UTM
UNIVERSITI TEKNOLOGI MALAYSIA
INTERNATIONAL JOURNAL OF
INNOVATIVE COMPUTING
ISSN 2180-4370
Journal Homepage : https://ijic.utm.my/

Comparative Review of the Blockchain Consensus Algorithm Between Proof of Stake (POS) and Delegated Proof of Stake (DPOS)

Sheikh Munir Skh Saad & Raja Zahilah Raja Mohd Radzi
School of Computing, Faculty of Engineering
Universiti Teknologi Malaysia
81310 UTM Johor Bahru, Johor, Malaysia
Email: skhmunir@gmail.com

Submitted: 06/09/2020. Revised edition: 19/10/2020. Accepted: 21/10/2020. Published online: 19/11/2020
DOI: https://doi.org/10.11113/ijic.v10n2.272

***Abstract*—Blockchain is a public ledger technology to which everyone has access without a central authority having control. This technology typically gets to use registration and smart contract. To make sure there are security and authenticity in the transaction information in blockchain, many researchers are study on consensus algorithm. There is a lot of consensus algorithm are using in blockchain. Determining leading research area and finding the best key of consensus algorithm is the motivation of this study. Thus, this study will investigate how consensus algorithm areas of research can be determined by study on the Proof of Stake (PoS) and Delegated Proof of Stake (DPos). Besides that, this research study about the key parameters that being using in these two algorithms. In addition, after getting the parameters we measure the comparison in terms of their transaction per second, nodes, and block sizes. Furthermore, we conclude the efficiency of these two algorithms in terms of their scalability. Although DPoS performance is expected to be much better than PoS, the impact of parameters can be assessed and analyzed to see and prove results. We hope after this study, can solved the performance and security affected by the application of consensus algorithm used in the blockchain.**

***Keywords*—Blockchain, Consensus, PoS, DPoS**

I. Introduction

Due to the use of Blockchain technology in terms of smart and registration contracts, it has become a topic of discussion by a majority of the researchers [1]. In simple terms, many scholars have been continually giving their opinion based on how Blockchain technology typically get to use registration and smart contracts. However, in the usage of a distributed ledger with cryptography, techniques to ensure there are security and authenticity in the transaction information, Block-chain is a data structure that is constituted of blocks of data in a manner the same to the linked list [2]. For the reasons that are efficient in the determination of the Blockchain's performance directly, a consensus algorithm is considered as the essential factor of the entire Blockchain system [3]. In other words, the consensus algorithm is a crucial element of every Blockchain network as they are responsible for maintaining the security and integrity of the distributed system in the context of cryptocurrencies. Generally, there are various forms of consensus algorithms. The most commonly used algorithm consists of Proof of Work (PoW), Proof of Stake (PoS). In terms of solving an existing problem within these two algorithms, Delegated of Proof of Stake (DPoS) is perceo be a new consensus algorithm which is known as the third generation Blockchain technology.

There are several existing comparative analysis papers being conducted for comparing the consensus algorithms. However, mostly the comparisons were being made between Proof of Works (PoW) and Proof of Stake (PoS). Importantly, one of the versions, which is created from the Proof of Stake PoS) consensus model, is Delegated Proof of Stake (DPoS). Besides that, in the finding of the difference in performances, there is no relevant analysis, which is conducted to distinguish the process, which coexists between the Proof of Stake (PoS) and Delegated Proof of Stake (DPoS) [4]. Even though there are some papers already stated the comparison of performances, but the real test often never tested and the data of the performances were taken from the source of the cryptocurrency's documents and white papers.

On the other hand, most of the current papers were discussing based on the theoretical information without any proof of concept such as simulation test environment. Without a test simulation, we will be facing difficulties to prove the fact and data that coming from the existing research. In terms of scalability of the consensus algorithm, it is important to conduct a test so that we able to identify the impact of the certain structures in the blockchain such as number of nodes and size of blocks that can really give an impact to TPS of the consensus algorithm. Lastly, it is hard to find a really straight forward papers that can explains in more understandable method so that new comers in the blockchain technology will hardly to understand the way of the evaluation being conducted.

The objective of this research to identify the key parameters for the evaluation of these two algorithms of consensus which are PoS and DPos, to measure the performance of PoS and DPos and to conclude the efficiency between PoS and DPos in terms of their scalability. The existing papers will be used as a reference and the simulation will be tested to come out with the comparison data.

II. BLOCKCHAIN CONSENSUS ALGORITHM

Each blockchain has its own algorithms for developing an agreement at the inputs to be brought inside its network. There are six layers in the architecture of blockchain: data layer, network layer, consensus layer, incentive layer, contract layer, and application layer. Mechanism of consensus is an algorithm collaborative process that clearly defines how consensus is reached between every consensus node and defines the record validation. Blockchain member uses it to reach an agreement whether the transaction is valid and to keep the synchronization of the account. So, every consensus node in the blockchain checks and validates the data based on the algorithm. After a certain number of nodes have been confirmed, the data that is valid can be entered in the blockchain [5].

A. PoS: Proof of Stake

This consensus was developed with an aim of proving a better solution to the previously used algorithm, Proof-Of-work (PoW) that was inefficient and poorly protected from unprofessional behaviour of the delegates. The witness selection systems ensure that the best suited individual is chosen in a democratic manner. In PoS system, a person can mine and certify block transactions according to their stake value. The more the stake a user has, the more the benefits they will get from the system. Through the algorithms, the users are required to stake a certain amount of their tokens to present them with a chance of being picked to validate transaction blocks, and get a reward for validating the blocks [6]. The first selection consideration is how much of currency the forger is staking. It in compulsory for every user to place a stake by depositing certain amount of tokens in the network. The stake is locked in a virtual safe and used as collateral for vouching the blocks. Chances of being chosen are increased according to how much the forger is willing to stake. The higher the stake, the higher chances a user stands of being chosen. The selected forger is only rewarded by the transaction fees since there is no block reward [7].

B. DPoS: Delegated Proof of Stake

DPoS generally helps in following the original PoS consensus model with proper improved speed that further creates issues related with security. It is further identified as democracy within blockchain where the various coin holders generally vote for selecting delegation that is known as block producers. Furthermore, DPoS generally helps in giving much faster processing-based transaction in comparison to PoW as PoS and therefore DPoS generally have a number of flaws including lesser decentralization as well as different types of security challenges [8]. In DPoS. A delegate is chosen to vote on behalf other users who elected them. Therefore, the power lies in the voters. If the voted witnesses underperform or misrepresent their voters, they can be removed from power and a new delegate is voted in. the benefits obtained by the delegates are distributed among the voters who elected them. The validation process is empowered to a small number of users. Since the system allows for users to choose individuals to represent them, the delegates might abuse power since they have the responsibility and authority to validate block chains. Such cartels in the system makes it prone to attacks and making the blockchains less decentralized.

C. Comparisons of PoS and DPoS

DPoS presents a new democratic voting system through which block producers are elected even though PoS and DPoS are similar in terms of stakeholder status. Since the voting Sheikh Munir Skh Saad (2020) system of the DPoS is maintained, the delegates are inspired to be honest and efficient or to vote out. Besides that, DPoS blockchains tend to be faster than PoS in terms of transactions per second.

PoS is considered as a consensus protocol that has a probabilistic-finality. PPcoin was the first cryptocurrency that applied PoS to the blockchain. In order to solving a PoS puzzle in addition to the size of the stake in PPcoin, the age of coin is also introduced [9]. For example, we holding 10 coins for 20 days in total then our coin age will be 200. Every time new block created by a node; the age of the coin will be cleared to 0. Besides PPcoin, there are many cryptocurrencies using PoS for example like Nxt and Ouroboros [3]. Even the Ethereum also plans to move from PoW to PoS.

The DPoS principle is that nodes holding a vote should be allowed to elect block verifiers example like block creators [10]. This means that stakeholders have the right to create blocks for the delegates that supported by them instead of creating blocks themselves, thus they can reduce the computational power consumption to 0. With DPoS, shareholder's vote is the most being used in order to reach the consensus with a democratic way and fair. DPoS is a low cost and high efficiency consensus compared to PoS protocol. They are various cryptocurrencies that use DPoS for their operations. The most common examples include, Bitshares, Steem, EOS and Lisk [11].

TABLE 1. Features different of PoS and DPoS

Features	**PoS**	**DPoS**
Less incentive to centralize	×	√
Higher transaction volume	×	√
Faster confirmation times	×	√
Energy efficient	√	√
Incentives development	√	√

III. PERFORMANCE OF POS AND DPOS

The most critical factor in the entire blockchain framework is the consensus algorithm because the efficiency of the consensus algorithm directly affects the performance of the blockchain. PoS uses stakes in order to compete for the chance of generating new blocks [12]. However, when a PoS node holds a stake for an extended period, its probability of calculating the nonce value is almost 100 percent. In terms of performance, PoS is highly reliant on computing power and still need to waste a lot of computing resources [13]. For this reason, DPoS was developed to use the PoS system but also use the voting model to improve both performance and energy utilization.

DPoS algorithm operates by giving the exceptional role of generating new blocks to a few users who are elected in a competitive election. However, the DPoS algorithm still allows for reorganization, although within a limited range. DPoS model follows the PoS framework but additionally maintaining a limited number of delegates (witnesses) [14]. As a result, the excessive energy consumption and the performance limitations in the PoS model are eliminated. DPoS algorithm works by developing a voting framework that is founded and dependent on the reputations of the delegates.

DPoS is one of the versions that are mainly created with the help of PoS consensus model with proper improved speed by compromising the security that is compared to PoW as well as PoS however it is generally affecting the operation of entire systems [5]. DPoS generally helps in following the original PoS consensus model with proper improved speed that further creates issues related with security [15]. It is further identified as democracy within blockchain where the various coin holders generally vote for selecting delegation that is known as block producers. Furthermore, DPoS generally helps in giving much faster processing-based transaction in comparison to PoW as PoS and therefore DPoS generally have a number of flaws including lesser decentralization as well as different types of security challenges [16]. This further inspires the various developers for developing proper consensus algorithm for solving the problem that is associated with PoW and PoS. DPoS generally follows PoS consensus model that have quite faster consensus real time process however it generally compromises the security [5]. DPoS can be considered as one of the representative democracies within the blockchain where the coin holders generally vote for selecting the delegation that is called block procedures. DPoS processes helps in undertaking transaction quite faster in comparison to PoW as well as PoS algorithm and yet it generally has a number of flaws in context to security [5].

DPoS generally have 21 block producers that mainly participate within the block production process however because the block producers (BP) are mainly exposed and the number of votes is found to be small therefore this type of algorithm generally helps in leaving the BPs quite vulnerable to a number of attacks from different hackers. The validation time of DPoS related transaction is very much faster than one PoS related transaction which further helps in referring the number of nodes that are mainly needed for conducting the verification of each of the transaction [15]. It is analyzed that if transaction mainly occurs in particular platform then it mainly follows PoS for validating transaction as DPoS based consensus platform generally needs around 51% however of only 20 nodes. Real time is important because it helps in determining how long a single transaction can take to get settled. Transaction time is depending on four things, block time and transaction fee traffic block size. If block time is reduced the block size increases. If there are less transaction then traffic is low [17]. Fee that is paid by transmitter helps the network to settle the transaction much faster.

Real time is one of the main factors that is used to evaluate a blockchain viability. DPoS is considered one of the consensus algorithms that help in maintaining proper irrefutable agreement on the truth across different networks that generally validates a number of transactions and its further act as one of the formsof digital-based democracy. It is found that at its core, DPoS generally seeks to increase the speed of block creation as well as transaction without making any type of compromise on the decentralized based incentive structure which is present at the heart of blockchain. Furthermore, it is analyzed that DPoS generally helps in properly proclaiming the improvement of highly flawed PoS based consensus mechanisms. The users are generally asked for properly delegating their voting-based power to different other users whom they generally trust for witnessing [16]. It is also claimed that the incentive structure is quite beneficial in increasing the integrity as well as security of the blockchain and as a result the end-user generally has proper incentive so that they can be able to perform a specific role quite honestly.

TABLE 2. Performance different of PoS and DPoS

PoS	**DPoS**
Take less time to consensus	Take more time to consensus
Has lower effectiveness	Has high effectiveness
Easy to produce Matthew effect and bring centralization	Takes a short period in block production
Management is centralized	Management is decentralized which encourage democracy

IV. COMPARATIVE ANALYSIS

The main aim of this research analysis is to study between PoS and DPoS. In order to understand the flow of the consensus algorithm in Blockchain's application, the evaluation of the PoS and DPoS algorithm is going to be considered [18]. In simple terms, the research analysis is going to show the way of measuring the performances of PoS and DPoS by using a simulation environment. This aspect is going to identify the key parameters in measuring the performances between these two algorithms. Generally, the transaction per second (TPS) will be measured by using a simulation tool with a different number of nodes and block sizes for both PoS and DPoS. Furthermore, the conclusion of the efficiency of these consensus algorithms will be defined based on the scalability comparison data of transaction per second (TPS) that influenced by a different number of nodes and block sizes that applied in the simulation.

V. METHODOLOGY

To ensure that the research stays on the intended course, a framework is developed that guides the research parties on the steps that will be followed. Also, this framework provides a basis of forming sprints for each task and assigning time for each sprint to ensure that the project is on the right course and the stipulated timeframe is adhered to avoid unnecessary extensions and delays of the entire project. It is also important to have sprints in such a research as they play a major role in project management processes. The framework for this research is as follows.

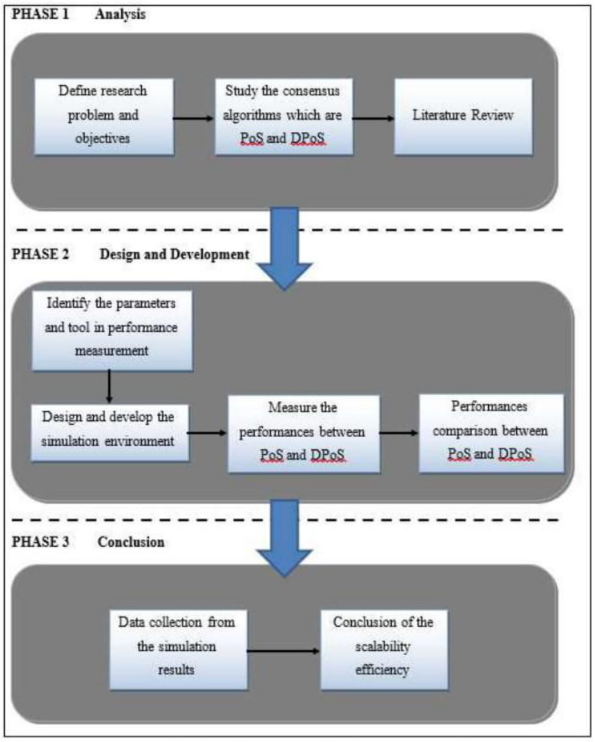
PHASE 1 Analysis
Define research problem and objectives
Study the consensus algorithms which are PoS and DPoS
Literature Review
PHASE 2 Design and Development
Identify the parameters and tool in performance measurement
Design and develop the simulation environment
Measure the performances between PoS and DPoS
Performances comparison between PoS and DPoS
PHASE 3 Conclusion
Data collection from the simulation results
Conclusion of the scalability efficiency

Fig. 1. Framework of the project

A. Phase 1: Analysis

The early stage of this research started by study on the blockchain and the consensus algorithm. The objective of this research to identify the key parameters of these two algorithms of consensus which are PoS and DPos, to measure the performance of PoS and DPos in terms of key parameters and to conclude the efficiency between PoS and DPos in terms of their scalability.

B. Phase 2: Design and Development

Second phase is for the design and development by identify the tools and parameters to be used in performances comparison in this research. This phase will be measuring the key parameters which are transaction per second (TPS), number of nodes and block sizes.

C. Phase 3: Conclusion

The last phase is to conclude the efficiency between the PoS and DPos. This phase will know which algorithm is the best to be applied in blockchain in terms of the scalability. Results will be collected based on the scalability test that being carried out by using a simulation tool which to identify the influence of the different number of nodes and block sizes in TPS measurement between PoS and DPoS.

VI. EVALUATION PARAMETERS

The performance will be measured based on the different amount of block sizes and also number of nodes. This is considered as a scalability test to compare the influences of the number of nodes and size of blocks in TPS measurement.

A. Parameter

The three key parameters that will be used for the simulation are described as below.

TABLE 3. Evaluation Parameters

Parameter	**Description**
Transaction per second (TPS)	Measure the amount of transactions executed in one second
Block sizes	Size of block Megabyte (MB) used in the performance measurement
Number of nodes	Number of nodes used in the performance measurement

B. Transaction per second (TPS)

TPS is transactions number that take place within a second via an information system. The TPS is measured to calculate the system's performance that handling the transaction routine and keep the record of its job. Transaction per second measured evaluate the speed for each of the consensus algorithm between PoS and DPoS. The transactions executed more fast, valid and confirmed when the transaction amount per second is getting higher.

$$\text{TPS} = \frac{Sum_t\,(Transactions)}{t}$$

Where, *t* is the time spent on transaction process and *Sum$_t$ (Transactions)* is a total number of transactions. For example, if it can execute 18 transactions in every minute, so it means that the TPS is 0.3.

C. Scalability Test

The influence of the increase or decrease in number of nodes and size of blocks during the operation of the consensus algorithm will be tested by measuring TPS. This is considered as a scalability test since the TPS will be measured based on its capacity of the nodes and blocks. In order to get the accuracy of the comparison results, the evaluation will undergo for a certain number of times that are based on the parameters that have been identified. The performance will be measured based on the different amount of block sizes and also number of nodes.

VII. SIMULATION DESIGN AND IMPLEMENTATION

The SimBlock is proposed to be used as a tool to simulate the comparison between PoS and DPoS in measuring its performances in terms of the TPS and Scalability. The main reason why the SimBlock has been chosen is because of the criteria that consists of the modules to evaluate the parameters for this research. For this simulation run, it will be test out with a different consensus algorithm which are PoS and DPoS. Consensus algorithm of PoS and DPoS will be adapted into the simulation run in order to simulate the parameters with a different consensus algorithm. By changing the parameter value, the testing will be conducted with a different pattern of simulation. The results will be showed how many transactions can be done according to the simulation patterns the output will be in transaction per second (TPS).

VIII. PREMILINARY RESULTS

The results of the simulation will be analyzed and validated against few existing related works. From there, comparison table will be structured and the graph will be plotted as well so that the comparison can be more understandable and clearer. With all these data, this research will reach its objectives whereby to understand the comparison between these two Consensus algorithms, PoS and DPoS, as discussed earlier in the framework and phases involved in this research.

IX. PREMILINARY CONCLUSIONS

In this initial research, the comparison is still unable to be illustrated in details. The initial results are still not being shown yet as the simulation is still under development. Further studies will continue more details in next phase of this research whereby the simulation will be fully tested, and all the data will be collected. The fully comparative analysis only can be conducted in the next phase of this research. For the future works, a complete comparison will be made between PoS and DPoS. The research will be conducted in more depth and the research will be analysed in more details. It will have an additional research papers be studied. For the simulation process, it will be done in a manner way by following the methodology that being discussed. Therefore, an accurate result can be obtained in this analysis. The simulation will be conducted by using open-source software tools and all the results will be stated clearly. Lastly, a complete comparative analysis will be able to be shown in the next phase of this research.

REFERENCES

[1] A. Li, X. Wei, and Z. He. (2020). Robust Proof of Stake: A New Consensus Protocol for Sustainable Blockchain Systems, *Sustain.*, 12(7), 2824. https://doi.org/10.3390/su12072824,

[2] A. Kumar, D. K. Sharma, A. Nayyar, and S. Singh. (2020). Lightweight Proof of Game (LPoG): A Proof of Work (PoW)' s Extended Lightweight Consensus Algorithm.

[3] A. Kiayias, A. Russell, B. David, and R. Oliynykov. (2017). Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol BT - Advances in Cryptology – CRYPTO 2017. *Advances in Cryptology - {CRYPTO} 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part {I}*.

[4] D. Valdeolmillos, Y. Mezquita, A. González-Briones, J. Prieto, and J. M. Corchado. (2020). Blockchain Technology: A Review of the Current Challenges of Cryptocurrency. *Advances in Intelligent Systems and Computing*.

[5] Q. Deng. (2019). Blockchain Economical Models, Delegated Proof of Economic Value and Delegated Adaptive Byzantine Fault Tolerance and their implementation in Artificial Intelligence BlockCloud, *J. Risk Financ. Manag.*

[6] S. M. H. Bamakan, A. Motavali, and A. Babaei Bondarti. (2020). A Survey of Blockchain Consensus Algorithms Performance Evaluation Criteria, *Expert Systems with Applications*.

[7] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. *Proceedings - 2017 IEEE 6th International Congress on Big Data, BigData Congress 2017*.

[8] J. He, P., Tang, D., and Wang. (2020). Stake Centralization in Decentralized Proof-of-Stake Blockchain Network (SSRN Scholarly Paper ID 3609817, *Social Science Research Network,* https://doi.org/10.2139/ssrn.3609817.

[9] S. King and S. Nadal. (2012). Peercoin-Paper. *Whitepaper*.

[10] Lovejoy, J. P. T. (2020). An Empirical Analysis of Chain Reorganizations and Double-Spend Attacks on Proof-of-Work Cryptocurrencies. Doctoral dissertation, Massachusetts Institute of Technology.

[11] T. Zhou, X. Li, and H. Zhao. (2019). DLattice: A Permission-Less Blockchain Based on DPoS-BA-DAG Consensus for Data Tokenization, *IEEE Access*.

[12] N. Kshetri. (2018). International Journal of Information Management 1 Blockchain's Roles in Meeting Key Supply Chain Management Objectives, *Int. J. Inf. Manage.*

[13] B. Cao *et al.* (2020). Performance Analysis and Comparison of PoW, PoS and DAG based Blockchains, *Digit. Commun. Networks*.

[14] X. Wei, A. Li, and Z. He, (2020). Impacts of Consensus Protocols and Trade Network Topologies on Blockchain System Performance.

[15] L. Jiang, S. Xie, S. Maharjan, and Y. Zhang. (2019). Blockchain Empowered Wireless Power Transfer for Green and Secure Internet of Things, *IEEE Netw.*

[16] I. Barinov *et al.* (2019). POSDAO: Proof of Stake Decentralized Autonomous Organization. *SSRN Electron. J.*

[17] Y. Yu, Y. Zhang, S. Qian, S. Wang, Y. Hu, and B. Yin. (2020). A Low Rank Dynamic Mode Decomposition Model for Short-Term Traffic Flow Prediction. *IEEE Trans. Intell. Transp. Syst.*

[18] M. Du, X. Ma, Z. Zhang, X. Wang, and Q. Chen. (2017). A Review on Consensus Algorithm of Blockchain. *2017 IEEE International Conference on Systems, Man, and Cybernetics, SMC 2017*.