BoomerNet: A Proof of Experience Consensus Protocol & Decentralized Network

Tarun Rajnish
tarun_rajnish@brown.edu
Brown University
Providence, U.S.A.

Abstract

For more than a decade, decentralized blockchain technology, and in particular cryptocurrencies, has grown in global adoption and real-world applications. Several mining and consensus protocols have been implemented to add blocks, flush the network with new coins and encourage miners and validators to contribute as nodes. Researchers and organizations have a range of consensus algorithms to choose from depending on their requirements, ranging from the well-known Proof-of-Work algorithm pioneered by Satoshi Nakamoto's Bitcoin white paper [8] to the more recent Proof-of-Stake, and even newer mechanisms such as Proof-of-Importance [11] and Proof-of-Activity [3]. Most of these approaches, however, share a flaw. They suffer from the risk of centralization and bless the wealthy with more influence over the network in the form of votes or chance. To this end, we introduce Proof-of-Experience, a novel consensus protocol based on node experience and reputation that tries to solve these issues by creating a more decentralized and secure network while simultaneously giving every node a fair shot at contributing to the blockchain and being rewarded.

Keywords: blockchain, consensus, boomernet, boomers, lydian, proof-of-experience

1. Introduction

There has been a need for centralized financial institutions to manage supply and distribute wealth since the start of economics. This is partly due to the fact that on a decentralized network, the double spending problem [4] has always created an accounting and accountability dilemma. However, distrust and misappropriation of funds by centralized institutions, as well as corruption and other problems, have always necessitated the development of secure, resilient, and fast decentralized methods of economics and asset transfer mechanisms.

A blockchain [10], or distributed ledger, is a decentralized network of nodes who commit transactions to a distributed ledger. Each block in a blockchain refers to the previous block's hash. A blockchain is tamper-proof thanks to this process, as changing any block breaks the hash pointer of all subsequent blocks.

Satoshi Nakamoto published the Bitcoin paper [8] in 2008, which used a Proof-of-Work consensus mechanism to solve the double-spending problem on a decentralized network. The network's nodes compete against one another to solve a cryptographic puzzle and try to be the first to do so. The winning node gets to add a block of transactions to the Bitcoin blockchain, and the rest of the nodes verify that the new block contains no double-spent transactions (along with a host of other validations). The winning node is rewarded through a coinbase transaction, and fresh coins are introduced onto the network as a result.

Despite the fact that Proof-of-Work was an innovative solution to the double-spending problem and gave rise to a completely new asset class and method of monetary transfer without the need for a central middleman, it was not without its fair share of flaws. Mining Bitcoin has a significant environmental impact [2] as it utilizes a huge amount of resources and electricity in order to find the winning nonce. In 2012, Sunny King et al. [7] devised a new consensus process known as Proof-of-Stake, which drastically lowered the amount of compute and energy required to mine new blocks. Staking is used as a way to determine the voting power of validators in PoS [9]. In other words, the more currency a validator stakes or locks into the network, the more voting power and chance of being the block miner they acquire.

Since the publication of the Bitcoin paper in 2008, many different consensus algorithms have been created, resulting in a wide range of blockchain applications. However, they all share two significant sources of concern: possibility of long-term centralization and unequal wealth advantages.

Mining blocks using a CPU or even high-spec graphics cards proved impossible as the Bitcoin network expanded in size. Specialized ASIC cards were required. Nodes must now combine their resources in order to have any chance of earning rewards, and they are compelled to form mining pools. The top five mining pools now control up to 62.7 percent of the bitcoin network's total hash rate [9]. This is a flaw in the

decentralized vision that Bitcoin began with. Staking pools are formed in Proof-of-Stake networks to address the same issue. Furthermore, both Proof-of-Work and Proof-of-Stake award more power to people who have more money. The more computing power you can afford, the better your odds of mining a block in PoW, and the more money you can stake, the better your chances in PoS. Our approach aims to address the unequal wealth disparity as well as centralization threat caused by mining and staking pools.

To address the aforementioned concerns, we propose a Proof-of-Experience consensus method that uses node reputation and total time spent on the network as metrics. Our network is called "BoomerNet" after popular meme culture slang and nodes are known as "Boomers". When a Boomer joins BoomerNet, they accumulate experience. The more experience a Boomer has, the more likely that they will win the competition to mine a block. The more valid blocks a Boomer mines throughout the course of their career, the higher its Reputation and Experience Score. As discussed in Section 3, it is in the best interest for a Boomer to add valid blocks to the BoomerNet chain as well as validate new incoming blocks and stay honest.

In short, BoomerNet solves the centralization problem since it is pointless to build mining pools in this network because experience cannot be aggregated. Furthermore, BoomerNet is not regulated by wealth, but rather by time, and time cannot be purchased. In Section 3, we go into the implementation in depth.

2. Related Work

Proof of Importance

Bingbing et al. [11] alleviate some of the problems with the Proof-of-Stake consensus mechanism, which serves as an inspiration to the BoomerNet network. They discuss how PoS is vulnerable to stake hoarding in order to boost a validator's PoS score. This is similar to the dilemma of the rich getting richer discussed in Section 1. They create a Dynamic Proof-of-Importance consensus mechanism that calculates and evaluates a node's importance score depending on its activity, transaction volume, reputation, and other factors. The higher a node's importance score, the better its chances of gaining accounting privileges and incentives. The Fibonacci Series is used to group nodes for validation, with nodes having a greater relevance score assigned to the top group number. We use a similar experience score allocation scheme, but we intend to eliminate the requirement for a node to vest currency in the network, reducing unfair wealth advantages still further. We also improve group allocation strategy and transaction throughput by selecting users using Algorand's [5] Byzantine Agreement Protocol.

Algorand

Silvio Micali et al. created Algorand [5] in order to scale blockchain consensus and solve the blockchain trilemma [6]. They accomplish this by employing a unique Byzantine Agreement Protocol to achieve network-wide consensus. Algorand picks committees of users using a verifiable random function, allowing them to privately check whether or not they have been picked to participate. Algorand assigns weights to users based on the amount of native Algos they own in order to prevent Sybil attacks. BoomerNet, like Algorands Byzantine Agreement Protocol, weights users but by their Experience score rather than staked amount, as defined in Section 3.

3. Method

The BoomerNet Consensus Protocol

The BoomerNet protocol aims to eliminate the unfair advantage of vested credit or invested money in Proof-of-Stake and Proof-of-Work systems respectively. In BoomerNet, time is God. Any node that wants to serve as a Boomer on the BoomerNet main-net, can do so by committing a specialized joining transaction that gets recorded on the blockchain. This transaction starts the Boomers' clock server that is updated in seconds. The node clock is a distributed clock server that pings active Boomers on the network on a regular basis. Any Boomer that joins BoomerNet must also operate a network-wide node clock server that is "eventually consistent". Life Seconds, or "LS," are the number of seconds a Boomer is active on the network. If a Boomer does not react to a ping from another Boomer, it is recorded as Death Seconds or "DS." A Boomers' Total Life Time or "TLT" is computed as follows:

$$TLT = LS - DS$$

The Reputation Score or "RS" of Boomers increase as they correctly and honestly validate blocks and add them to the network. This score is used as a metric to penalize Boomers that attempt to cheat or are malicious and dishonest. If a Boomer is found trying to contribute an invalid block to the network, their Experience Score or "ES" drops significantly. BoomerNet's Proof-of-Experience consensus protocol is built around this Experience Score.

$$ES = RS * TLT$$

However, time is a linearly increasing entity. As a result, it is evident that older Boomers will always be older than their competition by the same amount of time. BoomerNet divides Boomers based on a dynamically shifting threshold range to overcome this issue. Those with an ES of 5000-10000, for example, would fall into a specific group and form a level

playing field. The number of such fields is dynamically determined based on the number of transactions taking place in the network and the number of active Boomers, and it is done after each new block is minted. Boomers residing in a higher field have a higher chance of accounting and being rewarded. Thus it's in their best interests to stay honest and build their Experience Score. Experience Scores in BoomerNet cannot be combined. This discourages the establishment of pools, and each Boomer contributes to the network individually. As opposed to Proof-of-Stake and Proof-of-Work, this helps keep the network decentralized.

Validation and Committees

The Follow-the-Satoshi (FTS) [9] technique is employed first in BoomerNet to determine the field of Boomers that will participate in block consensus during a given round. The likelihood that a field will be chosen to participate in the procedure is given by [9]:

$$p_i = \frac{s_i}{\sum_{j=1}^{N} s_j}$$

Then, within a level, we use the Verifiable Random Function (VRF) from [5] to select a leader in a non-interactive and private manner. The other Boomers in the field then serve as validators for the leaders block, earning reputation points as a result. To balance incentives, the leader receives somewhat less reputation points than the validators, but is compensated with Lydian, BoomerNet's native cryptocurrency, named after one of the oldest coins in the world [1]. New coins are introduced into the network this way.

Tokenomics

Lydian (ticker LYDN) is BoomerNet's native cryptocurrency. They are given to leaders who successfully add a legitimate block to the main net through a coinbase transaction that refers to the Boomers' public key wallet address. Every four years, the number of Lydian awarded is halved, similar to [8], and the overall supply is restricted at 500 million coins. A Boomer will receive 100 Lydian per successfully minted block when the main-net goes live.

4. Conclusion

BoomerNet is a Proof-of-Experience consensus protocol that tries to solve the rich growing richer paradox and centralization difficulties that popular blockchain consensus protocols like Proof-of-Work and Proof-of-Stake have. PoE accomplishes this by assigning an Experience Score to each node (called Boomer) depending on the node's lifetime in the network and reputation. In BoomerNet, forming pools is futile because Experience Scores cannot be aggregated, which aids network decentralization. Lydian is the native cryptocurrency token of BoomerNet and is given to leaders that mine valid blocks.

5. Future Work

Future work in the Proof-of-Experience field has a lot of potential. In order to determine Experience Score, more extensive criteria and variables could be incorporated. It is possible to imagine a stronger leader and validator selection process based on more concrete probability logic. Furthermore, network security is a top priority, because the identities of nodes in BoomerNet are known, potentially exposing vulnerabilities and risks. Sybil attacks too could be an issue in BoomerNet as there is no currency staked in the network.

References

[1] Russel A. Augustin. "Ancient Coins: Lydian Gold Considered First Coins in the World". In: *Coin Week* (2022).

[2] Liana Badea and Mariana Claudia Mungiu-Pupazan. "The Economic and Environmental Impact of Bitcoin". In: *IEEE* (2021).

[3] Iddo Bentov et al. "Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake". In: *ACM* (2014).

[4] Usman W Chohan. "The Double Spending Problem and Cryptocurrencies". In: *SSRN* (2017).

[5] Yossi Gilad et al. "Algorand: Scaling Byzantine Agreements for Cryptocurrencies". In: *ACM* (2017).

[6] Dong Ku David Im. "The Blockchain Trilemma". In: *University of Pennsylvania* (2018).

[7] Sunny King and Scott Nadal. "PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake". In: *ISIJ* (2012).

[8] Satoshi Nakamoto. "Bitcoin: A Peer-to-Peer Electronic Cash System". In: *bitcoin.org* (2008).

[9] Cong T. Nguyen et al. "Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks: Fundamentals, Applications and Opportunities". In: *IEEE* (2019).

[10] Michael Nofer et al. "Blockchain". In: *Catchword* (2017).

[11] Bingbing Xiao et al. "Proof of Importance: A Consensus Algorithm for Importance Based on Dynamic Authorization". In: *ACM* (2021).