IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 13 September 2023, accepted 9 November 2023, date of publication 23 November 2023,
date of current version 1 December 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3336418

RESEARCH ARTICLE

Reward Distribution in Proof-of-Stake Protocols: A Trade-Off Between Inclusion and Fairness

SHENG-NAN LI[1], FLORIAN SPYCHIGER[1,2], AND CLAUDIO J. TESSONE[1], (Member, IEEE)
[1]Blockchain and Distributed Ledger Technologies Group, UZH Blockchain Center, University of Zürich, 8050 Zürich, Switzerland
[2]Institute of Organizational Viability, School of Management and Law, Zurich University of Applied Sciences, 8401 Winterthur, Switzerland

Corresponding author: Claudio J. Tessone (claudio.tessone@uzh.ch)

This work was supported in part by the Cardano Foundation, and in part by the Casper Association.

ABSTRACT Proof-of-Stake (PoS) variants provide an energy-efficient alternative to Proof-of-Work (PoW). However, it is not clear whether practical PoS implementations are fair with respect to wealth, stake, and reward distribution. In this paper, we analyse the fairness of the four well-known PoS platforms Tezos, Polkadot, Cardano, and Casper through a data-driven approach. For this, we collect data on stakes and rewards for all the four platforms over several years. We then apply four measures to study the fairness along different dimensions. We calculate the Gini coefficient to explore the wealth inequality, the Nakamoto coefficient to investigate the degree of decentralization, and the expectational and robust fairness of the stake-reward proportions, i.e., if the validators receive their fair share of the rewards given their stake share. We can show that there are dynamics of high wealth inequalities and stake centralization in all the systems with Polkadot being the exception. With respect to stake-reward fairness, the platforms differ in the distributions of deviations from the fair share, i.e., in Cardano and Tezos, the differences have a lower magnitue as many small validators participate. However, by examining specific outcomes, we can show that platforms with a limited validator set such as Polkadot and Casper tend to be fairer regarding the reward payoffs, but it is not possible for smaller validators to participate. This mechanism sheds light on a trade-off that the platforms face: the more inclusive (open) the validation process is designed, the unfairer the reward distribution tends to be. Our results allow us to conclude that the way of how PoS is implemented matters greatly for its fairness.

INDEX TERMS Blockchain, consensus mechanism, proof-of-stake, decentralization, inequality, fairness, inclusion.

I. INTRODUCTION

Blockchain is considered a trustless technology because it eliminates the need for trust between two parties [1]. Regardless of which protocol a blockchain is based on, a large number of participants is essential for both security and decentralization. However, in order to incentivise more participants to maintain the system, a fair consensus mechanism is a fundamental requirement [2]. Fairness refers hereby to the translation of the invested resources (like computing power, electricity, manpower and financial resource) into rewards. From the commonly held belief, the more people invest into a system, the more they should also receive in return. Nowadays, the two most commonly used consensus protocols are Proof-of-Work (PoW) and Proof-of-Stake (PoS) [3], [4], but many other variants exist [5].

In PoW-based blockchains, the participants, usually called miners, use their computing power to compete with each other and only the first among them to solve the cryptographic puzzle will receive a reward in a nominal amount of a certain cryptocurrency. However, as this mechanism consumes increasingly large amounts of computing power and energy, the waste of resources by PoW has become a major point of criticism of blockchain technology, especially in view of the increasing environmental awareness [6]. Furthermore, there are certain attacks possible in PoW-based systems that may affect their fairness [7]. As famously shown by [8] and [9], miners with a sufficient amount of computing power can decide to mine blocks privately and to publish it later on to earn more rewards than they would in a fair setting, namely

The associate editor coordinating the review of this manuscript and approving it for publication was Binit Lukose.

the selfish mining attack. In [10], [11], and [12], the authors show evidence of such selfish mining behaviour occurring in some popular PoW-based blockchain networks. Furthermore, strategies such as migration and infiltration in games among mining pools can lead to an unfair income share in Bitcoin mining: it was found that there exist incentives for mining pools to infiltrate other mining pools to increase their returns to an unfair level [13].

Nowadays, PoS is becoming more and more popular mainly because of its higher energy efficiency [14]. While PoW assures that each network participant has performed a certain amount of work to receive rewards, PoS requires participants to prove that they are willing to guarantee the consistency of the blockchain by bonding a certain amount of their assets, i.e., tokens. In PoS, the validators instead of miners gather transactions and create blocks. To become a validator, the participants have to hold a certain amount of stakes (tokens). Depending on the protocol, the validators may lose their own money if they misbehave in the system, e.g., propose two conflicting blocks. While PoS is energy-efficient, most existing PoS protocols suffer from the ''nothing at stake'' and the ''long range'' attacks which considerably degrade security in the blockchain [15]. Another widely-discussed potential problem: only rich enough participants can participate in the staking. Moreover, if reward chances are proportional to previous holdings, wealth naturally concentrates on the richer ones. Similarly argued by Fanti et al. [16], this scenario is called ''the rich get richer'' and is known in other contexts as the Matthew effect.

To enable a more equal stake distribution, a number of PoS variants have been proposed that allow more participants to join the staking process by delegating their assets to a validator. These delegated Proof of Stake (DPoS) should benefit the equality of reward distribution and eventually maintain the system's security [17]. Users who do not want to be responsible for the technical operation can delegate – respectively ''vote'' – for a set of validators. One can vote by attributing owned tokens to a validator (i.e. gifting him more chances to validate a block/receive rewards). The validators then receive rewards and share them with their delegators.

Previous studies have addressed the implications of general PoS consensus protocols and different reward functions on income and wealth distribution [18], [19]. Especially in 2021 the authors of [20] showed a counter-intuitive result that the PoS protocol does not lead to wealth accumulation and the rich getting richer but rather to stable investor shares, by considering that the evolution of investor shares in a general PoS protocol closely parallels the evolution of colour shares in a Pólya's urn [21]. However, PoS can be implemented in many different ways and it is in practice often quite different than the pure theoretical version analysed by the researchers in [20]. In [22], the authors looked at different implementations and studied the fairness analytically. They for example show that the Ethereum PoS system does quite well in terms of fairness, but it is not perfect. In general, all these studies examine the fairness of PoS-based systems theoretically and cannot give clear indications on how the wealth and reward distributions behave in a real-world system with its specific PoS implementation. As the respective PoS systems' characteristics differ, distinct monetary dynamics may be the result, creating different levels of wealth and income concentrations.

Thus, this paper aims to investigate the evolution of wealth and stake distribution and related fairness and decentralization measures in four real blockchain systems, including Tezos, Polkadot, Cardano, Casper (listed by the date of launching the PoS protocol) by a data-driven approach. For this, we collect data on the stake and reward dynamics in these systems. We then measure how the reward and stake distributions evolve over time in these systems by an inequality coefficient – the Gini index. In addition, in a PoS system, the decision power of a participant is given by its stake in the system. To measure the degree of decentralization, we apply the Nakamoto coefficient to the stakes. Eventually, we study the fairness of the stake-reward proportions by using two measures: expectational fairness and robust fairness.

In permissionless blockchain based systems, it is not only the networking stack and peering protocols that determine the level of trust that can be built around them, or dictate their resilience; the set of economic incentives that are placed in them are equally (if not more) important for their functioning. We show in this paper that design decisions that may be overlooked from a technical point of view have profound impact in the long-term functioning of PoS based systems. Our contributions are threefold: *First*, we explore the wealth inequalities in the systems and we show that there exist high wealth inequalities with the power being concentrated in the hands of a few validators. This differs among the platforms with Polkadot being the positive exception. *Second*, we apply two fairness measures to compare the stake-reward fairness across platforms. We can show that the platforms differ with respect to specific outcomes related to stake-reward differences. *Third*, we can identify a trade-off between an inclusive validator set and the fairness of reward payments among the validators.

The following parts of this paper are structured as follows: First, Section II introduces our methodology and explains the measures used in this work. Section III presents the four platforms and their specific PoS-implementations. In Section IV, we describe our data followed by Section V in which we explain our results. Lastly, Section VI concludes.

II. METHODOLOGY

To study the properties of the staking and reward distributions in PoS, we selected Tezos, Polkadot, Cardano, and Casper. The four platforms are well documented, active for several years, and have a substantial user base. They have similar PoS mechanism that allow for a comparison. We explore the inequality among the validators in terms of stakes and reward distribution. Additionally, we investigate the

decentralization of the networks by checking the minimum share of participants to gather 51% threshold of total stakes. We use fairness indicators to better understand the connection between the stakes and the rewards, i.e., if the rewards are indeed paid proportionally to the stakes. In the following, we introduce the four measures used in this paper.

A. GINI INDEX

The Gini index is the most frequently used inequality index for income or wealth distribution and has been introduced to measure financial inequality among a nation's residents [23], [24]. The Gini index can theoretically range from 0 (complete equality) to 1 (complete inequality, i.e. one participant has everything, the rest have nothing). The Gini index has been applied several times to blockchain-based systems, e.g. in [26]. In [11], the authors use the Gini index to measure the inequality of mining revenue distribution among miners in several PoW-based systems. Similarly, in the context of PoS protocols, equality refers to the distribution of the stakes and rewards of the validators in the system. Therefore, we apply the Gini index to the stakes and the rewards of the validators, i.e.,

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

where x_i is either the stake s_i or the reward r_i of a validator i, and there are n validators.

B. NAKAMOTO COEFFICIENT

The Nakamoto coefficient [27] is a measure to quantify decentralization. It specifies the number of participants needed to compromise the system. In our setting, we calculate the Nakamoto coefficient based on the stakes of the validators. It answers the question of how many validators are needed to have more than 50 percent of the total stakes. The higher the Nakamoto coefficient the better the protocol in terms of decentralization. We use a relative version of the Nakamoto coefficient that specifies the minimum share of participants that is needed to gather more than 50% of the total staking power S in the system. It can be expressed as

$$N_c = \frac{1}{n} min\{k \in [1, 2, \ldots, n] : S^{-1}\sum_{i=1}^{k} s_i > 0.5\}, \tag{2}$$

where s_i is the stake of validator i and there are again n validators. The validators are sorted by increasing stakes, i.e. $s_i \geq s_j$ if $i \geq j$.

C. EXPECTATIONAL FAIRNESS

In a protocol with a fair incentive mechanism, the rewards of the validators should be proportional to the amount of resources they contribute. Reference [22] introduce a simple measure called expectational fairness. An incentive mechanism preserves expectational fairness for a validator i possessing a fraction $\tilde{s}_i = \frac{s_i}{S}$ of the total stake S if i receives a fraction $\tilde{r}_i = \frac{r_i}{R}$ of the total reward R satisfying $\mathbb{E}\left[\tilde{r}_i\right] = \tilde{s}_i$. This means that a PoS protocol satisfies expectational fairness if for every validator the expectation of their reward fraction (reward compared to the total reward) they receive at a certain time t is the same as the stake fraction they pledged initially. To apply this to the data, we will investigate the expecational fairness by looking at the distribution of the differences between the reward proportion $\tilde{r}_i$ and stake proportion $\tilde{s}_i$ for every validator i:

$$E_i = \tilde{r}_i - \tilde{s}_i. \tag{3}$$

D. ROBUST FAIRNESS

While expectational fairness can provide a measure of fairness with respect to average outcomes, it cannot capture the fairness of specific outcomes. To cope with specific outcomes, [22] have proposed the concept of robust fairness to better characterize the relation between the initial investment and the reward distribution. In particular, robust fairness is a better measure to capture the uncertainty of rewards. It defines a (ε, δ)-fairness: for any given pair of (ε, δ) such that $\varepsilon \geq 0$ and $0 \leq \delta \leq 1$, a reward mechanism preserves an (ε, δ)-fairness if

$$\Pr\left[(1-\varepsilon)\,\tilde{s}_i \leq \tilde{r}_i \leq (1+\varepsilon)\,\tilde{s}_i\right] \geq 1-\delta. \tag{4}$$

Intuitively, robust fairness means that the proportional reward of a validator is relatively close (in a narrow band) to their proportional stake with a high probability. In other words, for a given $\delta \in [0, 1]$, the corresponding $\varepsilon \geq 0$ should be small. We extend the two-sided notion of robust fairness by decomposing it into a lower part and an upper part. We speak of an reward mechanism preserving lower (ε, δ)-fairness, if for any given pair of (ε, δ) such that $\varepsilon \geq 0$ and $0 \leq \delta \leq 1$, we have

$$\Pr\left[(1-\varepsilon)\,\tilde{s}_i \leq \tilde{r}_i\right] \geq 1-\delta, \tag{5}$$

and likewise, we have upper (ε, δ)-fairness if

$$\Pr\left[\tilde{r}_i \leq (1+\varepsilon)\,\tilde{s}_i\right] \geq 1-\delta. \tag{6}$$

To quantify robust fairness, we can plot δ and the corresponding ε for each reward period (see for example Fig. 1). More details about the reward period of each platform can be found in Table 1. To make the measure comparable across periods and platforms, we approximate the integral of this graph – the area under the curve (AUC) – with a simple quadrature rule. The larger the AUC, the less fair is the reward distribution. Therefore, as shown in Fig. 1, in period 300 of Tezos and Cardano, the reward payments are unfairer with respect to lower deviations, i.e., the unfairness is mainly driven by validators that receive proportionally too little, while for Polkadot and Casper, the upper deviations contribute more to the unfairness meaning that some validators receive too much.

III. OVERVIEW ON THE FOUR PoS-PROTOCOLS

We describe the PoS protocols of Tezos, Polkadot, Cardano, and Casper. In each of these platforms, validators stake coins

to become eligible for block producing and receive rewards. However, the protocols differ in the validator selection mechanism, the validator set size, the reward mechanism, the period length, and other technical details. Furthermore, they use different terminologies. We compare the platforms across periods, because this is the natural unit of time in blockchain systems.

A. TEZOS

Tezos[1] uses a liquid Proof of Stake (LPoS) algorithm. In LPoS a validator is called a baker or endorser. As opposed to dPoS, any user can become a validator if they have enough coins. Alternatively, they delegate their coins. Bakers create blocks and endorsers agree on blocks. A validator currently needs 6000 tez (called one roll) and run a full-node validator to take part in the consensus mechanism. Validators collect rewards and redistributed them proportionally amongst their delegators.

Tezos measures times in cycles, where each cycle has 4096 blocks and lasts approximately 2.8 days. Every 256 blocks a snapshot of owned rolls is created and at the end of each cycle, a random snapshot is selected. This provides the validator set for the cycle in t+2. For each block, two priority lists are created: A first list for determining the roll that can bake the next block and a second list with 32 slots for endorsers. In the first list, the owner of the list at position one can propose a block. Therefore, the more rolls, the higher the chance to bake and/or endorse a block. Note, the bakers need to make a security deposit of 512 tez per block, which can be claimed by an accusatory in case of maliciousness (half burned, half goes to accusatory).

Bakers and endorsers are rewarded with a fee for baking and endorsing blocks. When a baker bakes a block, they receive a reward composed of all the transaction fees contained in the block and a network reward. As of the time of writing, a block creates up to 40 new tez, 20 tez for baking and 20 tez for endorsements. However, the exact amount depends on the number of endorsements (only a fully endorsed blocks creates 40 tez).

B. POLKADOT

Polkadot[2] uses a nominated Proof of Stake (NPoS), where nominators (delegators) can elect up to 16 validators. The validators can indicate their willingess to operate a stake pool to the network to be elected by nominators. Validators are pre-selected to create the blocks. Polkadot uses eras (24 hours) during which the active set of validators can create blocks. The active validator set is limited to 297 validators as of the time of writing. The selection of the 297 validators is based on the elections of the nominators. Having said this, only the 264 highest nominations are applied to each validator. Polkadot uses an election algorithm to determine the active validator set in an era. The goals of the algorithm is 1) to maximize the total amount at stake, 2) to maximize the stake behind the minimally staked validator, and 3) to minimize the variance of the stake in the set. Since this is a rather complex optimization problem, Polkadot uses off-chain computation to determine the validator set.

Once the active validator set is defined, an era is further divided into 6 sessions consisting of 2400 slots. The validators are added to specific slots during the session where they can propose new blocks. This assignment is not dependent on their stake. Also the reward payout is independent of the validator's stake in the active validator set. They can collect era points for participating in the network. This adds a slight stochastic component to the reward payout, but in principle, the protocol pays out an equal reward for each validator. In reality, the final reward is paid out proportionally to the era points. The total reward in DOTs (the native cryptocurrency for the Polkadot blockchain) per era follows an inflationary target. To keep validators accountable, they may also lose part of their stake if they misbehave, i.e., going offline, attacking the network, or running modified software.

C. CARDANO

Ouroboros Praos, Cardano's[3] consensus algorithm, is a peer-reviewed PoS algorithm [28]. In Cardano, the native cryptocurrency is ADA, and staking is implemented via stake pools. Stake pools are operated by so-called pool operators. They make sure the stake pool is always online and running. Then delegators can add their stake to a stake pool of their choice. Cardano's Ouroboros Praos divides times into epochs, where each epoch consists of 432,000 slots (5 days). Based on the staked amount in each stake pool, the Ouroboros algorithm samples the stake distribution from the last block of 2 epochs ago. The algorithm then randomly selects zero or multiple slot leaders from all stake pools that can add the next blocks to the blockchain. This selection is proportionally to the staked coins in the stake pools. Since there can be several slot leaders in a slot, the network uses a variant of the longest chain rule as fork resolution. According to the protocol design, there is no slashing in Cardano.

Ouroboros rewards the stake pools 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 reward in each epoch). These funds are distributed among the stake pools and its members, 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.

D. CASPER

The consensus protocol of the Casper[4] network is called Highway. The Casper Highway protocol is a secure and live consensus model in the sense of a classic Byzantine Fault Tolerance (BFT) consensus protocol, however, compared to

[1] https://wiki.tezosagora.org/learn/baking/proofofstake
[2] https://wiki.polkadot.network/docs/learn-consensus
[3] https://docs.cardano.org/new-to-cardano/proof-of-stake
[4] https://docs.casperlabs.io/staking

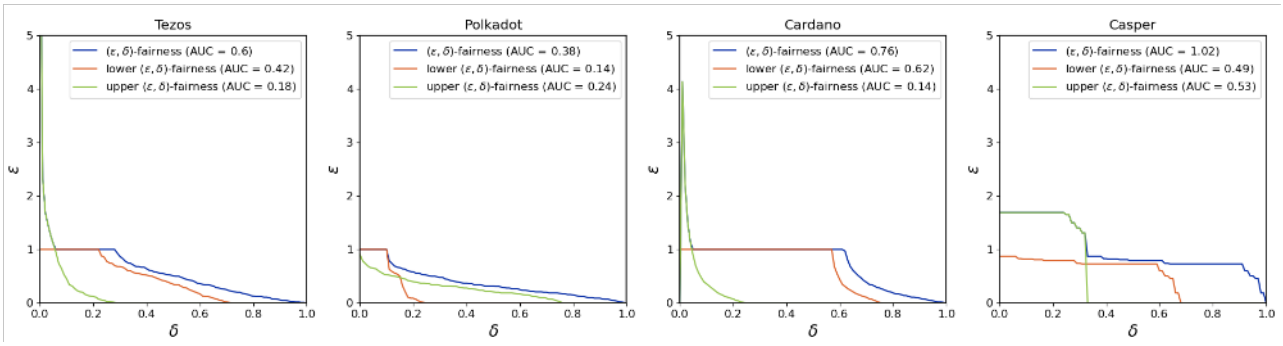


FIGURE 1. Illustration of the (ε, δ)-fairness of the reward distribution for a single period of different platforms.

TABLE 1. Overview of datasets.

Platform	Protocol	Reward Period	Begin	End (period index)	Validator Set
Tezos	Liquid Proof of Stake (LPoS)	Cycle (2.8d)	Sep. 2018	Oct. 2022 (531)	Unlimited
Polkadot	Nominated Proof of Stake (NPoS)	Era (24h)	May 2020	Jun. 2022 (746)	297
Cardano	Proof of Stake	Epoch (5d)	Aug. 2020 (210)	Oct. 2022 (366)	Unlimited
Casper	Proof of Stake	Era (2h)	Mar. 2021	Jun. 2022 (5446)	100

classical BFT PoS models, the block finality is no longer binary but rather expressed by a number. As a server operator, a validator must operate and maintain a Casper node. In order to stake tokens, participants do not need to set up a Casper node themselves, instead they can delegate their tokens to a validator, they are therefore referred to as delegators. The number of validators in the Casper network is limited to 100, and the 100 biggest nodes - measured by the size of their total staking balances - are selected. In Casper, time is measured in eras, and an era is currently set to 2 hours consisting of 225 blocks per era.

In the Casper network, the rewards are not paid out per block but once per era. The rewards (seigniorage) paid in the Casper network are independent of who proposed the block. As a result, in the Casper network, the reward-per-staked-token is the same for each validator. Both validators and delegators will receive a reward that corresponds to their proportional share of total staked tokens. In addition, the validator who was elected as block proposer will receive the transaction fees of the respective block. However, since transaction fees on the Casper network are rather low, these additional rewards are negligible. To pay out the rewards, new tokens are minted and transferred to the validators and associated delegators. The base annual reward rate is 8% of the total supply. However, a reward correction has been implemented: the total rewards paid out are adjusted to the proportion of participation in the network. In the case that only 90 percent of all validators send a message to finalise a block, the actual block reward R is corrected downwards and amounts to only $0.9 \times R$.

IV. DATA

We collect the fully historical records of every reward period from the APIs of the Tezos mainnet,[5] the Cardano mainnet,[6] and the Casper mainnet.[7] For the Polkadot dataset, we query the data from our own archive node which connected to the Polkadot mainnet.[8] Each of the four datasets contains the total reward and stake of every stake pool (shared by validator and all the delgators) in each reward period. Table 1 shows the overview of our datasets. The different system have different lengths of reward periods. In Tezos, Polkadot and Casper, we get the records from the first period of the system, and as Cardano's public staking began at epoch 210, we collect its data from then until October 2022 (epoch 366). All the datasets are open-source.[9]

V. RESULTS

A. BASIC STATISTICS

Firstly, to get an overview of the growth of stake pools, we show the number of active stake pools in each reward period and also the cumulative number of stake pools in Fig. 2. The four platforms are all still growing since the cumulative number of stake pools keeps increasing steadily. As we described in section III and Table 1, there is a fixed number of selected validators during the reward period in Polkadot (297) and in Casper (100). Even though there is no limitation on the selected validator in Tezos, always about 500 stake pools are active and this number is quite stable. In Cardano, not only the cumulative number of stake pools but also the dynamic active stake pools are large and keep growing, which shows a continuously increased inclusiveness of the stake pools. To reflect the concentration of stake pools among all the users, we count the number of account addresses in each transaction and in Fig. 3 we show the ratio of stake pools based on the total number of all the addresses. The growing system of Cardano has a low, but constant fraction of stake pools among all addresses reflecting a high user growth in the platform coupled with a corresponding

[5]https://tzstats.com/docs/api
[6]https://cardano-mainnet.blockfrost.io/api
[7]https://caspermetrics.io/api
[8]wss://rpc.polkadot.io
[9]https://github.com/lishengnanli/PoS_Staking_Reward

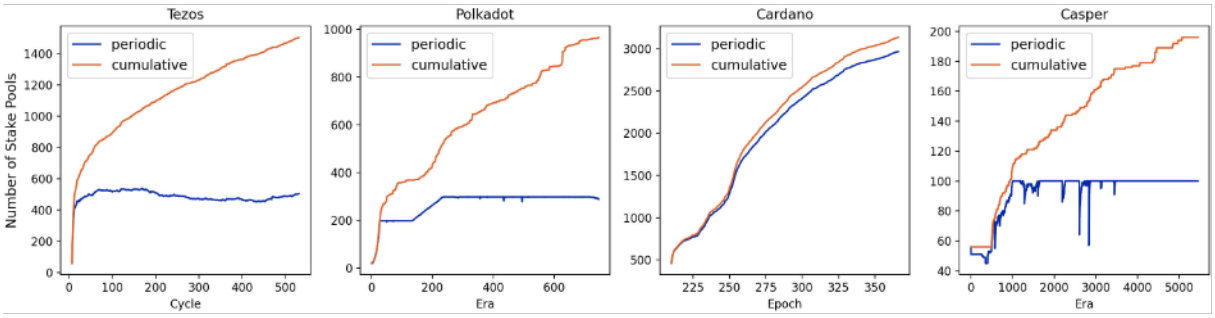


FIGURE 2. Number of stake pools.

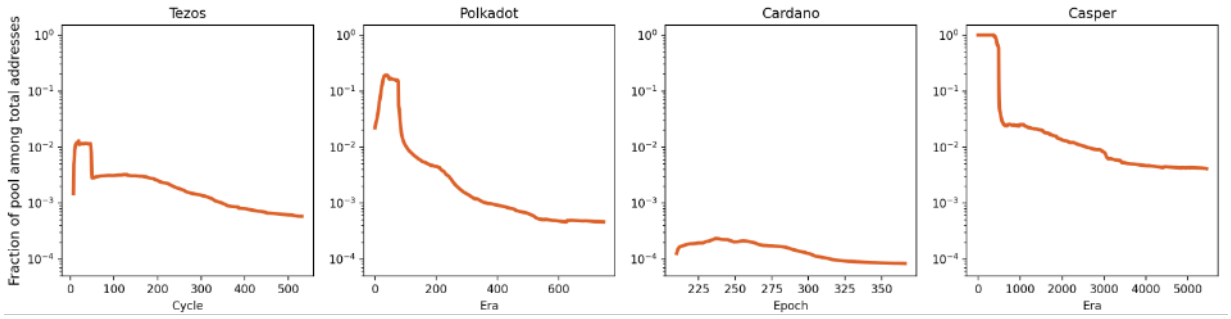


FIGURE 3. Fraction of stake pools among all the addresses.

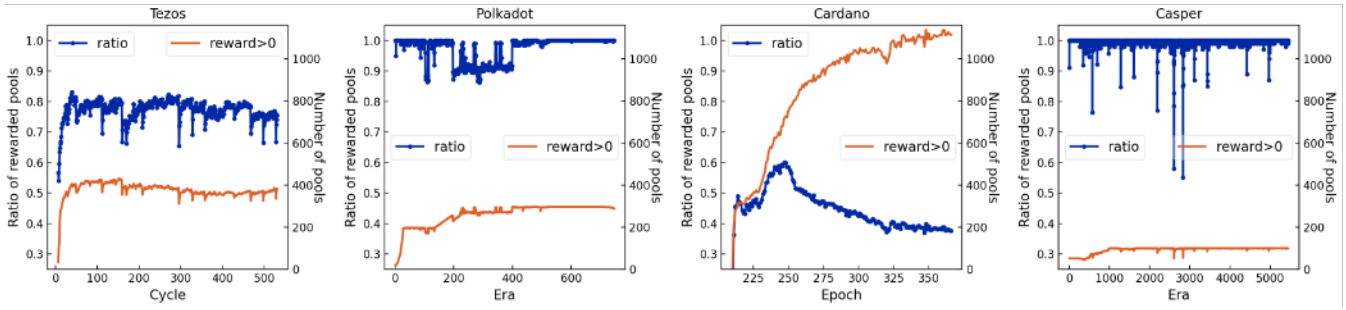


FIGURE 4. Rate of rewarded stake pools.

growth of stake pools (as shown in Fig. 2). In the other systems, the fraction of stake pools among all addresses decreases over time. In all the four platforms, compared with the systems' continuous growth, the stake pools tend to be owned by a limited amount of users, which may eventually cause the decentralized system to be maintained only by a very small set of users.

Further, we calculate the ratio of rewarded stake pools in Fig. 4. This figure (in blue line) shows the fraction of stake pools with a positive total reward among all the active pools with positive total stake during each period. The orange line represents the number of pools that received reward during corresponding period (i.e. pools with reward greater than 0). In Polkadot and Casper, where the number of active validators is limited, the ratio of the rewarded stake pools is almost always equal to 1. It means that these two systems can reward almost all the selected (active) validators in a period. In the other two platforms, not every staker receives a reward in every period. It is sometimes the case that a staker is simply not selected to propose or endorse a block in one period. In Tezos, around 80% of the active validators receive a reward in a period. The Cardano system has the largest number of active validators, but on average only 40% of them receive rewards in a period.

B. INEQUALITY IN STAKES AND REWARDS

Fig. 5 illustrates the evolution of the Gini index for the reward and stake distribution during each reward period, and also the Gini index of the wealth (cumulative reward) of each stake pool in the four platforms. Thanks to the equal reward distribution among stake pools and the election algorithm, Polkadot has the most equal reward and stake distribution, while Tezos is the most unequal. Cardano's

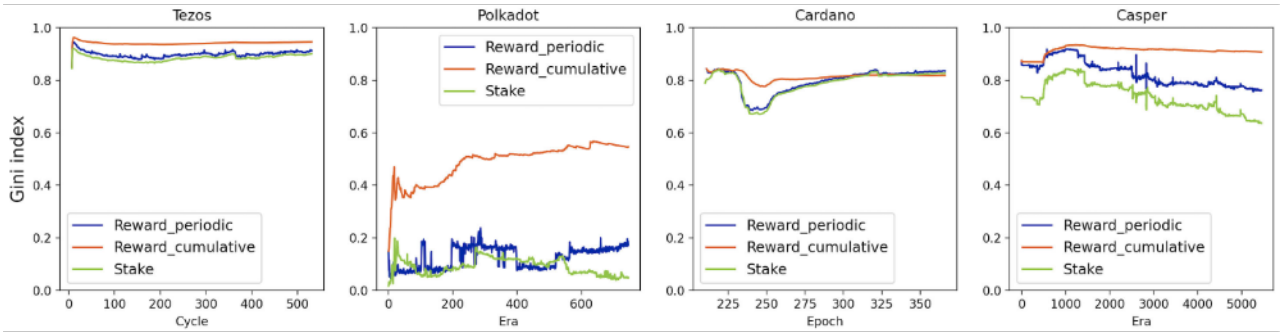


FIGURE 5. Gini index of reward and stake distribution.

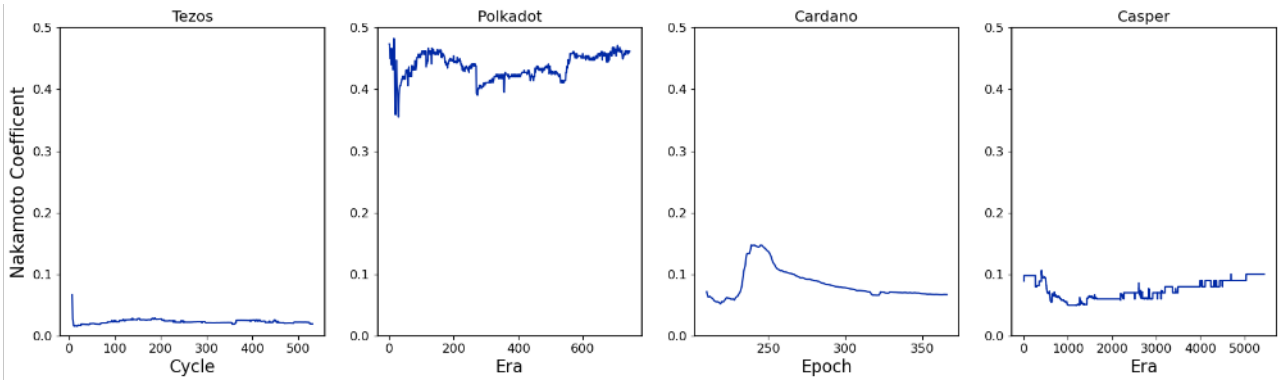


FIGURE 6. Nakamoto coefficient.

protocol increased its "target number of stake pools" (k) parameter from 150 to 500 at epoch 234, which decreased the saturation threshold. As a consequence, one can see that the update of that k parameter has effectively temporarily improved the equality of reward and stake distribution as shown by Cardano's Gini index. Therefore, the saturation threshold seems to be an effective way to influence the wealth distribution. However, now it has returned to the original level of inequality. Casper as the youngest one among these four PoS platforms, has been trending toward greater equality. To further investigate the perspective of wealth concentration, we also calculate the cumulative reward for each specific stake pool. All the four platforms have a larger cumulative Gini index value (in orange line) compared with the one of their periodic reward distribution (blue line), especially in Polkadot and Casper. It means all these platforms have issues of wealth concentration to some extent.

C. DECENTRALIZATION

Fig. 6 plots the Nakamoto coefficient for the stakes of the four platforms per period. The platforms differ not only in the values, but also in the dynamics. The most centralized platform in terms of staking distribution is Tezos as it has a stable, low Nakamoto coefficient. Similarly, Cardano has also a relatively low Nakamoto coefficient that is decreasing over time. Since Cardano introduced PoS rather recently, it remains to be seen how this dynamics develops. It comes not much as a surprise that Nakamoto coefficent of Polkadot's validator set is quite high. This is a direct result of Polkadot's election algorithm aiming at an equal stake distribution among the validators. This election algorithm can be considered as a centralized element though, especially as it computed off-chain. Casper seems also quite centralized, however, it sees a slight dynamics towards a less centralized stake distribution. Having said this, Casper is the youngest of the PoS systems and also Cardano experienced a similar trend in its early days. Furthermore, Polkadot and Casper achieve a somewhat higher decentralization, but they also limit the validator set to a fixed number which is in turn another centralizing force in the system.

D. FAIRNESS OF REWARD DISTRIBUTION

In terms of expectational fairness, we calculate the median and the 2.5% and 97.5% quantiles of the stake-reward differences. The median is almost for all platforms close to zero (see Fig. 7). Only Polkadot seems to have a slightly larger median. As the average of the differences is zero by construction, this is an indicator for a left-skewed distribution. Considering the higher moments of the deviations, there are some clear differences among the platforms. While the deviation of the stake-reward deviation of Tezos and Cardano are symmetrical around zero – with Cardano showing surprisingly regularly behaviour – Polkadot and Casper show some skewness. Casper's distribution shows heavier tails (see the y-axis of Casper's plot in Fig. 7) in the order of two magnitudes, which is quite substantial.

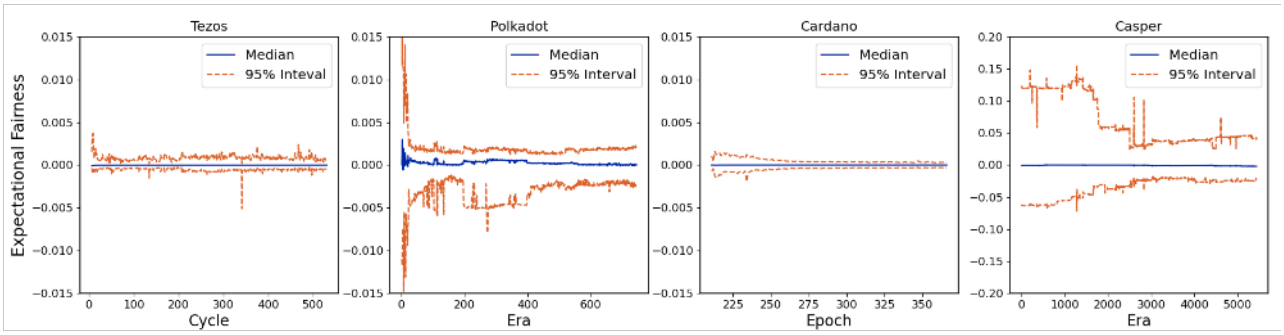


FIGURE 7. Expectational fairness.

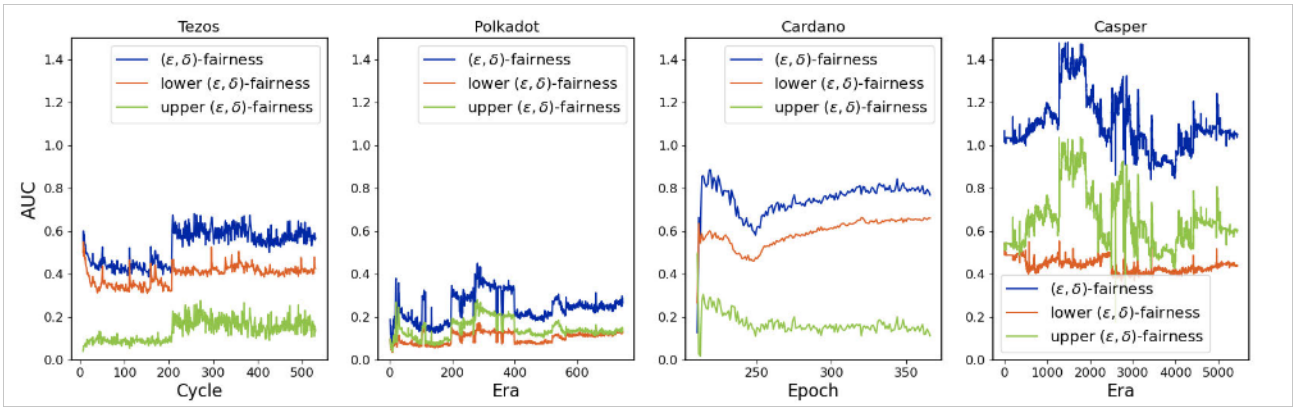


FIGURE 8. Robust fairness.

Furthermore, in the beginning, often some validators received a much higher reward than in the fair case. This skewed distribution was corrected with the mainnet update v.1.3.2. on 12th August 2021. However, the large variations remain as 95% of the variations are between $+/-0.05$). Polkadot shows a somewhat special behaviour: after an initial chaotic ramp-up phase, the system stabilised for some eras, but then started to branch out on the lower end of the distribution. The start of this effect coincides with the launch of parachains in Polkadot. Furthermore, it is in the middle of the gradual expansion of the validator set from 197 to 297 validators.[10]

With respect to robust fairness, the platforms show some interesting dynamics. Fig. 8 plots the area under the curves of the (δ, ε) plot. The higher this value, the less likely are the proportional returns close to the stake proportions. Having said this, there is no absolute interpretation of this value possible, e.g., one cannot say that an AUC below a certain threshold implies a fair system. However, we can use the dynamics of this value to compare the systems. For Tezos, the AUC remains relatively stable over time, however, it increased with the Carthage update in March 2020[11] that changed the formula for calculating the rewards for the bakers. For Cardano, the value seems to stabilise after the kink caused by the adjustment of the saturation threshold. However, the AUC is slightly larger than in Tezos meaning that the returns fluctuate more. Polkadot is the fairest system with respect to robust fairness. In Casper it shows again that the update of August 2021 has led to a fairer system, but the robust fairness seems to be rather volatile. It is also interesting to study the lower- and upper (ε, δ)-fairness: while in Tezos and Cardano, the AUC of the lower fairness is larger than the upper fairness, it is the opposite for Polkadot and Casper. The main difference between these platforms is the inclusiveness, i.e, the limitations on the number of validators. In Polkadot and Casper, the validator set is limited. In these systems, the upper ε-band contributes more to the unfairness, meaning that the reward mechanism leans toward overcompensating certain validators. On the contrary, in Cardano and Tezos the lower ε-band contributes more to their robust fairness. As also shown by Fig. 3, in Tezos and Cardano, a substantial part of the validators receive no rewards in a given period and are therefore undercompensated. Consequently, the AUC of the lower (ε, δ)-plot is relatively large since the ε quickly converges to 1 to satisfy Equation 5 (see also Fig. 1. This unfairness effect seems to be stronger in these platforms as expressed by the large difference between the lower- and upper-(ε, δ)-fairness. The small validators may have the possibility to participate, however, they are undercompensated for their stakes in a period.

VI. CONCLUSION

PoS comes in many variants and many protocols proclaim their implementation to be superior. While all PoS algorithms certainly outperform PoW with respect to energy efficiency,

[10] https://polkadot.polkassembly.io/referendum/9
[11] https://agora.tezos.com/period/24

it is not clear whether PoS is fair regarding the wealth, stake, and reward distribution. While [22] present analytical evidence for a few PoS-implementations showing that the fairness is not given and certain rich-get-richer tendencies apply, [20] show a theoretical argument that PoS leads to stable shares. We used a data-driven approach to explore four concrete implementations: Tezos, Polkadot, Cardano, and Casper. We have shown that all the platforms differ in terms of inequality, decentralization, and fairness all in quantitative evaluation and trends.

Some of the results are a direct consequence of the way how the PoS is implemented, i.e., Polkadot performs quite well with respect to stake decentralization and robust fairness, however, its system also imposes a restricted validator set and resorts on an off-chain allocation algorithm. Tezos on the other hand is a rather open system, however, the stake distribution has become quite centralized over time and also not all stakers receive a reward in each period. The rather recent systems – Cardano and Casper – also show similar tendencies: While Cardano's PoS is also unrestricted and inclusive, Casper imposes a maximum of 100 validators. Again, Cardano has a high degree of openness, but is experiencing a slight tendency towards centralization. In particular, only a low percentage of validators receive rewards in a period. This has lead to a less fair reward distribution for smaller validators compared to the other three platforms. Casper's system, however, sees the opposite tendency. While still on a high level, the inequality of cumulative rewards decreases and the fairness measures improves over time. However, its validator set is limited to 100.

In summary, there seems to be a trade-off between open, non-restricted PoS implementations and fairness – or in other words, between inclusion and fairness. While in non-restricted PoS implementations, the validator set is open, in reality, not all the validators receive the proportional rewards that they would deserve per period. However, everyone has a chance to receive a reward and the validator set is more mixed than in restricted validator sets.

Some potential explanations for these results could be that a restricted validator set allows for an easier selection of the PoS validators based on their stakes. A restricted validator set also matches a period, which is of course also restricted by time and number of blocks. However, such mechanisms exclude small validators as usually only the largest make it into the validator set. Therefore, an open validator set gives small validators a chance to participate, but as the period is limited in time, not all of them receive a reward in each period. This could in the end lead to the formation of larger stake pools since the smaller validators may earn a return in each period by delegating instead of validating.

It seems that more exploration is needed to balance this trade-off between inclusion and fairness and the current implementations can still be optimized. To refine PoS protocols, platforms have to calibrate different parameters such as the period length, validator set size, and minimum threshold for validators. There is no straightforward answer to what the best configuration might be and the optimum may differ on a case-by-case basis. A promising approach could be agent-based simulations to tune parameters of these protocols.

The systematic approach presented here can be applied to all the family of PoS-variants which have different characteristics in their protocols. Furthermore, there are limitations in our work that could be improved in future works. As a first step, we analyzed the fairness per period. To examine whether the systems favour unfairness in a systematic way, e.g., overcompensating always the same validators, a multi-period approach is needed. Moreover, we only looked at the fairness of the stake rewards of the validators and neglected the delegation dynamics. We plan to include the delegators in a follow-up work. Furthermore, we measured the fairness of the stake-reward dynamics from a financial perspective. However, the stake and the corresponding rewards usually also determine the voting power in such systems. Validators with a higher stake also have a higher say in the systems' which in turn is influenced by the rewards they receive. It would be interesting to connect our work with the governance mechanisms in these systems. Additionally, we applied four measures to capture the fairness in the PoS platforms. Fairness is a difficult concept and there are also other means to look at the fairness from a more qualitative side or from a moral perspective. For instance, to measure the level of decentralization more comprehensively, the recently introduced Edinburgh decentralization Index (EDI) [29] that takes numerous metrics from different disciplines – such as economics, information theory and network science – could be used. Lastly, we identified the validators by their addresses. However, a real-world entity may control several addresses which influence the nominal wealth distribution. Future work could use clustering heuristics to identify real-world entities.

We hope that our work inspires future researchers to closely look at the effective functioning of blockchains using a multidisciplinary approach. In the end, only properly understanding the fairness properties of practical implementations will allow people to implement fairer systems.

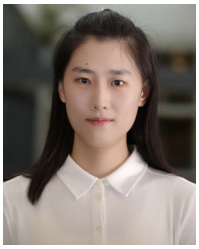
ACKNOWLEDGMENT

(Sheng-Nan Li and Florian Spychiger contributed equally to this work.)

REFERENCES

[1] P. Tasca and C. J. Tessone, "A taxonomy of blockchain technologies: Principles of identification and classification," *Ledger*, vol. 4, pp. 1–39, Feb. 2019.
[2] S. M. H. Bamakan, A. Motavali, and A. Babaei Bondarti, "A survey of blockchain consensus algorithms performance evaluation criteria," *Expert Syst. Appl.*, vol. 154, Sep. 2020, Art. no. 113385.
[3] L. M. Bach, B. Mihaljevic, and M. Zagar, "Comparative analysis of blockchain consensus algorithms," in *Proc. 41st Int. Conv. Inf. Commun. Technol., Electron. Microelectron. (MIPRO)*, May 2018, pp. 1545–1550.
[4] F. Spychiger, P. Tasca, and C. J. Tessone, "Unveiling the importance and evolution of design components through the 'tree of blockchain,'" *Frontiers Blockchain*, vol. 3, Jan. 2021, Art. no. 613476.

[5] W. Wang, D. T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen, and D. I. Kim, "A survey on consensus mechanisms and mining strategy management in blockchain networks," *IEEE Access*, vol. 7, pp. 22328–22370, 2019.
[6] K. J. O'Dwyer and D. Malone, "Bitcoin mining and its energy footprint," in *Proc. 25th IET Irish Signals Syst. Conf. China-Ireland Int. Conf. Inf. Commun. Technol. (ISSC/CIICT)*, Ireland, Jun. 2014, pp. 280–285.
[7] S. Li, "Effects of consensus and incentives on the functioning of blockchains," Ph.D. dissertation, Fac. Econ., Univ. Zürich, Zürich, Switzerland, 2023. [Online]. Available: https://www.zora.uzh.ch/id/eprint/233775/
[8] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," *Commun. ACM*, vol. 61, no. 7, pp. 95–102, Jun. 2018.
[9] C. Schwarz-Schilling, S.-N. Li, and C. J. Tessone, "Stochastic modelling of selfish mining in proof-of-work protocols," *J. Cybersecurity Privacy*, vol. 2, no. 2, pp. 292–310, May 2022.
[10] S.-N. Li, Z. Yang, and C. J. Tessone, "Mining blocks in a row: A statistical study of fairness in Bitcoin mining," in *Proc. IEEE Int. Conf. Blockchain Cryptocurrency (ICBC)*, Toronto, ON, Canada, May 2020, pp. 1–4.
[11] S.-N. Li, Z. Yang, and C. J. Tessone, "Proof-of-Work cryptocurrency mining: A statistical approach to fairness," in *Proc. IEEE/CIC Int. Conf. Commun. China (ICCC Workshops)*, Chongqing, China, Aug. 2020, pp. 156–161.
[12] S.-N. Li, C. Campajola, and C. J. Tessone, "Twisted by the pools: Detection of selfish anomalies in proof-of-work mining," 2022, *arXiv:2208.05748*.
[13] C. Li, F. Spychiger, and C. J. Tessone, "The miner's dilemma with migration: The control effect of solo-mining," *IEEE Trans. Netw. Service Manage.*, vol. 20, no. 3, pp. 2760–2770, Sep. 2023.
[14] C. T. Nguyen, D. T. Hoang, D. N. Nguyen, D. Niyato, H. T. Nguyen, and E. Dutkiewicz, "Proof-of-stake consensus mechanisms for future blockchain networks: Fundamentals, applications and opportunities," *IEEE Access*, vol. 7, pp. 85727–85745, 2019.
[15] W. Li, S. Andreina, J.-M. Bohli, and G. Karame, "Securing proof-of-stake blockchain protocols," in *Proc. Int. Workshops Data Privacy Manage., Cryptocurrencies Blockchain Technol. (ESORICS)*, Oslo, Norway, Sep. 2017, pp. 297–315.
[16] G. Fanti, L. Kogan, S. Oh, K. Ruan, P. Viswanath, and G. Wang, "Compounding of wealth in proof-of-stake cryptocurrencies," in *Proc. Int. Conf. Financial Cryptography Data Secur., 23rd Int. Conf. FC*, F. Bay and S. K. Nevis, Eds. Cham, Switzerland: Springer, Feb. 2019, pp. 42–61.
[17] S. M. S. Saad and R. Z. R. M. Radzi, "Comparative review of the blockchain consensus algorithm between proof of stake (POS) and delegated proof of stake (DPOS)," *Int. J. Innov. Comput.*, vol. 10, no. 2, pp. 27–32, Nov. 2020.
[18] N. Dimitri, "Monetary dynamics with proof of stake," *Frontiers Blockchain*, vol. 4, May 2021, Art. no. 443966.
[19] Y. Wang, G. Yang, A. Bracciali, H.-F. Leung, H. Tian, L. Ke, and X. Yu, "Incentive compatible and anti-compounding of wealth in proof-of-stake," *Inf. Sci.*, vol. 530, pp. 85–94, Aug. 2020.
[20] I. Roşu and F. Saleh, "Evolution of shares in a proof-of-stake cryptocurrency," *Manage. Sci.*, vol. 67, no. 2, pp. 661–672, Feb. 2021.
[21] R. Pemantle, "A survey of random processes with reinforcement," *Probab. Surv.*, vol. 4, pp. 1–79, Jan. 2007.
[22] Y. Huang, J. Tang, Q. Cong, A. Lim, and J. Xu, "Do the rich get richer? Fairness analysis for blockchain incentives," in *Proc. Int. Conf. Manage. Data*, Jun. 2021, pp. 790–803.
[23] J. Morgan, "The anatomy of income distribution," *Rev. Econ. Statist.*, vol. 44, no. 3, pp. 270–283, Aug. 1962.
[24] P. Crucitti, V. Latora, and S. Porta, "Centrality measures in spatial networks of urban streets," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 73, no. 3, Mar. 2006, Art. no. 036125.
[25] J.-H. Lin, K. Primicerio, T. Squartini, C. Decker, and C. J. Tessone, "Lightning network: A second path towards centralisation of the Bitcoin economy," *New J. Phys.*, vol. 22, no. 8, Aug. 2020, Art. no. 083022.
[26] C. Campajola, R. Cristodaro, F. M. De Collibus, T. Yan, N. Vallarano, and C. J. Tessone, "The evolution of centralisation on cryptocurrency platforms," 2022, *arXiv:2206.05081*.
[27] Q. Lin, C. Li, X. Zhao, and X. Chen, "Measuring decentralization in Bitcoin and Ethereum using multiple metrics and granularities," in *Proc. IEEE 37th Int. Conf. Data Eng. Workshops (ICDEW)*, Apr. 2021, pp. 80–87.
[28] T. Kerber, A. Kiayias, M. Kohlweiss, and V. Zikas, "Ouroboros crypsinous: Privacy-preserving proof-of-stake," in *Proc. IEEE Symp. Secur. Privacy (SP)*, San Francisco, CA, USA, May 2019, pp. 157–174.
[29] D. Karakostas, A. Kiayias, and C. Ovezik, "SoK: A stratified approach to blockchain decentralization," 2022, *arXiv:2211.01291*.



SHENG-NAN LI received the bachelor's degree in financial engineering and the master's degree in systems analysis and integration from the University of Shanghai for Science and Technology. She mainly focuses on the functioning of consensus and incentives in blockchain-based systems, including identifying the attacks and risks in consensus, such as selfish mining behavior and consensus without block reward, and evaluating the fairness of incentives in various blockchain protocols.

FLORIAN SPYCHIGER received the M.Sc. degree in quantitative finance from the University of Zürich and ETH Zürich. He is currently pursuing the Ph.D. degree with the Blockchain and Distributed Ledger Technologies Group, UZH Blockchain Center, University of Zürich. He is a Researcher with the UZH Blockchain Center and a Research Associate with the Zurich University of Applied Science. He researches incentives in blockchain systems. He analyses existing incentives in blockchain protocols and blockchain applications and designs new incentive systems. His research interests include consensus design, decentralized autonomous organizations, and blockchain governance.

CLAUDIO J. TESSONE (Member, IEEE) is currently the Head of the Blockchain and Distributed Ledger Technologies Group, University of Zürich (UZH). He is also the Co-Founder and the Chairman of the UZH Blockchain Center. He studies blockchains as a paradigm of socio-economic complexity: linking microscopic agent behavior, incentives (placed on purpose or inadvertently), and interactions with their emergent properties. His research interests include consensus analysis and modeling (looking at the quality of consensus achieved in real-world situations, the effects of incentives, and inequality effects of reward distribution), crypto-economics (inequality, centralization, asset circulation, and hoarding), large-scale blockchain analytics and forensics, and the design of token-based economies.