platforms, to ensure the proportional justified representation (Sánchez-Fernández et al. 2017), the system assigns each delegator d ($d \in \mathcal{D}$) to choose only one validator v to stake the available balance. So it's reasonable to assume that delegators do not split their balance among multiple validators.

Delegators's selection is based on an exponential "memory" function of validators' historical participation level $\rho(v)_t$ (Equation 4) and the reward rate $r(v)_t$ (Equation 5). Then, at each time t we iterate the delegator selection process by mixing the following two probabilities:

- $\mathbb{P}_\rho(v)$ is the probability that delegator s select validator v based on their participation level

$$\mathbb{P}_\rho(v) = \frac{\sum_{t'=0}^{t} \exp\left(-\lambda(t-t')\right) \rho(v)_{t'}}{\sum_{v_i \in \mathcal{V}} \sum_{t'=0}^{t} \exp\left(-\lambda(t-t')\right) \rho(v_i)_{t'}} \tag{6}$$

- $\mathbb{P}_r(v)$ is the probability that delegator s select validator v based on their reward rate.

$$\mathbb{P}_r(v) = \frac{\sum_{t'=0}^{t} \exp\left(-\lambda(t-t')\right) r(v)_{t'}}{\sum_{v_i \in \mathcal{V}} \sum_{t'=0}^{t} \exp\left(-\lambda(t-t')\right) r(v_i)_{t'}} \tag{7}$$

where $\exp\left(-\lambda(t-t')\right)$ is a memory function which assigns weight to the node's participation level and reward rate at time t'; and λ is a discount factor.

Finally, in every reward period t, each validator will then receive a score $\texttt{Score}(v)_t$ based on the combination of the two above memory functions as follows:

$$\texttt{Score}(v)_t = \beta_\rho \big[\mathbb{P}_\rho(v)\big] + \beta_r \big[\mathbb{P}_r(v)\big] + \varepsilon \tag{8}$$

where $\varepsilon \sim U(0, 0.1)$ brings some level of noise as random behavior in the selection process. The $\texttt{Score}[v]_t$ is a (dynamic) probability assigned to node v to be chosen by the stakers at time t. If $\lambda = 1.7$, it considers 30 days of memory $(t - t')$. To keep the reasonable weight of two different factors, β_ρ and β_r are adjustable in the modeling based on specific protocols.

6.3 Reward distribution

The reward distribution to each staking pool in Cardano follows the equation design by the protocol, as follows,

$$f(s, \sigma) = \frac{R}{1 + a_0} \times (\sigma' + s' \times a_0 \times \frac{\sigma' - S' \frac{Z_0 - \sigma'}{Z_0}}{Z_0}) \tag{9}$$

where the parameters are defined as: R is total available rewards for the current period; a_0 is the influence factor of the pledge; Z_0 is relative pool saturation size; σ is the total stake delegated to the pool including stake pledged and delegated by others and S is the stake pledged by the pool owner; $\sigma' = \min(\sigma, Z_0)$ and $s' = \min(s, Z_0)$. Thus, in the modeling, according to Equation 9 the reward should be distributed to the individual staking pool that met the threshold of the participation level (in Equation 4 can be calculated. Then after charging 350 ada as a fixed cost (we didn't consider the margin in the current model), the remainder is split proportional to delegated stake, amongst all stakeholders who delegated to the pool, including the pool owners.

In the Hedera, the reward distribution is relatively simple. The total reward for each day R_t is calculated based on the money issuance rate and total active stake, $R_t = \varphi \times \sum \sigma$. Then the reward will be distributed to individual validators (council node) that met the threshold of the participation level and minimum stake, proportionally to their total stake (stake from delegators and and themselves).

6.4 Parameters

The list of parameters used in the modeling is shown as follows in Table 1.

Parameter	Description	Value
Global:		
a_0	shape value of initial wealth distribution amount all users	1.16 (pareto)
T	total length of simulation time	5 years
λ	discount factor in the memory function	1.7
β_ρ	weight of participation level (ρ) in the score of validator's performance	0.3
β_r	weight of reward rate (r) in the score of validator's performance	0.6
Cardano: (native currency: ADA, *ada*)		
	simulation starting time (1 year after launching PoS, Epoch 283)	Aug. 8. 2021
	initial total stake	23B *ada*
	initial balance of reserve	12B *ada*
	initial total circulating supply	37B *ada*
$\mathcal{V}$	total number of validators	3000
$\mathcal{D}$	total number of delegators	27000
φ	fixed percentage of money issued from the reserves	0.0003
τ	certain percentage of outflow pot sent to the treasury	0.2
$Z_0 = C^{MAX}$	staking pool saturation (maximum amount of pool's total stake)	0.002
C^{MIN}	minimum amount stake for a pool to receive reward	0
α_0	influence factor of the pledge	0.3
ρ	participation threshold	0.9
Hedera (native currency: Hbar, $\hbar$)		
	simulation starting time	Aug.12.2024
	initial total stake	7B $\hbar$
	initial balance of reserve (reward account: 0.0.800)	4M $\hbar$
	fixed total supply	50B $\hbar$
$\mathcal{V}$	total number of validators	30
$\mathcal{D}$	total number of delegators	300
φ	percentage of money issued from the reserves	2.5% (base rate)
τ	certain percentage of outflow to the treasury	0.9
C^{MAX}	staking saturation (maximum amount of validator's total stake)	1.67B $\hbar$
C^{MIN}	minimum amount stake for a pool to receive reward	0
ρ	participation threshold	0.5

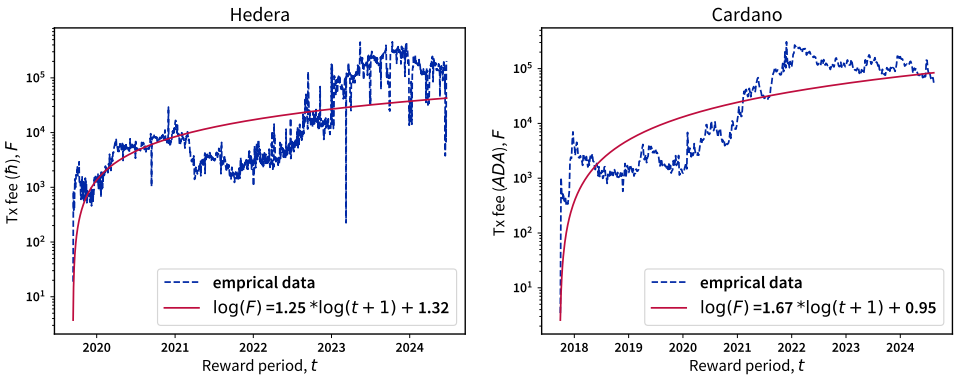
Table 1: Parameters Table for PoS Modeling implemented in Cardano and Hedera

7 Results

7.1 Fitting of the transaction fee

Given that the transaction fee contributes to the total reward in both the Hedera and Cardano systems, modeling historical transaction fee trends can improve the accuracy of transaction fee forecasts and, consequently, enhance the precision in calculating total rewards. The fitting results are shown in Figure 4.

The growth of transaction fees in both systems can be relatively well-fitted with a log-log model. Despite the distinct technologies and mechanisms of Hedera and Cardano, the two systems suggest a similar scale of total transaction fees in their native tokens. As shown by the fitting equations in Figure 4a and Figure 4b, the transaction fees in Cardano might grow at a slightly faster rate over time compared to Hedera.



(a) Hedera (b) Cardano

Figure 4: Fitting of the growth of transaction fee

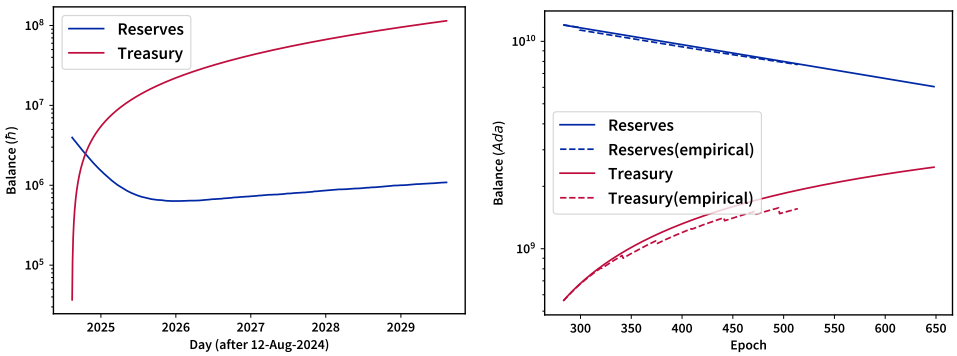
7.2 Dynamic of Monetary Policy

With the network growth at the currently predicted trajectory, disregarding non-staking related spending and income, our model simulates the reward process over 5 years for both two systems, and the dynamic of the balance of treasury and reserve for both Hedera and Cardano are shown in Figure 5a and Figure 5b separately.

In Hedera, the trends are over days, starting from August 12, 2024). In Cardano, trends are shown across epochs, with a comparison between model simulation and empirical data for both reserves and treasury. The close alignment between the model and empirical data indicates that our model captures the essential dynamics of the system's monetary policy with high accuracy.

Both systems maintain distinct treasury balances, but the trends over time or epochs might reveal differences in how each system prefers to manage its treasury funds in response to network growth or operational costs. Cardano's higher fund in the reserve at the beginning may help attract more investment by providing a relatively higher reward. However, Hedera's stability-focused mechanism could mitigate the system's risks associated with fluctuating transaction volumes or token value, potentially supporting a more sustainable economy.

These trends in treasury and reserve balances suggest differences in the mechanisms governing monetary policy in each network. Cardano aims to ensure sufficient funds for potentially higher returns, while Hedera's stability-focused model emphasizes predictability. These contrasting approaches provide a basis for comparing monetary policies in blockchain networks, highlighting the sustainability of blockchain ecosystems.



(a) Hedera (b) Cardano

Figure 5: Dynamics of the balance of treasury and reserve

7.3 Return rate

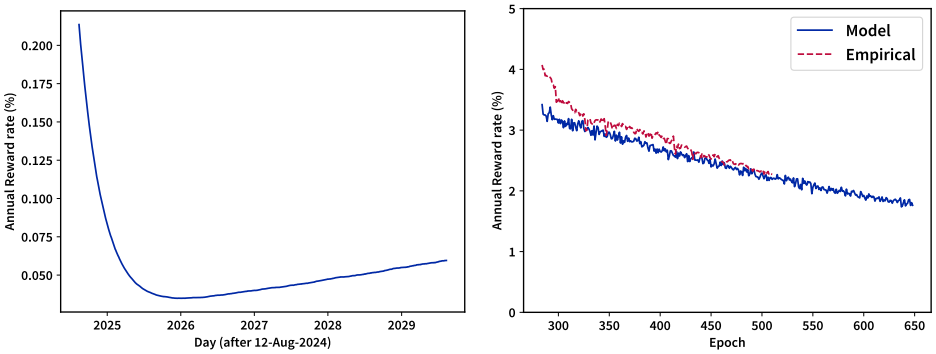
To assess the effectiveness of staking rewards and monetary policy sustainability, we calculate the annual percentage yield (APY) for both Hedera (as shown in Figure 6a) and Cardano (as shown in Figure 6b).

The staking annual reward rate for Hedera, shown over time in days, fluctuates within a low range of approximately 0.2% to the bottom point lower than 0.05%. This reflects a conservative, stable reward structure. The higher reward range for Cardano suggests attractive yields combined with a steady monetary policy. Our model simulations closely match the empirical data also in the APY index, indicating that the model reliably captures the actual reward dynamics.

Hedera's lower APY range offers a reliable, conservative return, supporting a steady but modest growth strategy. Cardano's higher APY range is likely more attractive to yield-seeking participants. These distinct reward rates stem from differing monetary policy designs within blockchain ecosystems: Hedera's low, stable rewards emphasize predictability, while Cardano's higher rate seeks to balance competitiveness and sustainability. This contrast provides valuable insights for analyzing staking incentives and reward mechanisms in various networks.

7.4 Inequality

To assess wealth distribution within Hedera and Cardano, we calculate the Gini index for both periodic rewards and accumulated balances. The Gini index measures inequality, indicating how rewards are distributed across participants. With delegator selection modeled in both systems, this metric



(a) Hedera (b) Cardano

Figure 6: Staking annual reward rate

helps gauge the impact of not only the reward mechanism but also delegators' choices on wealth concentration.

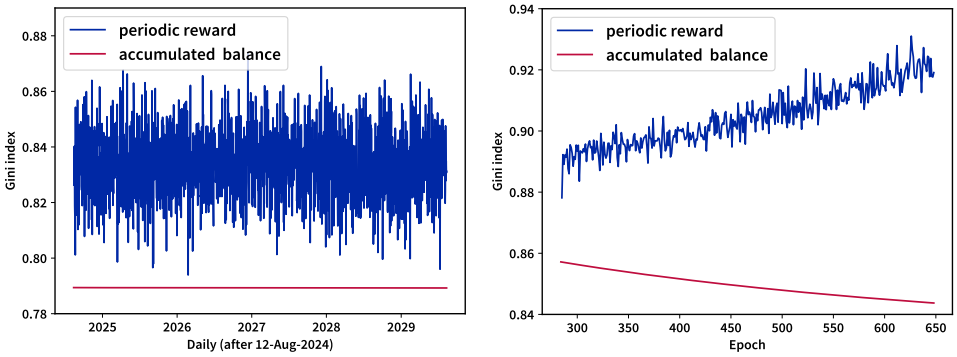
As shown in Figure 7a Figure 7b, both systems exhibit relatively high Gini index values, which shows the inequality reward distribution and wealth concentration. The Gini values at the beginning are largely determined by an initial wealth distribution that follows a Pareto pattern in the model. In Hedera, the Gini index is relatively low. The trend of the gini of periodic rewards distribution is more stable but has larger fluctuation over time. In contrast, Cardano's higher Gini index for periodic rewards shows a gradual increase, indicating growing inequality in reward distribution as the amount of total active stake expands. However, for accumulated wealth, Cardano displays a slight trend toward equality, suggesting that while reward distribution becomes more concentrated, the overall wealth distribution is leveling out slightly over time.

These differences could reveal how delegator selection shapes wealth distribution and the trade-offs in designing staking incentives.

7.5 Decentralization

To understand the degree of decentralization and security in Cardano and Hedera, we calculate the Nakamoto index, which assesses the minimum fraction of validators required to control either 1/2 or 1/3 of the total active stake.

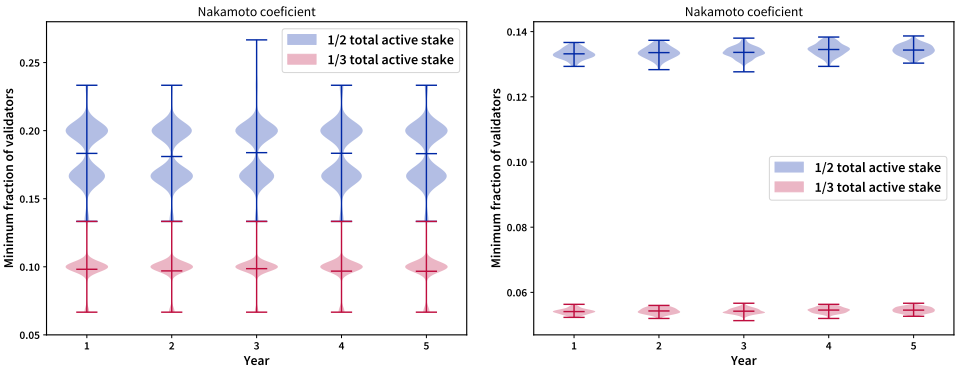
The results shown in Figure 8a and Figure 8b reveal the differences between the two systems. For Cardano, the Nakamoto index remains relatively low over five years, ranging from approximately 0.05 and 0.13 for the 1/2 and 1/3 thresholds. This indicates that 13% of top large staking pools could hold



(a) Hedera (b) Cardano

Figure 7: Gini index of reward and wealth distribution

more than 1/3 of the total stake, suggesting some concentration within the network. In contrast, Hedera's larger value implies that more validators are required to reach critical control thresholds in Hedera, suggesting a relatively more decentralized system.



(a) Hedera (b) Cardano

Figure 8: Nakamoto index of stake distribution

8 Conclusion

In this paper, we introduced a generalized modeling framework for PoS blockchains. In particular, we consider the monetary policy, and reward distribution scheme (all of them being design decisions), as well as modeling the staking behavior of the various agents, and the combined effect on the oevrall network's cryptoeconomics at the macro level. Our framework

is the first attempt to abstract and generalize PoS cryptoeconomics design, which, when adequately configured with certain specifications, can be applied to various PoS implementations. Under this framework, we are able to further simulate the staking and reward dynamics and show the level of decentralization – measured with different metrics – of two example protocols, Hedera and Cardano. We observe similar levels of reward concentration on both systems, with Hedera oscillating around a stationary level, while Cardano slowly tending towards higher level of inequality. In terms of level of decentralization, the fraction of active stakers required to control half of the network is higher in Hedera than with Cardano, suggesting a higher relative level of decentralization with the former than with the latter.

Overall, the proposed framework not only fits well with empirical data but also offers valuable insights into the future trajectory of a network's cryptoeconomic dynamics. By providing a comprehensive approach to understanding PoS systems, this framework can guide the design, evaluation, and comparison of different blockchain protocols, fostering more informed decisions in blockchain governance and development.

9 Acknowledgment

We would like to express our sincere gratitude to The DLT Science Foundation, and Cardano Foundation for their grants to this research. We are also grateful to the Hedera team for their support in providing the datasets analyzed.

References

Baird L, Harmon M, Madsen P (2018) Hedera: A Governing Council & Public Hashgraph Network The Trust Layer of the Internet. Technical report.

Buterin V, Griffith V (2017) Casper the Friendly Finality Gadget. *arXiv:1710.09437* URL `http://dx.doi.org/https://doi.org/10.48550/arXiv.1710.09437`.

Cong WL, He Z, Tang K (2023) The Tokenomics of Staking. Technical report, URL `www.financetheory.com`.

Dalton H (1920) The Measurement of the Inequality of Incomes. *The Economic Journal* 30(119):348–361, ISSN 0013-0133, URL `http://dx.doi.org/10.2307/2223525`.

Dimitri N (2021) Monetary Dynamics With Proof of Stake. *Frontiers in Blockchain* 4:443966, ISSN 26247852, URL `http://dx.doi.org/10.3389/FBLOC.2021.443966/BIBTEX`.

Eyal I, Sirer EG (2018) Majority Is Not Enough: Bitcoin mining is vulnerable. *Communications of the ACM* 61(7):95–102, ISSN 15577317, URL http://dx.doi.org/10.1145/3212998.

Gans JS, Halaburda H (2024) "Zero Cost" Majority Attacks on Permissionless Proof of Work Blockchains. *Management Science* 70(6):4155–4165, ISSN 15265501, URL http://dx.doi.org/10.1287/mnsc.2023.02426.

Gilad Y, Hemo R, Micali S, Vlachos G, Zeldovich N (2017) Algorand: Scaling Byzantine Agreements for Cryptocurrencies. *SOSP 2017 - Proceedings of the 26th ACM Symposium on Operating Systems Principles* 51–68, URL http://dx.doi.org/10.1145/3132747.3132757/SUPPL{_}FILE/ALGORAND.MP4.

Goodman LM (2014) Tezos: A Self-Amending Crypto-Ledger Position Paper.

Kiayias A, Russell A, David B, Oliynykov R (2017) Ouroboros: A provably secure proof-of-stake blockchain protocol. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 10401 LNCS:357–388, ISSN 16113349, URL http://dx.doi.org/10.1007/978-3-319-63688-7{_}12/FIGURES/6.

Li SN, Campajola C, Tessone CJ (2024) Statistical detection of selfish mining in proof-of-work blockchain systems. *Scientific Reports* 14(1), ISSN 20452322, URL http://dx.doi.org/10.1038/s41598-024-55348-3.

Li SN, Spychiger F, Tessone CJ (2023) Reward Distribution in Proof-of-Stake Protocols: A Trade-Off Between Inclusion and Fairness. *IEEE Access* 11:134136–134145, ISSN 21693536, URL http://dx.doi.org/10.1109/ACCESS.2023.3336418.

Lin Q, Li C, Zhao X, Chen X (2021) Measuring Decentralization in Bitcoin and Ethereum using Multiple Metrics and Granularities. *Proceedings - 2021 IEEE 37th International Conference on Data Engineering Workshops, ICDEW 2021* 80–87, URL http://dx.doi.org/10.1109/ICDEW53142.2021.00022.

Luu L, Teutsch J, Kulkarni R, Saxena P (2015) Demystifying Incentives in the Consensus Computer. *Proceedings of the ACM Conference on Computer and Communications Security* 2015-October:706–719, ISSN 15437221, URL http://dx.doi.org/10.1145/2810103.2813659.

Nguyen CT, Hoang DT, Nguyen DN, Niyato D, Nguyen HT, Dutkiewicz E (2019) Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks: Fundamentals, Applications and Opportunities. *IEEE Access* 7:85727–85745, ISSN 21693536, URL http://dx.doi.org/10.1109/ACCESS.2019.2925010.

Roşu I, Saleh F (2020) Evolution of Shares in a Proof-of-Stake Cryptocurrency. *INFOMRS Management Science* 67(2):661–672, ISSN 15265501, URL http://dx.doi.org/10.1287/MNSC.2020.3791.

Sánchez-Fernández L, Elkind E, Lackner M, Fernández N, Fisteus JA, Val PB, Skowron P (2017) Proportional Justified Representation. *Proceedings of the AAAI Conference on Artificial Intelligence* 31(1):670–676, ISSN 2374-3468, URL http://dx.doi.org/10.1609/AAAI.V31I1.10611.

Schwarz-Schilling C, Saleh F, Thiery T, Pan J, Shah N, Monnot B (2023) Time is Money: Strategic Timing Games in Proof-of-Stake Protocols. *Leibniz International Proceedings in Informatics, LIPIcs* 282, ISSN 18688969, URL http://dx.doi.org/10.4230/LIPIcs.AFT.2023.30.

Spychiger F, Tasca P, Tessone CJ (2021) Unveiling the Importance and Evolution of Design Components Through the "Tree of Blockchain". *Frontiers in Blockchain* 3, ISSN 26247852, URL http://dx.doi.org/10.3389/fbloc.2020.613476.

Tasca P, Tessone CJ (2019) A Taxonomy of Blockchain Technologies: Principles of Identification and Classification. URL http://dx.doi.org/10.5195/LEDGER.2019.140.

Wang Y, Yang G, Bracciali A, Leung Hf, Tian H, Ke L, Yu X (2020) Incentive Compatible and Anti-compounding of Wealth in Proof-of-stake. *Information Sciences* 530:85–94, ISSN 0020-0255, URL http://dx.doi.org/10.1016/J.INS.2020.03.098.

Xiao Y, Zhang N, Lou W, Hou YT (2020) A Survey of Distributed Consensus Protocols for Blockchain Networks. *IEEE Communications Surveys and Tutorials* 22(2):1432–1465, ISSN 1553877X, URL http://dx.doi.org/10.1109/COMST.2020.2969706.

Yan T, Li S, Kraner B, Zhang L, Tessone CJ (2024) Analyzing Reward Dynamics and Decentralization in Ethereum 2.0: An Advanced Data Engineering Workflow and Comprehensive Datasets for Proof-of-Stake Incentives URL https://arxiv.org/abs/2402.11170v1.

Acronyms

APY Annual Percentage Yield

BA Byzantine Agreement

DAG directed acyclic graph

DPoS Delegated Proof-of-Stake

NPoS Nominated Proof-of-Stake

PoS Proof-of-Stake

PoW Proof-of-Work