Proof-of-Stake Is a Defective Mechanism

Vicent Sus
(vicent@vicentsus.org)

September 23, 2021

Abstract

Proof-of-stake algorithms implemented as distributed consensus mechanisms in the protocol layer of blockchain networks present some flaws from a monetary economics perspective. Such systems create a perpetual oligopoly that tends towards the centralization of capital, resulting in a plutocracy.

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 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 proof-of-work as a consensus mechanism. 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, while in proof-of-work one unit of computing power 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 $224B.

2 A Perpetual Oligopoly

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

2.1 Pre-Mining and Initial Distribution

Distribution has been a fundamental problem to tackle and to take into consideration when designing a cryptocurrency. Due to proof-of-stake's intrinsic initial supply requirements, blockchain networks implementing proof-of-stake as a consensus mechanism present an important pre-mined initial distribution, in terms of coin percentage of the entire network. These coins must be created later – or at the same time – of the genesis block.

Natural money, as opposed to *forced money*, exists because it fulfills human needs better than other mediums of exchange, and is the a result of a free market and a completely free society in which private property is inviolable, as described in *The Ethics of Money Production* by J. G. Hülsmann, one of the first books of its kind where he analyzes the economics of money production addressing some of the most important topics of monetary systems, which since then, had been quietly discussed and appeared in only a few literature. 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]. Bitcoin was described by Satoshi Nakamoto as a collectible or commodity rather than a security as bitcoins have no dividend[3]. Contrarily, coins that have been created and distributed using proof-of-stake should be considered securities on account of the simile of how *stakeholders* receive block rewards from owning and *staking* coins, and how *shareholders* earn dividends from owning stocks' shares. To the present, the majority of pre-mined coins from already deployed proof-of-stake blockchain networks have been distributed to its founders, investors and developers. It is, in fact, a centralized initial distribution.

2.2 Supply Issuance, Reward System, and Distribution

In both initial distribution and supply issuance from staking mechanisms there is present the theory of first-round effects, better known as the *Cantillon Effect* due to Richard Cantillon's essay on economic theory in the 18th century, where he also described the non-neutrality of money [5]. Considering supply issuance as a constant expansionary monetary policy, the first recipients of the new supply of coins (*stakers*) can keep their overall percentage of coins – regarding the network – unaffected by the inflationary policy (non-dilutive inflation or neutral inflation), and in some cases increase it, according to the blockchain rules. Those who are close to the money are the ones who profit from monetary expansions, and in staking these are coin owners. First recipients can get loans and make investments, prior to late recipients who can only get the new coins

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

in circulation by buying them from previous coin owners who benefited from the proof-of-stake reward process.

Game theory in proof-of-stake systems incentivizes stakeholders to not sell their coins, taking in consideration that proof-of-stake does only require an initial investment while proof-of-work requires a constant re-investment. Additionally, as the cost of *staking* is far from the cost of mining in proof-of-work, added to the inexistence of externality in proof-of-stake, *stakers* do not have the need to sell their coins. In *Oligopoly Theory*, James Friedman makes an in-depth explanation of the oligopoly concept. Briefly summarized, an oligopoly is a market having a few participants on the supply side and a very large 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 [6]. In proof-of-stake there may be thousands of coin owners but only a few of them will own the majority of coins, the supply side is small, and game theory confirms why it is non competitive. Indirectly, it increases the oligopolistic power and incentivizes coin owners to keep their coins instead of selling them, there is no natural selling pressure for the recipients of block rewards. However, miners of blockchain networks implementing proof-of-work in the protocol layer as a consensus mechanism are, in a certain way, forced to partially sell their rewards to cover costs (pay equipment and electricity bills). That is the moment 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.

2.3 Permissioned

For a blockchain to not be dependable on external trusted third parties nor central authorities, it must be permissionless, where anybody may be able to join the network and become a participant (miner, node operator, and/or developer) at their will. 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 node operators use software and resources to validate blocks and transactions, keep a historic record of transactions, and dictate and enforce the rules of the network. Proof-of-work is a consensus mechanism which 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 node operators is limited by the network rules and its supply, preventing a major decentralization [7], 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 its members may block new entrants, and in this case, with a central authority managing the initial supply of the cryptocurrency, it is this authority 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.

2.4 Plutocratic Result

In proof-of-work, mining is a computational egalitarian meritocratic process run by an external third party, while in proof-of-stake the *staking* process forms a plutocracy which tends towards the centralization of capital. The inexistence of externality in proof-of-stake is what makes it a plutocratic consensus mechanism, where protocol upgrades are also linked to the *stake*.

3 Conclusion

For obvious reasons, developers starting new blockchain networks prefer to implement proof-of-stake as their distributed consensus mechanism instead of proof-of-work.

Due to the required pre-mine in proof-of-stake systems, the 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 resulting plutocracy, and even include investors and venture capitals as early participants. Furthermore, 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.

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://people.cs.georgetown.edu/ clay/classes/fall2017/835/papers/peercoin-paper.pdf, 2012.

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

[5] R. Cantillon, *An Essay on Economic Theory*. Ludwig von Mises Institute, pages 147-153, 2010.

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

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