The Application of Proof of Stake: Advantages, Challenges and Future Development

Zhenhao Zhang*

School of Foreign Languages and Cultural Communication, Shanghai Polytechnic University, 201209 Shanghai, China

Abstract. With the development of consensus mechanism, researchers emphasize the need to strengthen the Proof of Stake consensus process. Problem like how to keep the transaction platform protocol fair; how to decentralize the digital transaction system etc. have still remained to be solved. The Proof of Stake also has potential to be applied in various fields. So, it is worth reviewing on the research in recent years to summarize the research methods and conclusions. Study is based on the classical research on Proof of Stake consensus mechanism, improvement of protocol and algorithm of Proof of Stake and application of Proof of Stake. Related developer documentation website, conference papers and authoritative papers were considered. The selected paper was systematically reviewed to make comments on their research methods and analysis the advantages and disadvantages of the research method. After that, the research conclusions are summarized, and potential valuable project or future challenge are described. Through researching on current researches in Proof of Stake, it ultimately leads to the conclusion that Proof of Stake consensus mechanism has better energy efficiency and scalability comparing to the Proof of Work. However, the problems of security and centralization have remained to be solve. In the future, these problems can be solved by improving the algorithm of it or develop new protocol like mixed one of Proof of Stake and Proof of Work.

1 Introduction

A block chain is a publicly accessible database that is shared and updated by numerous computers connected to a network [1]. Transactions (data) are kept on the block chain in blocks, which together create an ever-expanding sequence (chain) that is shared by all network users [2]. There into, Proof of stake is technique to demonstrate that validators have contributed something worthwhile to the network—which might be destroyed if they behave dishonestly—is through proof-of-stake [3]. Proof of stake is used in Ethereum that is a computer embedded in a block chain. It serves as the basis for creating decentralized, permissionless, and censorship-resistant programs and organizations [4]. Proof of stake is a sort of consensus system. The function of proof of stake is that keeping the benefit of users and punish those who are against the rules or do something harmful to block chain and

* Corresponding author: ZhenhaoZhang@fsu.edu.pa

common users. In the Ethereum, the smart contract plays a similar role like proof of stake. It makes those who engage in dishonest behavior in Ethereum transactions punished accordingly, which means it makes the block safer and decentralized.

Since block chain was published in 2008 by Satoshi Nakamoto, block chain has gradually developed into one of the vital technologies of digital finance. In 2009, Satoshi Nakamoto introduced a decentralized currency for the first time. He did this by fusing a consensus mechanism called "proof of work" with well-established primitives for controlling ownership through public key cryptography [5]. To ensure the security of block chain, people committed to work on consensus mechanisms to protect against external attacks. In the beginning, people used a consensus mechanism based on Proof of Work (PoW) to protect the block chain. However, ecological damage is caused by proof-of-work for its huge consumption of energy [6]. Then, On September 15, 2022, the Merge was completed. With this, Ethereum's switch to proof of stake consensus was finalized, formally rendering proof of work obsolete and saving around 99.95% of its energy usage [7]. It comes to a conclusion that proof of stake is better than proof of work on energy consumption, so people use proof of stake or mixed consensus mechanism in block chain transactions. Currently, people commit to the application of proof of stake in various fields and how to improve the proof of stake. Instantly, researchers discuss their extended proof of stake (e-PoS) protocol, and it is based on the PoS protocol and provides decentralization, security, and fairness [8]. Their research proposes extended proof-of-stake and validates whether it can resist centralization or provide fairness to block chain. There are also researchers making comparisons between proof of work, proof of stake and mixed consensus mechanism on their energy consumption. For example, researchers constructed a block chain system model based on agents equipped with PoW and PoS, and hybrid consensus processes which use NetLogo, and conducted simulated studies with six consensus modes and simulation experiment results indicate that mixed consensus mechanism realize the lowest consumption [9]. Furthermore, researchers also propose a new project on proof of stake. For instance, researchers propose a scheme based on proof of stake, by creating a price that is more agreeable for buyers and sellers than dealing with a utility grid, the suggested pricing plan seeks to achieve this goal [10]. In brief, proof of stake can be continuously applied in various fields and the improvement of proof of stake has remained to be continued.

The aim of the paper is to provide a relatively comprehensive perspective on the development of the proof of stake. The following is how the paper is structured. First, it will be the traditional and innovative methods of realizing the proof of stake consensus mechanism in section 2. Secondly, some applications of the proof of stake consensus mechanism are listed such as mechanism data protection, block chain etc. and some related discussions are provided in section 3. Section 4 provides a final summary of the entire paper.

2 Method

2.1 Proof of stake

Fahad Saleh first briefly introduced the block chain and proposed the disadvantages of Proof of Work. Then, Proof of Stake is described to take place of proof of work. After that, the research explains the Nothing-at-Stake Problem, provides an elevated explanation of the PoS protocol (as implemented by the FTS algorithm), other PoS implementations and practical context for PoS are discussed [11]. The research next proposes some other PoS questions and simply describes the solution or mechanism of these things like validator fraud, wealth concentration, etc. Finally, the research comes to the conclusion that there are two ways provided in research to generate consensus of PoS.

2.2 e-PoS

Muhammad Saad et al. who develop e-PoS first considered about the disadvantage of Proof of Stake and then proposed e-PoS to improve fairness, security and decentralization. The research structure is divided into 4 parts: first propose extending PoS and describe its function; Secondly design the construction of e-PoS and using theoretical primitives and engineering needs, show the e-PoS design constructs and their translation into the blockchain framework [8]; then analyze the feasibility of appositionally present how to apply e-PoS into digital transactions. The research model is designed to validate the feasibility of e-PoS and its application. In the first part, Researchers first solve the problem of determination of epoch length, then using 3 algorithms to solve baseline stake, block auction and miners finalization. In the second part, researchers validate its feasibility on its requirements: decentralization and skews, security. After that, provide simulation results to verify e-PoS's performance against traditional PoS systems [8]. Finally, it comes to its applications in Bitcoin and Ethereum and summarizes its disadvantages. The research clearly describes the aim of research and provides branches of validation to prove the feasibility of e-PoS.

2.3 Evaluation of energy consumption

Rong Zhang et al. first proposed the problem that the high energy consumption of blockchain technology prevents it from being used in more areas, despite its many unique qualities, which include machine trust, traceability, and security [9]. Comparing the reliability, equity, and energy consumption of PoW, PoS, and mixed consensus processes is the aim of this research [9]. First, researchers created a model consisting of 3 modules and gave a clear description of them; Next, researchers simulated the experiments in Netlogo using Proof of Work, Proof of Stake and mixed consensus mechanism, 6 modules in total to assess energy consumption, fairness and reliability index. The research raises the problem of energy consumption and describes the model then do the experiments to get the data. After that, analyze the data graph to get the conclusion.

2.4 Improved delegated proof of stake consensus algorithm

Qian Hu et al. aim to focus on enhancing the algorithm based on Proof of Stake. First, give clear introduction of Proof of Work, Proof of Stake and DPoS consensus mechanism. Then research introduces the Reputation -DPoS model and describes its mechanism; After that, research mainly expresses the improvement of incentive mechanism and selection of consensus nodes; ultimately, do the comparison experiment between DPoS and Reputation-DPoS in the Ethereum. It comes to a conclusion that nodes with poorer reputation ratings need additional votes in order to be proxy nodes when they have varying trusted states and receive an equal number of votes [12]. The Research write a lot on mechanism of PoW, PoS and reputation-PoS and find a solution to improve the algorithm. It comes to the conclusion through analyzing the data of votes.

2.5 Improving proof of stake economic security

The research briefly introduces the Maximal Extractable Value, Proof of Stake, staking, lending and primitives. The aim of research is to find out whether the impact of these competitive equilibria is lessened by MEV redistribution, the practice of sharing MEV earnings with validators and provide a positive solution. Researchers use dynamical systems theory to examine asymptotic stability in stake systems with MEV redistribution and analyze the equilibria of the joint staking-lending dynamics [13]. Then researchers describe the model

of protocol and raise three assumptions with conclusion that, if possible, in practice, MEV redistribution can lessen the possibility of economically unstable equilibria for PoS systems. These equilibria reduce the cost of executing assaults [13]. The research first describes the premises and general experimental process, then uses a large number of mathematical proofs and lemmas based on the theory of dynamic systems to finally obtain the experimental results.

2.6 A protocol for proof of stake sharding in scalable block chains

The research first briefly introduces the history of Bitcoin and advantages of block chain. The purpose of this work is to provide a blockchain protocol that is scalable and incorporates the proof of stake (PoS) algorithm [14]. Then, the research introduces three concepts: Proof of Work, Proof of Stake and Sharding which are related to the work. After that the method is based on a sharding protocol and PoS consensus scheme and assessment on the security and complexity of method is written. Finally, it comes to the conclusion that the suggested approach could make the blockchain more scalable in a linear fashion as network size increases [14]. The whole research mainly describes the method of block chain protocol and conducts a series of assessments on it, which prove the feasibility of method.

2.7 A Proof-of-Stake mechanism for Bitcoin subchain consensus

Research introduces the mechanism of block chain and raised the problem that No secure protocol is used by any of the current platforms to determine whether a subchain is consistent [15]. Then a method is proposed that permits reliable subchain maintenance by meta-nodes over the Bitcoin blockchain. The foundation of the protocol is Proof of-Stake [15]. After that, research introduces the mechanism of block chain and clearly describes the protocol for consensus on Bitcoin subchains. Next, research conducted experiments to assess the security of protocol and examine the potential effects of Bitcoin assaults on subchains constructed atop its blockchain [15]. Finally it comes to the conclusion that the security of protocol is as same as Bitcoin. The research mainly describes their proposed protocol and assesses the method through simulating attack to the platform, which provides reliable data to prove how secure the protocol is.

3 Discussion

Based on the current progresses in this field, the Proof of Stake can be applied into parts of digital finance transaction and cybersecurity. For example, Puncturable Signatures and Applications in Proof-of-Stake Blockchain Protocol, which provides the function that offers a satisfactory way to build a workable proof-of-stake blockchain that is resistant to LRSL attacks [16]; A proof of stake protocol called snow white which is used as a "green" consensus substitute for an open-enrollment, decentralized cryptocurrency system [17]. Applications like puncturable signature and protocol ‘Snow White’, etc. improve the security of digital transactions but these applications still need to be improved on energy consumption, decentralization, security etc.

The current studies most illustrate the tendency to improve the protocol to reduce energy consumption. The research made a comparison between Proof of Work and Proof of Stake to express the importance of it and the mixed consensus should be the main object of energy consumption research. Additionally, some innovative protocols tend to improve the mechanism of protocol. Research carried out by Muhammad Saad et al. proposes a new protocol based on Proof of Stake which can make the block chain decentralized and fair, but it still need to solve the problem that there are two limitations of e-PoS: limit the network

size or extend the block mining period; the slight compromise in the system's fault tolerance [8]. he research carried out by Hu Q et al, enhance the conventional DPoS consensus algorithm and suggest Reputation-DPoS, A delegated proof of stake mechanism based on reputation and the improved algorithm still need to Tbe enhanced in the system's security and throughput performance even more by using sharding technology[12].Ultimately, it is essential for researchers to keep improving the protocols, algorithm or develop new ones.

While numerous current studies provide various improvement projects and use mathematics and simulation experience to validate the feasibility of project, there is limitations or disadvantages of these projects remained to be improved. As the researches described above, there are quite a lot things remained to be improved, In the future, it is essential to put emphasis on the security of the protocols based on Proof of Stake for its easily being attacked and lead to unfairness of system; concentrating on the decentralization of system is also a vital problem, so designing the effective mechanism to promote solo stake is remained to solved, too. On the other hand, the application of proof of stake can also be improved and applied in other fields. Instantly, the research on Puncturable Signatures mentioned that designing an effective punctuation signature without the Bloom filter is a good endeavor and Applications for puncturable signatures will extend beyond blockchain technologies that use proof-of-stake [16].

There are also a few solutions proposed to solve such problems. For example, developing a Proof of Stake Sharding Protocol for Scalable Blockchains. While the experiments are still ongoing, it is anticipated that the suggested approach will scale linearly [14]. The plan can improve efficiency in dealing with the digital finance transactions. In addition, considering about the proof of stake in digital Ethereum, in research, Tarun Chitra et al raised future work for improving model includes: employing various usage formulas, closely analyzing the choice between burn or models of protocol-owned liquidity, as well as the expected reward's random fluctuations at the height of the finite block [13].Obviously, future work on Proof of Stake should put emphasis on mechanism and protocol model improvement; energy consumption; various application situation etc.. Proof of Stake still remains to be improved in application fields and protocols, it has potential to improve the security of digital finance transactions and fairness of it.

4 Conclusion

In this paper, the current research and application of Proof of Stake are reviewed. Research methods and potential challenges are summarized through viewing current literature. It is clear that the method of research on Proof of Stake usually uses the method of proposing a hypothesis, proving it through theory, simulating experiments and finally drawing conclusions. There are also some studies proposed to make improvement and provide some theory mathematical proof. The paper also discusses the disadvantages of proposed protocol and mechanism of Proof of Stake, its future work and the potential of its application in the various fields. The paper provided researchers and readers with a view on Proof of Stake and current research status and application scenarios of it. In the future, the improved protocols and models based on Proof of Stake could complete the decentralization and fairness of the digital transaction system and provide better protocols to enhance the security of block chain.

References

1. V. Buterin. Ethereum white paper: Intro to Ethereum. https://ethereum.org/en/developers/docs/intro-to-ethereum/ (2024)

2. C. T. Nguyen, D. T. Hoang, D. N. Nguyen, D. Niyato, H. T. Nguyen & E. Dutkiewicz. Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks: Fundamentals, Applications and Opportunities. IEEE Access, 7, 85727-85745 (2019)
3. V. Buterin. Ethereum white paper: Proof of Stake. https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/ (2024)
4. V. Buterin. Ethereum white paper: Ethereum. https://ethereum.org/en/developers/docs/intro-to-ethereum/. Accessed 2024 Sep 30.
5. The history of Ethereum. https://ethereum.org/en/whitepaper/#history (2024)
6. V. Buterin. Ethereum white paper: Proof of Work. https://ethereum.org/en/developers/docs/consensus-mechanisms/pow/. Accessed 2024 Sep 30.
7. The Merge. https://ethereum.org/zh/roadmap/merge/ (2024)
8. M. Saad, Z. Qin, K. Ren, D. Nyang & D. Mohaisen. e-PoS: Making proof-of-stake decentralized and fair. IEEE Transactions on Parallel and Distributed Systems, 32(8), 1961–1973 (2021)
9. R. Zhang & W. K. V. Chan. Evaluation of energy consumption in block-chains with proof of work and proof of stake. In: Journal of Physics: Conference Series, Vol. 1584, No. 1, p. 012023, IOP Publishing (2020)
10. J. Yang, A. Paudel, H. B. Gooi, et al. A proof-of-stake public blockchain-based pricing scheme for peer-to-peer energy trading. Applied Energy, 298, 117154 (2021)
11. F. Saleh. Blockchain without waste: Proof-of-stake. The Review of Financial Studies, 34(3), 1156–1190 (2021)
12. Q. Hu, B. Yan, Y. Han, et al. An improved delegated proof of stake consensus algorithm. Procedia Computer Science, 187, 341–346 (2021)
13. T. Chitra & K. Kulkarni. Improving proof of stake economic security via MEV redistribution. In: Proceedings of the 2022 ACM CCS Workshop on Decentralized Finance and Security, pp. 1–7 (2022)
14. Y. Gao & H. Nobuhara. A proof of stake sharding protocol for scalable blockchains. Proceedings of the Asia-Pacific Advanced Network, 44(1), 13–16 (2017)
15. M. Bartoletti, S. Lande & A. S. Podda. A proof-of-stake protocol for consensus on bitcoin subchains. In: Financial Cryptography and Data Security: FC 2017 International Workshops, WAHC, BITCOIN, VOTING, WTSC, and TA, Sliema, Malta, April 7, 2017, Revised Selected Papers, Springer International Publishing, pp. 568–584 (2017)
16. X. Li, J. Xu, X. Fan, et al. Puncturable signatures and applications in proof-of-stake blockchain protocols. IEEE Transactions on Information Forensics and Security, 15, 3872–3885 (2020)
17. P. Daian, R. Pass & E. Shi. Snow white: Robustly reconfigurable consensus and applications to provably secure proof of stake. In: Financial Cryptography and Data Security: 23rd International Conference, FC 2019, Frigate Bay, St. Kitts and Nevis, February 18–22, 2019, Revised Selected Papers, Springer International Publishing, pp. 23–42 (2019)