Proof-of-Stake Is a Defective Mechanism

Vicent Sus
vicent@vicentsus.org

March 24, 2022

Abstract

Proof-of-stake algorithms implemented as distributed consensus mechanisms in the base layer of blockchain networks are defective cryptosystems by nature. By trying to improve the energy efficiency of blockchains using proof-of-work in the consensus mechanism, proof-of-stake is introducing a set of significant new flaws in both monetary and governance models. Such systems are plutocratic, oligopolistic, and permissioned.

1 Introduction

A cryptographic currency — abbreviated as cryptocurrency — is a cryptosystem or a combination of cryptosystems, designed to store and facilitate transfers of value. Bitcoin was the first real implementation of a cryptocurrency not dependable on trusted third parties nor central authority. It consisted, and still does, of a distributed universal public ledger, secured, verified, and maintained in a completely decentralized way by full node operators and miners.

The most challenging part in Bitcoin's development was to reach a solution for the double-spending problem, as in previous cryptocurrencies such as eCash[1], double-spending was prevented by a central authority — compromising the system to different security holes [1].

In Bitcoin, double-spending was prevented using a distributed consensus mechanism known as Nakamoto Consensus, which implements proof-of-work. 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 [2].

Proof-of-stake is a distributed consensus mechanism initially designed to improve the energy consumption derived from proof-of-work [3]. Since its first implementation, proof-of-stake has evolved[2] and many researchers have been discussing different approaches. However, the key concept remains the same, in proof-of-stake one coin equals one vote.

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

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

2 Centralized Initial Distribution

When designing a cryptocurrency, initial supply and subsequent distribution are fundamental problems to tackle and consider.

Due to proof-of-stake's intrinsic initial supply requirements, blockchain networks implementing proof-of-stake as a distributed consensus mechanism present an important pre-mined initial distribution — in terms of coin percentage of the entire network.

Natural money, as opposed to *forced money*, exists because it fulfills human needs better than other mediums of exchange, and is the result of a free market in which private property is inviolable, as described in *The Ethics of Money Production* by J. G. Hülsmann, where he analyzes the economics of money production addressing some of the most important topics of monetary systems.

Historically, different commodities such as gold and silver have acted as natural monies in many societies, having been adopted and discarded voluntarily and spontaneously by the market participants [4]. Satoshi Nakamoto described Bitcoin as a collectible or commodity rather than a stock as bitcoins have no dividend[3]. Additionally, its distributed consensus mechanism made it possible not to need a significant pre-mine to run the network.

Contrarily, coins created and distributed using proof-of-stake present four substantial similarities with stocks. First, there is a centralized creation of the initial supply, followed by its distribution, and ending with stakeholders (*shareholders*) receiving block rewards (*dividends*) by holding coins (*stocks*). The last similarity is production costs, as the cost of creating pre-mined coins and block rewards is nearly zero. The almost inexistence of production costs reintroduces the concept of seigniorage[4] — an inherent property of proof-of-stake.

3 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, proof-of-stake enables an artificial financial state ruled and controlled by plutocrats — the first to receive huge amounts of coins from the pre-mining process and the centralized initial distribution.

In contrast, Bitcoin's distributed consensus mechanism, for example, does not allow miners alone to rule the network nor make changes on the protocol. In Nakamoto Consensus, miners are subject to the rules and changes set by full nodes. So controlling the 51% of the hashrate does not imply controlling the 51% of the vote.

[3] See `https://bitcointalk.org/index.php?topic=845.msg11403#msg11403`

[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`

4 Oligopolistic

Blockchain networks implementing proof-of-stake algorithms as distributed consensus mechanisms are oligopolistic cryptosystems. Block rewards are directly linked to the amount of coins participants own and *stake*. The more coins stakeholders have, the more they will be earning in the future. Miners, or in this case *stakers*, are not being rewarded for work but capital.

In matters of coin issuance and distribution, blockchains using consensus mechanisms based in proof-of-work are dynamic computational meritocracies, as they reward computational achievements and, despite mining pools, earners of block rewards constantly vary.

In summary, proof-of-stake rewards wealth, and proof-of-work rewards computational work. Stakers *receive* coins, and miners *earn* coins.

In *Oligopoly Theory*, James Friedman explains the oligopoly concept in-depth. Briefly summarized, an oligopoly is a market having a few participants on the supply side and a considerable number of buyers on the demand side, where the supply side is not only owned mainly by a few participants, but also it is non-competitive, while the demand side remains competitive [5].

There may be thousands of coin owners in proof-of-stake systems, but only a few of them will own the vast majority of coins. The supply side is small, and it is non-competitive. There is no natural selling pressure for the recipients of block rewards. However, miners of blockchain networks implementing consensus mechanisms relying on proof-of-work are, in a certain way, forced to partially sell their rewards to cover costs (pay equipment and electricity bills). That is when newly issued coins enter the market — there is a market distribution coming from the participants engaged in the opportunity cost that the mining process offers.

Considering that proof-of-stake does only require an initial investment while proof-of-work requires a constant re-investment, added to the fact that staking costs are far from mining costs, stakeholders in proof-of-stake systems do not need to sell their coins. In fact, they are incentivized not to sell their coins due to the perpetual oligopoly and the plutocratic governance model.

5 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 (miner, full node operator, and/or developer) at their will. In blockchains using consensus mechanisms based in proof-of-work, anybody can become a node operator or a miner, and consequently, participate in the distribution of coins and in the validation and verification process by running a full node without having to own any stake. Miners exchange computational power, time, and energy for coins, 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 proof-of-work enables a truly permissionless cryptosystem.

Conversely, in blockchain networks using proof-of-stake as a consensus mechanism there is only a single way for users to join the network, by buying coins from coin owners willing to sell. There is no possibility that somebody without coins can participate in the reward distribution, in the process of securing the network, or running a node. Moreover, the total amount of nodes is limited by the network rules and its supply, preventing a major decentralization [6], and making many users dependable of external node operators in view of the minimum requirements to run a node.

One of the main concerns of oligopolies is that their members may block new entrants. In this case, with a central authority managing the initial supply of the cryptocurrency, attached to the fact that the system is plutocratic and oligopolistic, this centralized authority is the one dictating who can join the network. Therefore, proof-of-stake implemented in the protocol layer of a blockchain network only enables a permissioned system.

6 Conclusion

By trying to improve the energy efficiency of blockchains using proof-of-work in the consensus mechanism, proof-of-stake is introducing a set of significant new flaws in both monetary and governance models.

It is concluded that proof-of-stake algorithms implemented as distributed consensus mechanisms in the base layer of blockchain networks are defective cryptosystems by nature. And for obvious reasons, developers starting new blockchains prefer using proof-of-stake instead of proof-of-work:

Due to the required pre-mine in proof-of-stake systems, the centralized initial supply distribution makes developers very wealthy regarding the network's total supply. As early stakeholders, they can easily maintain and increase their stake thanks to the perpetual oligopolistic system, benefit from the plutocracy, and include investors and venture capitals as early participants. Furthermore, the current global hashrate is mainly used in the Bitcoin network, being very difficult for new blockchain networks to achieve a decent amount of hashrate to be considered secure enough.

7 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] N. Szabo, "Trusted Third Parties Are Security Holes," `https://nakamotoinstitute.org/trusted-third-parties/`, 2001.

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

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

[4] J. G. Hülsmann, *The Ethics of Money Production.* Ludwig von Mises Institute, 2008.

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

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