Proof-of-Stake Is a Defective Mechanism

Vicent Sus

visus@uoc.edu

Published in March 2022

Proof-of-Stake (PoS) algorithms, implemented as foundational components of the consensus mechanism of distributed ledgers, are defective cryptosystems by nature. This paper presents intuitive arguments for why PoS, by trying to improve the energy efficiency of Proof-of-Work (PoW) when implemented as a Sybil control mechanism in distributed ledgers, introduces a set of significant new flaws. Such systems are plutocratic, oligopolistic, and permissioned.

INTRODUCTION

A distributed ledger is a cryptographic system, or a combination of cryptographic systems, designed to store and facilitate the transfer of value and data, and to ensure integrity and security through its immutable and tamper-proof nature. This value and data can be in the form of digital currencies, tokens representing assets, and non-financial information such as legal contracts, property records, supply chain details, identity verification data, among other types of digital assets.

The concept of digital currencies based on cryptography is not new, it has existed since the beginnings of digital cryptography [1]. The novelty aspect that current distributed ledgers aim to introduce is the non-dependence of central authorities nor trusted third parties.

The first implementation of a digital currency claiming not to be dependable on trusted third parties nor central authorities was Bitcoin. It consisted of a distributed public ledger (a chain of blocks, or blockchain), secured, verified, and maintained by full node operators and miners [2]. The most challenging part in Bitcoin's design was to reach a solution for the double-spending problem, as in previous digital currencies such as eCash[1], double-spending was prevented by a central authority.

Double-spending, in Bitcoin, was prevented using a distributed consensus mechanism known as Nakamoto Consensus, which implements Proof-of-Work (PoW) as a Sybil control mechanism[2]. Bitcoin achieves distributed consensus by "introducing an opportunity cost from outside of the system (expenditure on computing time, and energy) and providing rewards within the system, but only if consensus on an unbroken transaction history is maintained", as described by Andrew Poelstra [3].

[1] David Chaum designed eCash in 1983, a cryptographic electronic cash system that later would be developed by his company, Digicash.

[2] In a Sybil attack one entity illegitimately adopts multiple identities to gain disproportionate influence in a network.

Proof-of-Stake (PoS) is a Sybil control mechanism that was initially designed to improve the energy consumption derived from PoW when implemented as a foundational component of the consensus mechanism of distributed ledgers, specifically of blockchains [4], which is this paper's focus of examination. PoS successfully prevents Sybil attacks in distributed ledgers, but as it will be seen, it is a defective mechanism when implemented as a foundational component of the consensus mechanism.

Since its first implementation, PoS has evolved into different forms and has garnered a substantial portion of the current market share of distributed ledgers[3]. It has also been the focus of discussion and study by many researchers. Despite the emergence of new PoS algorithms, the key concept that allows this mechanism to prevent Sybil attacks remains the same for all of its forms: in PoS blockchains one coin equals one vote.

Previous Considerations

When designing a distributed ledger, initial supply and subsequent distribution are fundamental problems to tackle and consider. Due to PoS' intrinsic initial supply requirements, blockchains implementing PoS in the distributed consensus mechanism, since the blockchain's initial deployment, present an important pre-mined initial distribution in terms of native tokens percentage of the entire supply. A PoW-based blockchain does not require a substantial pre-mined initial distribution, and the new supply can be created through a process that does not rely on token holders but on computational resources. Note that a blockchain's functional structure and rules are limited but not defined by its Sybil control mechanism.

Contrarily to the technical properties of native tokens derived from pure PoW-based blockchains, native tokens created and distributed using PoS-based algorithms always present, due to its technical nature, four substantial similarities with stocks. There is a centralized creation of the initial supply, followed by its distribution, ending with stakeholders (shareholders) receiving block rewards (dividends) by holding native tokens (stocks). The last similarity is production costs, as the cost of creating pre-mined tokens and block rewards is nearly zero. The almost inexistence of production costs reintroduces the concept of seigniorage[4], an inherent property of PoS.

PLUTOCRATIC

Proof-of-stake essentially means *proof of wealth*. And blockchain protocol's rules, upgrades, and changes are directly linked to its participants' stake (wealth), making these systems a plutocracy by nature –a form of oligarchy where rules are vested in individuals based on their wealth (stake). This way, PoS enables a cryptographic financial system ruled and controlled by plutocrats –most commonly those who initially received large amounts of native tokens from the pre-mining process and the centralized initial distribution.

[3]Despite market capitalization not being a reliable source to determine the actual financial impact on distributed ledgers, it is worth mentioning that the sum of the 10 principal already deployed blockchains implementing PoS with higher capitalization currently is $246B.

[4]The profit made by a government by issuing currency, especially the difference between the face value of coins and their production costs. See `https://mises.org`

PoS blockchains present two different governance models, on-chain and off-chain, and sometimes a combination of both in a hybrid approach.

On-chain governance: In PoS blockchains relying on on-chain governance, decision-making power is often correlated with the size of stakeholders' holdings. This model enables those with substantial stakes, frequently the early recipients of significant native tokens from pre-mining or centralized initial distributions, to apply considerable influence over the network. They have the capability to propose, vote on, and enact changes to the blockchain's protocol. This model leads to a scenario where a small group of wealthy stakeholders, plutocrats, dominate decision-making processes and potentially prioritizing their interests.

Off-chain governance: Contrasting with on-chain governance, off-chain governance in PoS-based blockchains involves decision-making processes that occur outside the blockchain. The community plays a role in shaping rules and protocol changes. Even if this suggests a more democratic approach, the influence of wealthier stakeholders remains significant. They may strategically accept or reject proposals, effectively controlling the flow and implementation of changes. Plutocrats may not be in control of the proposals (or in some cases yes) but they are still in control of the decisions. It is just a matter of time to inject a proposal and to pass it.

OLIGOPOLISTIC

In PoS blockchains, block rewards are directly linked to the amount of native tokens that participants own and stake. The more native tokens stakeholders own, the more they will be earning in the future. *Stakers* are not being rewarded for computational work but capital.

Alternatively, in matters of coin issuance and distribution, PoW-based blockchains are dynamic computational meritocracies as they reward computational achievements and, despite mining pools, earners of block rewards constantly vary.

In summary, PoS rewards wealth, and PoW rewards computational work. Stakers *receive* native tokens (PoS), while miners *earn* native tokens (PoW).

In PoS blockchains, the supply side is small and tends to be non-competitive, analogous to an oligopoly in terms of concentrated control. This concentration occurs because the ability to validate transactions and create new blocks becomes dominated by a few large stakeholders. Unlike traditional markets where an oligopoly involves few suppliers dominating a market with significant influence over prices, in PoS, this dominance is more about control over the network rather than direct market supply and demand [5].

Additionally, in PoS systems there is no natural selling pressure for the recipients of block rewards due to the lower operational costs associated with staking compared to the ongoing expenses in PoW systems, where miners are, in a certain way, forced to partially sell their rewards to cover costs (electricity and equipment) –that is when newly issued native tokens enter the market, there is a market distribution coming from the participants engaged in the opportunity cost that the mining process offers.

Considering that PoS blockchains only require an initial investment while PoW blockchains requires a constant re-investment, added to the fact that staking costs are far cheaper in comparison to mining costs, stakeholders in PoS systems do not need to sell their native tokens. In fact, they are incentivized not to sell their native tokens due to the almost costless recurrent block rewards and the plutocratic governance model.

PERMISSIONED

For a blockchain to not be dependable on external trusted third parties nor central authorities, it must be permissionless –anybody may be able to join the network and become a participant at their will.

In blockchains relying purely in PoW-based consensus mechanisms anybody can become a full node operator or a miner, and consequently, participate in the distribution of native tokens and in the validation process by running a full node without having to own any stake. Miners exchange computational power, time, and energy for native tokens, and full node operators use software and resources to validate blocks and transactions, keep a historical record of transactions, and dictate and enforce the rules of the network. Consensus based in PoW enables a truly permissionless cryptosystem.

Conversely, in PoS blockchains there is only a single way for users to join the network: by acquiring native tokens from existing stakeholders willing to sell. There is no possibility that somebody without stake can participate in the reward distribution and in the validation process. Users without native tokens can only run non-validating nodes.

Moreover, the total amount of validators is limited by the network rules and its total supply, preventing a major decentralization [6], and making many users dependable of other full node operators in view of the minimum requirements to run a node.

This economic barrier to entry, together with the potential influence of initial native token distribution and the accumulation of wealth in a few hands, create a system where entry and influence are effectively regulated by existing wealth and stake. In such a scenario, where a blockchain's core functions and governance are dominated by a plutocratic subset of participants, the system leans more towards being permissioned in practice, despite being open in theory. The PoS model sets a structure where permission, in the form of economic capability and token ownership, becomes a critical determinant of participation and influence within the network.

CONCLUSION

This paper has examined PoS as a foundational component for achieving consensus in distributed ledgers when implemented as a Sybil control mechanism in the base layer of such systems.

Despite the fact that PoS was initially designed to be an energy-efficient alternative to PoW, it is fundamentally defective and introduces a set of significant new flaws to its distributed ledger (which were previously nonexistent): plutocratic governance, oligopolistic control, and permissioned nature.

The plutocratic nature of PoS, where wealth equates to influence, results in a system where decision-making power is concentrated in the hands of a few, often those who were part of the initial distribution of native tokens.

Additionally, the oligopolistic tendencies in PoS blockchains, where control over network validation and native token creation is held by a small number of stakeholders, create an environment completely opposite to the competitive and dynamic nature of PoW-based blockchains.

Furthermore, the permissioned aspect of PoS blockchains, wherein participation in consensus and governance depends upon native token ownership, establishes economic barriers to entry that contradict the foundational principle of an open blockchain network. This model, while theoretically open, in practice limits participation and influence to those who can afford it.

In conclusion, while PoS successfully prevents Sybil attacks and may offer efficiencies and advantages in energy consumption, these benefits come at a trade-off. The resulting system's properties diverge from the core principles and goals of a distributed ledger.

Acknowledgements

I would like to thank Andrew M. Bailey, Jeremy Rubin, and others for providing valuable feedback on earlier versions of this paper.

References

[1] D. Chaum, Blind signatures for untraceable payment, in: Advances in Cryptology: Proceedings of Crypto 82. Boston, MA: Springer US, 1983. p. 199-203.

[2] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf, 2008.

[3] A. Poelstra, A Treatise on Altcoins, https://download.wpsoftware.net/bitcoin/alts.pdf, 2016.

[4] S. King and S. Nadal, PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake, https://www.peercoin.net/whitepapers/peercoin-paper.pdf, 2012.

[5] J. W. Friedman, Oligopoly Theory, Cambridge University Press, 1983.

[6] P. Sztorc, Measuring Decentralization, https://www.truthcoin.info/blog/measuring-decentralization/, 2015.