

# A Comment on “e-PoS: Making PoS Decentralized and Fair”

Suhyeon Lee and Seungjoo Kim

**Abstract**—Proof-of-Stake (PoS) is a prominent Sybil control mechanism for blockchain-based systems. In “e-PoS: Making PoS Decentralized and Fair,” Saad et al. (TPDS’21) introduced a new Proof-of-Stake protocol, e-PoS, to enhance PoS applications’ decentralization and fairness. In this comment paper, we address a misunderstanding in the work of Saad et al. The conventional Proof-of-Stake model that causes the fairness problem does not align with the general concept of Proof-of-Stake nor the Proof-of-Stake cryptocurrencies mentioned in their paper.

**Index Terms**—blockchain, double-spending, majority attack, Proof-of-Stake

## 1 INTRODUCTION

CONSENSUS mechanisms in blockchain prevent Sybil attacks but are also related to fairness and decentralization. Among them, Proof-of-Stake (PoS) is a notable mechanism in the blockchain industry since it provides economically and environmentally beneficial aspects. It is based on a deposit made by miners to pick a block proposer. Staking is the act of securing tokens as a deposit. As a result, a number of cryptocurrencies, like Ethereum, Cardano, Tezos, and Blackcoin, have included PoS in their Sybil control mechanism. In 2021, M. Saad et al. [1] proposed a new PoS scheme, named e-PoS, as a solution to decentralization and fairness issues of the conventional PoS in their paper titled “e-PoS: Making PoS Decentralized and Fair”.

In this comment paper, we present that the description of PoS in [1] does not match the general definition used in PoS-based coins. Thus, we conclude that the issues of decentralization and fairness they seek to address do not exist in the conventional PoS.

## 2 MISUNDERSTANDING OF POS LEADING TO A FALSE QUESTIONING

In this section, we demonstrate that the conventional PoS concept in Saad et al. is significantly different from real-world cryptocurrencies including PoS-based cryptocurrencies mentioned in their paper.

### 2.1 Approach to Conventional PoS Concept

In Saad et al., the authors attempted to address two main issues with the conventional PoS, namely, fairness and decentralization. For the conventional PoS, they mentioned Blackcoin and Nxt as PoS-based cryptocurrencies. We regard the conventional PoS to be the PoS concept which is already in use for real-world PoS applications and which is shared

among these PoS applications. Therefore, we propose to refer to additional real-world cryptocurrencies to understand the conventional concept of PoS.

We analyze 6 PoS-based cryptocurrencies including 2 cryptocurrencies (Nxt and Blackcoin) mentioned in [1]. We selected Cosmos (ATOM) [2], Tezos (XTZ) [3], Cardano (ADA) [4], and Algorand (ALGO) [5] without loss of generality. Table 1 shows the search results in *Google Scholar* and market ranks of PoS cryptocurrencies. We searched the full name of each cryptocurrency with blockchain in quotation marks to avoid irrelevant results. For example, we searched “Algorand”, and “blockchain” with the AND condition. The PoS cryptocurrencies that we introduced in this paper show equal or higher market ranks<sup>1</sup> and citations. We could find the common probability concept in these PoS applications.

TABLE 1: Proof-of-Stake cryptocurrencies with search results and market ranks

Coin	BLK	NXT	ATOM	ADA	XTZ	ALGO
# of Search	638	1710	2070	2640	1540	1890
Market Rank	1486	1020	26	9	42	28

### 2.2 Comparison of the PoS next-block probability in Saad et al. and real-world PoS cryptocurrencies

First of all, the description of the conventional PoS in [1] is the basis of their problem statement and evaluation. It is clearly given in the equation in Saad et al. (Eq. 1) where  $\alpha$  is a miner’s stake, and  $\beta$  is the total amount of stake in the blockchain. According to the equation, it is similar to an auction system. A 51% attacker is always selected as a block proposer in the conventional PoS. It is the main reason which brings unfairness and centralization issues in the conventional PoS [1].

Second, based on the conventional PoS concept, we provide the revised equation (Eq. 2). The miner’s probability of being a block proposer is proportional in the range [0, 1]

- Suhyeon Lee is with Tokamak Network, Singapore and Korea University, Seoul, Korea.
- Seungjoo Kim is with School of Cyber Security, Korea University, Seoul, Korea.  
E-mail: {orion-alpha, skim71}@korea.ac.kr

1. <https://coinmarketcap.com/> May 3, 2022

TABLE 2: PoS leader selection processes and their probabilities under attackers can distribute their stakes into the minimum scale for the leader election

PoS	Leader selection	Probability
Peercoin [6]	$\text{hash}(M_i, T) < D \times C \times A$	$p_i = \frac{s_i a_i}{\sum_{k=1}^n s_k a_k}$
Blackcoin [7]	$\text{hash}(M_i, T) < D \times C$	$p_i = \frac{s_i}{\sum_{k=1}^n s_k}$
Nxt [8]	$\text{hash}(M_i, T) < D \times C$	$p_i = \frac{s_i}{\sum_{k=1}^n s_k}$
Ouroboros [4]	$\text{leader} = \mathcal{F}(S, M)$	$p_i = \frac{s_i}{\sum_{k=1}^n s_k}$
Algorand [5]	$\text{leader} = \underset{\text{participant } k}{\text{argmin}} H(M_k)$	$p_i = \frac{s_i}{\sum_{k=1}^n s_k}$

in Eq. 2. It always provides an opportunity to be a block proposer for a miner in real-world PoS cryptocurrencies while a 51% miner is always a block proposer in Eq. 1.

**Equation in Saad et al.** The probability to mint a next block in the conventional PoS

$$Pr(\alpha, \beta) = \begin{cases} \alpha/\beta & , \alpha/\beta < 0.5 \\ 1 & , \alpha/\beta \geq 0.5 \end{cases} \quad (1)$$

**Revised Equation.** The probability to mint a next block in the conventional PoS

$$Pr(\alpha, \beta) = \alpha/\beta \quad (2)$$

To get this revised equation, we double-checked formal descriptions and implementations of PoS coins. Table 2 shows leader selection processes and their consequent probabilities to be selected as a block proposer. In the table,  $\text{hash}$  denotes a one-way cryptographic hash function. Let  $M_i$  be a miner  $i$ 's unique seed value,  $T$  be a timestamp, and  $D$  be a current difficulty in PoS.  $C$  is the number of ages of staked coins by a miner.  $A$  is a coin age.  $p_i$  is the probability of being a leader for a miner  $i$ .  $s_i$  is a miner  $i$ 's stake amount.  $a_i$  is a miner  $i$ 's coin age.

**Peercoin** is the first cryptocurrency to adopt PoS. It applied PoW and PoS at the same time. It uses the concept of *coin age* which is the time duration from the coin reception. A miner can check if the miner can be a block proposer every second by comparing a hash value named *proofhashOfStake* [6] and *difficulty*  $\times$  *stake amount*  $\times$  *coin age*. The hash value is the output of a cryptographic hash function with a miner's unique seed and the time value as inputs. The unique seed refers to former blocks and the miner's staking transactions. Therefore, it is hard to modify the seed value. Assuming that every seed value is unique and unmodifiable, the cryptographic hash function outputs a random value from a uniform distribution. The probability to be a block proposer at every second is proportional to the miner's stake and coin age.

**Blackcoin** and **Nxt** are PoS cryptocurrencies mentioned in Saad et al. [1]. They are early PoS coins and followed Peercoin's PoS without the concept of *coin age* because of security. Blackcoin [7] described its PoS mechanism as

$\text{proofhash} < \text{coins} \times \text{target}$ . The *proofhash* corresponds to the hash value in Peercoin. The *target* is the difficulty to control block generation speed. In the same way, if *proofhash* is given randomly, the probability to be a proposer is proportional only to a miner's stake amount. It is similarly designed in Nxt [8].

**Ouroboros** and **Algorand** more directly select a block proposer. For example, Ouroboros [4] has a special election function  $\mathcal{F}$  which outputs a leader miner using a current stake distribution. It is designed to select a miner with a probability  $p_i = \frac{s_i}{\sum_{k=1}^n s_k}$  [4]. In Algorand, any miner can be a potential leader only with one token. Therefore, we assume that an adversary can split his stake into the least scale to be a potential leader. The adversary's probability is proportional to his stake ratio compared to the total stake amount. Therefore, the probability to be a next miner is  $p_i = \frac{s_i}{\sum_{k=1}^n s_k}$ , which is identical with Eq. 2.

### 3 CONCLUSION

In this comment paper, first, we provided a conventional concept of PoS based on real-world PoS cryptocurrencies. Second, we compared the probability to mint the next block in the conventional PoS with the probability presented in Saad et al. [1]. Even though our conventional PoS concept covers Blackcoin and Nxt, which are mentioned in Saad et al., it does not match with the conventional PoS probability in [1]. It implies the fairness and decentralization issues that Saad et al. attempted to solve may not exist.

### REFERENCES

- [1] M. Saad, Z. Qin, K. Ren, D. Nyang, and D. Mohaisen, "e-pos: Making proof-of-stake decentralized and fair," *IEEE Transactions on Parallel and Distributed Systems*, vol. 32, no. 8, pp. 1961–1973, 2021.
- [2] J. Kwon, "Tendermint: Consensus without mining," *Draft v. 0.6, fall*, vol. 1, no. 11, 2014.
- [3] "Proof-of-stake in tezos," [https://tezos.gitlab.io/whitedoc/proof\\_of\\_stake.html](https://tezos.gitlab.io/whitedoc/proof_of_stake.html), [Online; accessed 29-April-2023].
- [4] A. Kiayias, A. Russell, B. David, and R. Oliynykov, "Ouroboros: A provably secure proof-of-stake blockchain protocol," in *Annual International Cryptology Conference*. Springer, 2017, pp. 357–388.
- [5] J. Chen, S. Gorbunov, S. Micali, and G. Vlachos, "Algorand agreement: Super fast and partition resilient byzantine agreement." *IACR Cryptol. ePrint Arch.*, vol. 2018, p. 377, 2018.
- [6] "Peercoin's proof-of-stake validation source code," <https://github.com/peercoin/peercoin/blob/c8eea17d3e4880b7aed77ebcde6f46>, [Online; accessed 29-April-2023].
- [7] P. Vasin, "Blackcoin's proof-of-stake protocol v2," <https://blackcoin.org/blackcoin-pos-protocol-v2-whitepaper.pdf>, [Online; accessed 29-April-2023].
- [8] "Nxt whitepaper," [https://nxtdocs.jelurida.com/Nxt\\_Whitepaper](https://nxtdocs.jelurida.com/Nxt_Whitepaper), [Online; accessed 29-April-2023].

This figure "figure2.PNG" is available in "PNG" format from:

<http://arxiv.org/ps/2504.17256v1>