COMPARATIVE ANALYSIS OF CONSENSUS ALGORITHMS IN BLOCKCHAIN NETWORKS

Luka Lukić[1]*,
Nenad Kojić[1],
Mladen Veinović[2]

[1]Academy of technical and art applied studies Belgade,
Department: School of applied studies for Information and communication technologies,
Belgrade, Serbia

[2]Singidunum University,
Belgrade, Serbia

Abstract:
Since 2009, with the invention of Bitcoin, the usage of blockchain technology is constantly increasing. From its initial financial use case, blockchain as a decentralized data storage system has grown to an entirely new information ecosystem and has been successfully applied in a wide range of applications in other industrial sectors, outside of finance. Given that the data is decentralized, the computer nodes participating in the network are in charge of adding new data to the blockchain, the authenticity of which is determined by consensus algorithms as a mechanism for maintaining data integrity. Bearing that in mind, consensus algorithms and their application are crucial for the reliability and data security in a blockchain. The aim of this paper is to perform an analysis of currently most used consensus algorithms, as well as their impact on key blockchain attributes.

Keywords:
Blockchain, Consensus algorithm, Decentralization.

INTRODUCTION

At its core, the blockchain represents a decentralized database, developed in the form of a ledger with its data being timestamped and immutable. Bitcoin was developed using such technology, as a form of digital money, serving as the first such implementation to successfully solve the double-spending problem, due to the nature of how blockchain works [1]. With the growing popularity of Bitcoin, other "currencies" based on the same technology have been developed, and due the fact that the technology significantly relies on cryptography, they are collectively called cryptocurrencies. Although it has been attracting public attention since 2009 with the advent of Bitcoin, the concepts presented in the Bitcoin whitepaper written in 2008. date significantly earlier. Back in 1982, David Chaum presented in his dissertation a protocol that significantly resembles a blockchain [2]. Its application would allow for the development of a computer system in which participants do not have to have mutual trust, but the system is designed as trustworthy allowing such parties to interact. Relying on his work, Harber and Stornetta developed a document time-stamping system as a mechanism to guarantee its integrity [3].

Correspondence:
Luka Lukić

e-mail:
luka.lukic@ict.edu.rs

DOI: 10.15308/Sinteza-2021-128-133

As a blockchain system is distributed and spreads through a computer network, it is necessary that all participants in the network agree on the correctness of the data it holds. For these purposes, the so-called "Proof of Work" (PoW) was first to be implemented and used as a consensus algorithm to guarantee the credibility of the data that the network participant was trying to write on the blockchain. PoW was first presented in 1992 as an attempt to combat spam emails.

Although it is considered a new revolutionary technology, it can be noticed that the foundations of blockchain were built years ago and have a sound scientific basis. From its inception until today, Bitcoin has had significant fluctuations in terms of market value. Starting at just $0.09 in 2010, the value of Bitcoin has had significant ups and downs over the years, but looking at the general trend, the price of Bitcoin seems to constantly rise. The popularity of Bitcoin has contributed to the further development of cryptocurrencies and blockchain as a technology. As a consequence of this development, other blockchain implementations were designed promoting Turing completeness and providing the possibility of writing programs that could be both stored and executed within the blockchain. Such programs are called smart contracts, with Ethereum being an example of a blockchain that provides such a possibility. It was developed in 2014 with an original cryptocurrency called Ether. Although the primary focus is on the financial sector, blockchain as a decentralized database has found application in other fields as well, such as healthcare, supply chain, voting systems, Internet of Things, insurance, digital rights management and real estate [4] [5] [6]. This expansion in blockchain's applicability has naturally led to the further development of the technology itself. Initially, the proposed consensus algorithm, PoW, although meeting the needs in terms of data security and integrity, turned out to be impractical from the scalability point of view. This scalability issue has served as a catalyst to the emerging interest for finding the alternative algorithms upon which the network participants would agree and thus keep the blockchain secured [7] [8] [9]. The aim of this paper is to analyse currently most used consensus algorithms, compare their advantages and disadvantages and suggest situations in which it is appropriate for them to be used.

This paper is organized through five chapters: After the Introduction, the second chapter presents blockchain core principles. The third chapter provides an overview and analysis of existing consensus algorithms, while the fourth chapter is devoted to comparative analysis. Finally, a conclusion was given with plans for further development of the proposed idea.

2. THE PRINCIPLE OF OPERATION OF THE BLOCKCHAIN

The first version of blockchain was developed on top of the model provided by Bitcoin's whitepaper and thus has laid the foundation in terms of the blockchain technological principles [1] [5]. The main idea behind the blockchain is the removal of the third party whom the business participants have to trust.

In the initial implementation, this has meant the removal of financial institutions, allowing the participants to transact directly, which Bitcoin blockchain successfully allowed for [10]. By doing so, Bitcoin has served as an example, spreading the idea of independence from centralized third parties to industries outside the financial sector [5] [6]. In order to achieve such independence, the blockchain is designed as a decentralized database, where each computer (node) in the network contains part of or the entire data set. It consists of interconnected blocks of data, each containing transactions portrayed in a form of Merkle's tree and being cryptographically linked to the block preceding it. As the blocks are arranged chronologically, the blockchain can be seen as a ledger containing the history of all transactions. In order to maintain data integrity, nodes in the network work together as transaction validators and only when most of the nodes agree on the correctness of transactions, and the block itself containing them, the block is added to the chain. This decision about data correctness is based on a consensus algorithm defined at the blockchain level. The Bitcoin blockchain uses the PoW consensus mechanism, and currently popular next to it are "Proof of Stake" (PoS) and "Delegated Proof of Stake" (DPoS) [8]. When it comes to cryptocurrencies, nodes participating in the network and thus making it possible are rewarded with appropriate amounts of cryptocurrency [8].

From the access point of view, blockchain networks can be divided into private and public ones. Regarding private blockchains, only computers that are granted access can interact with the blockchain, while with the public ones anyone can access and interact with the blockchain. Bitcoin and Ethereum are examples of a public blockchain, while the popular implementation of private blockchain Hyperledger Fabric [1] [11]. From the extensibility point of view, some blockchain implementations can be additionally programmable, i.e., provide the ability to implement and execute program code. This way, applications that could previously only be executed through a trusted intermediary, now

can work in a fully decentralized manner, without the need for a central authority, while providing the same set of functionalities. Bearing that in mind, blockchain is said to enable thrustless networks, because interested parties can participate in transactions even though they do not trust each other. This absence of intermediaries means faster and often more reliable transaction resolution [12]. Program code execution within the blockchain is achieved by deploying and triggering smart contracts, and the blockchain networks that support them are considered to be Turing complete. Depending on the platform, there is a wide range of programming languages for smart contract implementation, the most used among them being Solidity, initially designed for Ethereum blockchain.

Although the concept of smart contract directly corresponds to applications related to the financial sector, they can be used for various forms of blockchain programs and are considered a distributed form of business logic [5] [13]. An example of a smart contract that is used significantly is the Uniswap decentralized application. It represents a decentralized cryptocurrency exchange where anyone can, unlike centralized exchange where it is previously necessary to prove their identity, trade cryptocurrencies as long as there is enough liquidity for the cryptocurrency of concern. That being said, users are divided into two groups: traders who pay a certain amount of fee for participation in the trading transaction, and liquidity providers who expose their cryptocurrencies to exchange, to make the exchange possible, and in return are rewarded with part of the fee from participants [14]. An example of an application that is not intended for financial services is the application for the implementation of decentralized voting in elections [6]. With blockchain, the entire voting flow was performed in a decentralized manner, and the management was left to the software, thus removing the need for trust in any intermediary.

3. ANALYSIS OF BLOCKCHAIN CONSENSUS ALGORITHMS

Consensus algorithms are used to determine the credibility of a network node trying to write data to a blockchain [1] [7] [8] [9]. The first such algorithm, POW, although satisfying security needs, was criticized upon its development primarily for its poor scalability as well as intensive use of computing power resulting in significant power consumption [8] [9]. Blockchain implementations of the two most popular cryptocurrencies, Bitcoin and Ether, are currently facing this problem. As a solution, alternative consensus algorithms have been developed and proposed, however, each brings with itself certain advantages and disadvantages [8]. As mentioned in the previous section, currently most used consensus algorithms are PoW, PoS and DPoS, and in this chapter an analysis of each of them will be performed, followed by a comparative analysis. It is important to mention that the consensus mechanism of the Ethereum blockchain mechanism is in process of transition from PoW to PoS [15].

3.1. PROOF OF WORK

Proof of work is a consensus algorithm that relies on performing computer-intensive operations. This way, the participant in the network guarantees that he has done enough work to be worthy of capturing the transaction on the blockchain, while nodes in the network compete to perform such an operation faster.

The process is organized in such a way that the participant in the network who has successfully completed the work attaches evidence for other members of the network to confirm the authenticity of his contribution. The mentioned computer-intensive work is called mining, and after the network participants have confirmed the performed work, the node is being rewarded with cryptocurrency serving as the origin for the mining analogy [1] [16]. This approach to consensus relies on the assumption that more than half of the nodes in the network are honest. That way, if someone possessed more than half the computer power of the network, he would be able to compromise the data. Such a form of attack is by its nature called "51% attack". The additional limitation of this approach relates to costs in terms of power consumption and hardware requirements [8]. The pronounced hardware needs are the result of the complexity of operations performed by nodes, which negatively affects the time required to process the transaction. However, this form of complexity makes such an attack difficult and unprofitable in large blockchains, such as Bitcoin [1]. Consequentially, the main problem that arises when using such an algorithm relates to the scalability of the network [18].

3.2. PROOF OF STAKE

Unlike PoW, where network participants compete using their computing power to be selected to write data to the blockchain, and are rewarded for that, PoS is a consensus algorithm stating that the decision on which computer authors a new blockchain block directly depends on the stake that network participant has accumulated. This form of stake corresponds to a number of cryptocurrency coins that are locked, i.e., invested in the network. In that sense, participants who own large amounts of coins have an advantage over others. The first cryptocurrency to apply this approach was Peercoin in 2012 [8]. This process requires information about the coin possession of each of the participants, as well as the amount of time spent in their possession. Participants are required to stake more coins than they can be rewarded upon adding a transaction on the blockchain. In case of detecting a transaction that is considered to be fraudulent, the network confiscates all the coins that are being staked from the participant who tried to carry out such a form of attack. The advantage of this approach is that it is not as hardware-intensive as PoW, and therefore more environmentally friendly. It is important to note that this approach also relies on computing power when generating the block, but significantly less than is the case with PoW. Bearing in mind that participants who own more coins have a higher chance of adding transactions to the blockchain and thus be rewarded with cryptocurrencies, this process potentially makes them richer from the point of view of cryptocurrency as the time goes by. That way, a member who owns a significant number of coins could endanger the network [8]. Also, it should be taken into account that the possession of so many coins locked could represent an extremely large monetary representation of the cryptocurrency. If such a member would jeopardize the network, it would negatively affect the market value of the cryptocurrency, which would in turn jeopardize his own profit, thus making the "attack of 51%" less likely than in PoW blockchain implementations. Although unlikely, such attacks could be subtle and difficult to detect.

3.3. DELEGATED PROOF OF STAKE

The DPoS algorithm is the successor to the PoS algorithm, with significant improvements in terms of transaction execution speed and network scalability, first proposed in 2014 by Daniel Larimer [17]. This approach utilizes a significantly smaller number of nodes to maintain network security and add new blocks, thus significantly increasing the speed of execution of new transactions, whose time is often fixed and much smaller than those using PoW or PoS [17]. A small number of participants who ensure the operation of the network is enabled by providing a voting system by the stakeholders. The stakeholder is a special member of the network who has staked coins, an approach that is inherited from PoS. As is the case with PoS, such a member proves its credibility to participate. However, this participation process does not imply directly submitting and validating transactions but participates in the voting process for the node that plays that role. Voters with the largest number of coins have the greatest voting power, and after voting a certain number of so-called witnesses are selected to validate the transactions and write them on the blockchain. After the successful transaction execution and validation, witnesses are rewarded with digital coins that are also distributed proportionally to their voters. The entire process is monitored by specialized nodes called delegates, who, among other things, can propose a change in block size, transaction costs, the amount of money that selected witnesses will be rewarded for participating in transactions, and more. Delegates are also elected by voters. The primary motive of this approach as an improvement of PoS is to reduce the influence of centralized entities that have a significant number of coins in their possession. Also, having in mind that the number of nodes that process and validate transactions is significantly lower, the transaction processing is faster up to several times [17]. However, although the influence of central entities is reduced, the blockchain network itself is more centralized in terms of the number of nodes that have the privilege of performing transactions than is the case with PoW and PoS.

4. COMPARATIVE ANALYSIS

The first analysed parameter is the amount of necessary computational resources, given that network nodes are using their computational power while adding pieces of data to a blockchain, being awarded for doing so with cryptocurrency. Figure 1 shows the analysis of the three used algorithms in terms of hardware load.

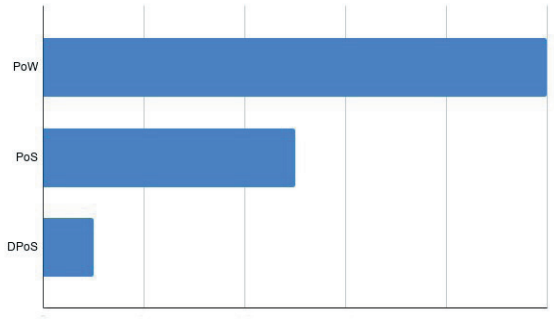

Figure 1 - Hardware load of network participants

PoW uses the most amount of computing power, while DPoS uses the least, which gives DPoS a significant advantage over other algorithms.

One of the key parameters of these algorithms, which directly affects the performance of the network, is the number of nodes participating in the validation process of the credibility of the proposed block. From the point of view of the observed algorithms, only DPoS works with predefined fixed (usually around 20) nodes, while PoS and PoW rely on the entire network [17]. The more nodes are involved in the transaction validation process, the more decentralized the network is considered, and consequently, the more secure it is. In this regard, it is concluded that PoW and PoS promote higher levels of decentralization compared to DPoS.

Number of participants	PoW	PoS	DPoS
Entire network	x	x	
Fixed (20)			x

Table 1 - Number of nodes in the network participating in block validation

In addition to the analysis based on one parameter, very useful indicators are comparative analysis based on multiple parameters.

Decentralization and scalability are often seen as key attributes of a blockchain network. Figure 2 shows the results of this comparison.

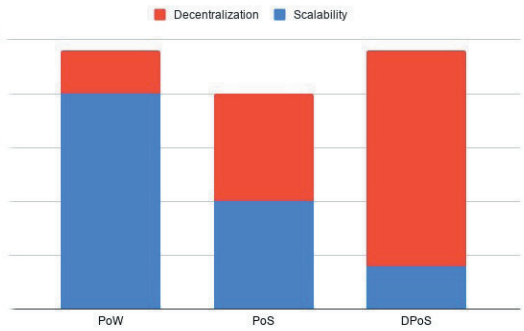

Figure 2 - Attributes of the blockchain network (scalability/decentralization)

The conclusion to be drawn is that networks that are highly scalable are very poorly decentralized except in the case of PoS where this ratio tends to be more neutral. Thus, deciding which algorithm is better directly depends on the need for a centralization / scalability ratio. It's worth noting that private blockchain networks might be a more suitable match for DPoS given that they by definition are less centralized.

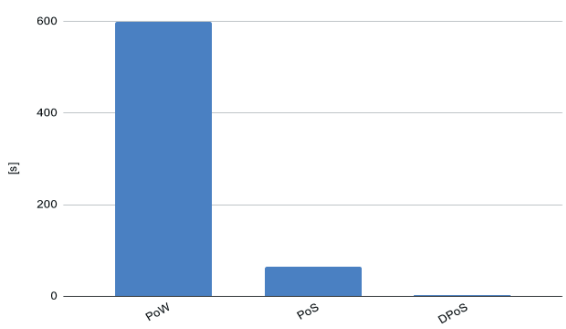

Figure 3 - Block addition time

The key parameter, if the network speed is observed, is the time required to add a block in the blockchain. Figure 3 portrays how this time is the highest for networks that use PoW, being ten times longer than what is necessary for PoS. On the other hand, in PoS this time is twenty times longer than in DPoS [17].

In that sense, from the point of view of the time required to write a block on a blockchain, DPoS gives the best results. Each of the mentioned algorithms comes with its advantages and disadvantages and therefore the selection process of these algorithms should be done carefully, in accordance with the case of use that a specific blockchain is trying to solve.

5. CONCLUSION

This paper presents a comparative analysis of the three most popular consensus algorithms used to prove the data integrity within a blockchain. Thus, for the purposes of this paper, Proof of Work, Proof of Stake and Delegated Proof of Stake were selected. These algorithms were observed and compared with each other from different aspects in order to show the comparative advantages and disadvantages of each other. A number of parameters were analysed and comparative results were presented graphically. The analysis shows that there is a great diversity in the optimization of several criteria by which algorithms can be described. It is concluded that certain algorithms in accordance with their properties are better or worse for specific practical applications. Further work will be focused on the analysis of additional algorithms and modification of existing ones in order to improve their characteristics.

REFERENCES

[1] N. Satoshi, „Bitcoin: A peer-to-peer electronic cash system," 2008.

[2] D. Chaum, „Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups," University Of California, 1982.

[3] S. Haber i W. S. Stornetta, „How to Time-Stamp a Digital Document," u *Advances in Cryptology-CRYPTO' 90*, Berlin, 1991.

[4] PengZhang, D. C.Schmidt, JulesWhite i Gunther-Lenz, „Blockchain Technology Use Cases in Healthcare," *Advances in Computers,* t. 111, pp. 1-41, 2018.

[5] B. K. Mohanta, S. S. Panda i D. Jena, „An Overview of Smart Contract and Use Cases in Blockchain technology," u *International Conference on Computing and Networking Technology (ICCNT*), Bengaluru, 2018.

[6] N. Malenčić, „PRIMENA ETHEREUM BLOKČEJN PLATFORME ZA RAZVOJ DECENTRALIZOVANE APLIKACIJE ZA GLASANJE," *Zbornik radova fakulteta tehničkih nauka*, pp. 1910-1913, 2020.

[7] S. S. Hazari i Q. H. Mahmoud, „Improving Transaction Speed and Scalability of Blockchain Systems via Parallel Proof of Work," *Future Internet*, t. 12, 2020.

[8] S. Sayeed i H. Marco-Gisbert, „Assessing Blockchain Consensus and Security Mechanisms against the 51% Attack," *Applied Sciences*, t. 9, 2019.

[9] Q. Zhou, H. Huang, Z. Zheng i J. Bian, „Solutions to Scalability of Blockchain: A Survey," *IEEE Access*, t. 8, pp. 16440-16455, 2020.

[10] M. Nofer, P. Gomber i O. Hinz, „Blockchain," *Business & Information Systems Engineering*, t. 59, br. 3, pp. 183-187, 2017.

[11] S. Pongnumkul, C. Siripanpornchana i S. Thajchayapong, „Performance Analysis of Private Blockchain Platforms in Varying Workloads," u *International Conference on Computer Communications and Networks (ICCCN)* , Vancouver, 2017.

[12] K. Christidis i M. Devetsikiotis, „Blockchains and Smart Contracts for the Internet of Things," *IEEE Access*, t. IV, pp. 2292 - 2303, 2016.

[13] R. M. Parizi, Amritraj i A. Dehghantanha, „Smart Contract Programming Languages on Blockchains: An Empirical Evaluation of Usability and Security," u *International Conference on Blockchain, Seattle*, 2018.

[14] G. Angeris, H.-T. Kao, R. Chiang i C. N. a. T. Chitra, „An analysis of Uniswap markets," arXiv, 2021.

[15] O. Ogino, „Proof-of-stake (PoS)," Ethereum Org, 16 April 2021. [Na mreži]. Available: https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/. [Poslednji pristup 29 May 2021].

[16] A. M. Antonopoulos i G. Wood, Mastering Ethereum: Building Smart Contracts and DApps, O'Reilly Media, 2018.

[17] F. Yang, W. Zhou, Q. Wu, R. Long, N. N. Xiong i M. Zhou, „Delegated Proof of Stake With Downgrade: A Secure and Efficient Blockchain Consensus Algorithm With Downgrade Mechanism," *IEEE Access,* t. 7, pp. 118541 - 118555, 2019.