Methodology for Choosing a Consensus Algorithm for Blockchain Technology

Viktoriia Zhebka[1], Serhii Zhebka[1], Tetiana Bazhan[1], Pavlo Skladannyi[2],
and Volodymyr Sokolov[2]

[1] *State University of Information and Communication Technologies, 7 Solomenskaya str., Kyiv, 03110, Ukraine*
[2] *Borys Grinchenko Kyiv University, 18/2 Bulvarno-Kudriavska str., Kyiv, 04053, Ukraine*

Abstract

Blockchain technology is rapidly integrating into various spheres of human activity. Private companies, government agencies, and international organizations are gradually adapting this technology to solve a wide range of tasks. The main areas of its use include financial transactions, document management, digital identification, control of logistics links, and tokenization of physical and classical financial assets. The more a technology develops, the more it needs to be updated and improved. For blockchain, the chosen consensus algorithm is very important. There is a need to ensure control over data and resources and their copies on different nodes to avoid conflicts between nodes. After all, any conflict between nodes can lead to inefficient and inconsistent data storage. As a blockchain is a specialized type of database that stores this data by distributing it among several completely independent nodes, i.e. computers or devices, blockchains allow data to be added to databases and make it impossible to attempt to change or delete them. Therefore, this article is based on the study of the criteria that can help in the selection of a consensus algorithm. Four main criteria are identified, which in combination, allow us to select a consensus algorithm more accurately. The main selection criteria are energy consumption, decentralization, security, and bandwidth. Each feature of these criteria has been considered during the study and highlighted in this article. It is very important to combine different criteria and their parameters to choose the most successful consensus algorithm. Different approaches make it possible to find the most optimal option. Based on the introduced criteria and the proposed methodology, a program for selecting the optimal consensus algorithm has been created using the Python programming language.

Keywords

Consensus algorithm, energy consumption, bandwidth, decentralization, security, blockchain.

1. Introduction

Blockchains are decentralized, meaning that data can be distributed across multiple host servers, which distinguishes them from conventional databases. Decentralization is the main feature of blockchain.

Since control over data or resources is shared among several nodes simultaneously, it makes it very difficult for an attacker to delete or use resources. The process of changing data or using resources can only take place with the consent of the majority of nodes in the blockchain if the blockchain is large and contains sufficiently independent nodes, which makes it impossible for an attacker [1].

Blockchain decentralization also comes with a social and technical challenge, which is maintaining consensus between nodes. Consensus maintenance can ensure that all participants agree with the decisions made by the network [2, 3].

Consensus maintenance is very important because, without it, copies of data on different

DECaT'2024: Digital Economy Concepts and Technologies, April 4, 2024, Kyiv, Ukraine

EMAIL: viktoria_zhebka@ukr.net (V. Zhebka); szhebka@hotmail.com (S. Zhebka); tetiana.olexandrivna@gmail.com (T. Bazhan); p.skladannyi@kubg.edu.ua (P. Skladannyi); v.sokolov@kubg.edu.ua (V. Sokolov)
ORCID: 0000-0003-4051-1190 (V. Zhebka); 0009-0007-4620-9888 (S. Zhebka); 0009-0007-6594-1695 (T. Bazhan); 0000-0002-7775-6039 (P. Skladannyi); 0000-0002-9349-7946 (V. Sokolov)

nodes may conflict with each other, leading to inefficient and inconsistent data storage. Consensus also makes it possible to update the underlying blockchain protocol, i.e. the rules for node interaction and regulation of its organization. If it became necessary to modify the protocol due to security or performance issues, all nodes would have to agree to accept the change, as different nodes cannot use different protocols in the same blockchain.

Because all nodes in a blockchain are decentralized and work independently, maintaining consensus creates a complex problem, which different types of blockchains have solved in different ways. Different solutions for maintaining consensus between nodes provide us with technical innovations for further updates of algorithms for blockchain technology.

2. Research Results

The first blockchain networks used the Proof-of-Work (PoW) consensus mechanism, the main disadvantages of which are high energy costs, low network bandwidth, and high transaction costs. Alternative mechanisms have been developed to overcome these issues. Currently, the most common replacement for PoW is the Proof-of-Stake (PoS) consensus mechanism.

The essence of this approach is that to generate a new block, the holder of the validator node must stake a certain number of the native tokens and interact with other nodes to reach a consensus on the chain. In case the validator node engages in malicious activity, it risks losing the blocked tokens partially or completely.

This approach, inherently, has several vulnerabilities; the main one is the possibility of accumulating a significant number of tokens with a small number of related holders, which can lead to catastrophic consequences for the entire network. This problem is called capital centralization or oligopoly.

A typical solution to ensure the consensus of PoS networks is a scheme for distributing rewards and penalties to validator nodes.

The purpose of this paper is to analyze the criteria and parameters of a blockchain network to determine the optimal consensus algorithm.

A successful consensus algorithm should help a blockchain application achieve its goal. The purpose of the blockchain is to provide a tool for decentralized decision-making. The complex nature of blockchain consensus stems from its original goal of making decisions without a central authority. Therefore, the level of decentralization of the consensus algorithm is included in the evaluation criteria. A consensus algorithm with a higher level of decentralization is considered good [4].

Decentralization plays a key role in a blockchain network as it determines the level of power and control distribution among participants. Let’s consider several criteria that can be taken into account when choosing a consensus algorithm in terms of decentralization:

- Level of equality (how equally the power is distributed among the network participants, the fewer centralized control points there are and, the more decentralized is the system);
- Decentralized decision-making mechanisms (how decisions are made about the direction of the network development and whether there are mechanisms, which allow participants to contribute to the decision-making process).
- Scalability of decentralization (how the system decentralizes as the number of participants and the volume of transactions increase; and whether the network can remain decentralized over time and grow in scale).
- Fault tolerance to attacks (i.e. how the system responds to attempts to hack into the decentralized structure and whether there are mechanisms to prevent concentration of power or a controlled attack).
- The number of nodes (the more nodes in the network, the more decentralized the system can be considered, but it is also important to consider how these nodes are selected and controlled).
- Sybil Resistance (how the system prevents attacks in which an attacker can create many artificial identities to gain control over the network).
- Algorithmic implementation (how the consensus algorithm promotes decentralization) [5–11].

Taking these criteria into account helps to show that the chosen consensus algorithm promotes the highest possible level of decentralization in the blockchain network.

Another important criterion is whether the consensus algorithm can fulfill its own goal, which is to achieve consensus. In the context of blockchain and cryptocurrencies, this can be defined as the speed at which the algorithm reaches consensus or the amount of bandwidth. For example:

- Fast action and number of transactions per second (TPS) (i.e. how fast a particular consensus algorithm can be processed and how many transactions can be processed in one second. This is especially important for blockchain networks that have a high transaction flow).
- Scalability (how well the algorithm scales when the number of participants and the flow of transactions increase).
- Processing multitasking (whether the algorithm can efficiently process many transactions simultaneously).
- Latency (how quickly transactions can be confirmed in the network).
- Resource dependence (the system must be efficient in terms of resource use).
- Network efficiency (whether the algorithm works well in a network with a large number of participants and a large amount of data).
- Protocol flexibility (the ability to adjust algorithm parameters to achieve optimal bandwidth in specific conditions) [12–19].

These criteria help to establish that the selected consensus algorithm meets the network capacity requirements and ensures efficient transaction processing in the blockchain system.

The blockchain network criteria play an important role in the selection of a consensus algorithm and in the process of developing a blockchain solution. Let's consider, in detail, the formulas for calculating the main blockchain network metrics, which will allow us to determine the optimal consensus algorithm:

1. Transaction speed: This criterion determines how quickly the network can process and confirm transactions. It is important for applications that require high transaction speeds, such as payment systems or micropayments.

Metrics: Number of Transactions Per Second (TPS), transaction confirmation time.

The calculation of transaction speed in the form of formulas can look like this:

$$v_T = \frac{n}{t}, \tag{1}$$

where v_T is the speed of transactions; n is the number of transactions that have been successfully processed over a certain period; t is the time interval, during which the transactions have been processed.

2. Scalability: Scalability determines how easily the network can be increased in size and load to serve more users and transactions without losing performance.

Metrics: Infrastructure to scale up the network, network bandwidth, horizontal and vertical scalability.

The formula for calculating the scalability coefficient:

$$M = \frac{P}{\text{к}}, \tag{2}$$

where M is the scalability coefficient; P is the maximum number of transactions that the network can process within one second; k is the average number of active users in the network.

3. Decentralisation: This criterion indicates the degree of distributed control and participation in the network. A higher level of decentralization means greater independence and security.

Metrics: Number of nodes, participating in the consensus, concentration of power, location of geographically different nodes.

To find the decentralization ratio, use the following formula:

$$D = 1 - K, \tag{3}$$

where D is the decentralization factor and K is a value that determines the degree of centralization of control in the network, it can be a numerical value from 0 (full decentralization) to 1 (full centralization).

4. Security: Security is defined as the level of protection a network has against attacks and misuse. The data must be securely protected from unauthorized access.

Metrics: Level of cryptographic security, resistance to 51% attack, protection against double-spending, vulnerability detection, and remediation.

The formula for calculating the security factor:

$$S = R_s(1 - R_a), \quad (4)$$

where S is the security factor, R_s is the level of cryptographic security, i.e. an assessment of the level of data protection in the network, which can be a numerical value from 0 (no security) to 1 (high security); R_a is the risk of attack, i.e. the probability of an attack on the network.

5. Costs: Costs include the cost of operating the network, including equipment, electricity, and transaction fees. Low costs can be important for maintaining network stability and attracting users [20–24].

Metrics: Network maintenance costs, transaction fees, block mining costs (in the case of PoW).

The formula for calculating the cost ratio:

$$N = \frac{N_i}{m}, \quad (5)$$

where N is the cost coefficient; N_i is the total cost of network maintenance, the total cost of maintaining and mining blocks in the network; m is the number of transactions, the total number of processed transactions in the network.

Now consider the calculation of parameters for two imaginary blockchain networks.

Network A (Proof of Work (PoW):

1. The number of miners: 1000.
2. Transactions flow per second (TPS): 100.
3. Block size: 1 MB.
4. Time between blocks: 10 minutes.

Network B (Proof of Stake—PoS):

1. Number of active master nodes: 500.
2. Transactions flow per second (TPS): 200.
3. Block size: 2 MB.
4. Time between blocks: 5 minutes.

Metric calculation—Transaction speed (TPS):

For Network A (PoW):

$$v_T = (100*1{,}000)/600 = 166{,}67$$

For Network B (PoS):

$$v_T = (200*500)/300 = 333{,}33$$

As can be seen, the "Transaction Rate" (TPS) metric for network B (PoS) is higher than for network A (PoW), which indicates that network B can process more transactions per second. According to this data, network B may be more suitable for applications that require high transaction speeds, while network A has more miners and possibly more security due to PoW.

Scaling Score:

For Network A (PoW):

M = (10 minutes/block)*(1 block/10 minutes) = 1 block/minute.

For Network B (PoS):

M = (5 minutes/block)*(1 block/5 minutes) = 1 block/minute.

Decentralization Index:

For Network A (PoW): Decentralisation is difficult to calculate without up-to-date concentration data.

For Network B (PoS):

D = 1–0.9 = 0.1.

Security Score:

For Network A (PoW): The security level will be high due to the powerful hash power.

For Network B (PoS): Security can be determined based on the level of cryptographic security and the risk of attack, which are difficult to calculate without specific data.

Cost Index:

For Network A (PoW):

The cost of PoW includes the cost of equipment and electricity to mine the blocks. The number of transactions is also difficult to estimate without specific data.

For Network B (PoS):

PoS costs include master node maintenance and transaction fees.

A consensus algorithm is considered more secure if it can protect against different types of security threats.

Therefore, security is a critical aspect when choosing a consensus algorithm in blockchain technology. Here are some key security criteria:

- Attack resistance (how well the system can resist various types of attacks, such as double costs, white hat attacks, consensus attacks, etc;).
- Decentralization (the gradient of decentralization can determine how difficult it is to carry out successful attacks on the system, the more different participants in the network, the more difficult it is to interfere with the consensus).
- Key protection methods (what methods are used to store and protect the private keys of network participants and the security of the key storage system).

- Fault tolerance (restoring the system after errors or attacks is important for the continuous operation of the network).
- Algorithmic strength (determining the strength of the cryptographic algorithms, which are used in the consensus algorithm. For example, if a hash function is used, how resistant it is to collisions and attacks).
- Sybil Attack Resistance (how the system prevents attacks in which one participant can create many pseudo-identities to dominate the network).
- Active cooperation (Byzantine Fault Tolerance–BFT) (the requirement for the network to be immune to attacks that may lead to a discrepancy in information between participants).
- Protocol upgrades and changes (how easy it is to implement changes to the consensus protocol, and how much this can affect network security) [25–27].

Finally, one should not consider only theoretical aspects. There is another criterion—the energy consumption of the algorithm. If an algorithm consumes too much energy, it should be changed and more environmentally friendly options should be considered.

The following energy consumption criteria for choosing a consensus algorithm in blockchain technology should be considered:

Proof of Work (PoW):

- Computational complexity (the more difficult the task is for miners, the more energy is consumed).
- Algorithm efficiency (some PoW algorithms may be more energy efficient than others).

1. Proof of Stake (PoS):

- Selective efficiency (the less currency a participant has, the less energy he uses).
- Methods for controlling misuse (it is important to have mechanisms to prevent concentration of power that may affect the effectiveness of PoS).

2. Delegated Proof of Stake (DPoS):

- Chosen legitimacy (some participants may spend more energy to obtain delegate status).
- Flexibility of the voting policy (if the voting system is not efficient, it can lead to an incorrect distribution of power and energy costs).

3. Proof of Burn and other alternatives:

- Spending strategies (determining exactly how currency is spent in the consensus process and how this affects energy costs.
- Innovative approaches (alternative methods such as Proof of Space (PoSpace) or Proof of Time (PoT) may offer lower energy costs).

However, the energy consumption criteria must be balanced with other important aspects, such as security, decentralization, and bandwidth, when choosing a consensus algorithm for blockchain technology.

Here is a comparative description of consensus algorithms for different types of cryptocurrencies (Table 1).

Table 1
Characteristics of consensus algorithms

Cryptocurrency	Type	Security	Decentralisation	Energy consumption	Bandwidth
Dash	Hibrid	Medium	Medium	Medium	OK
Peercoin	Hibrid	Medium	Medium	Low	Not So Fast
Verus coin	Hibrid	Medium	Medium	Low	OK
Decred	Hibrid	Hight	Hight	Medium	OK
Stratis	Hibrid	Medium	Medium	Medium	Fast
Bitcoin	PoW	Hight	Hight	Hight	Not So Fast
Conflux	PoW	Hight	Medium	Low	Very Fast
Ethereum Classic	PoW	Medium	Medium	Medium	Fast
Monero	PoW	Hight	Hight	Medium	OK
Dogecoin Litecoin	PoW	Medium	Medium	Medium	OK
Ethereum	PoS	Medium	Hight	Low	Fast
Polygon	PoS	Hight	Medium	Low	Fast
TON coin	PoS	Medium	Medium	Low	Fast
Solana	PoS	Hight	Medium	Hight	Very Fast
Cardano	PoS	Hight	Medium	Low	Fast

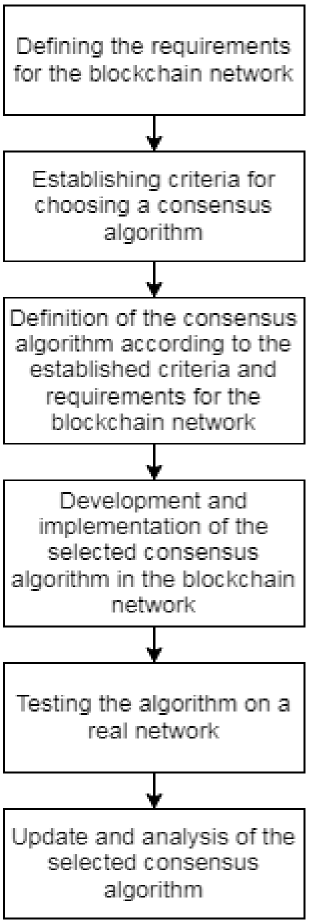
Defining the requirements for the blockchain network
Establishing criteria for choosing a consensus algorithm
Definition of the consensus algorithm according to the established criteria and requirements for the blockchain network
Development and implementation of the selected consensus algorithm in the blockchain network
Testing the algorithm on a real network
Update and analysis of the selected consensus algorithm

Figure 1: Definition of the consensus algorithm

The main steps of determining the consensus algorithm by the selected criteria are shown in Fig. 1.

3. Discussion

The obtained results formed the basis of the methodology for determining the consensus algorithm for the blockchain network. Based on the obtained data, a program for determining the optimal algorithm has been created in the Python programming language. The program allows choosing one of the available consensus algorithms by the established criteria. The program can be extended to take into account more metrics and conditions for choosing an algorithm.

4. Conclusion

The criteria for helping to select a consensus algorithm, by reviewing popular algorithms and providing a solution in the form of a decision tree have been presented in this article. This solution is very useful for the further selection of consensus algorithms and the development of blockchain technology.

In general, the criteria, discussed in this article, make it clear how important the method of selecting a consensus algorithm is. After all, a successfully selected consensus increases the efficiency of blockchain technology.

This study is limited in time. For the whole population, the consensus algorithm may be useful to study more algorithms and create a larger decision tree, as they all have their characteristics. Also, this article is an impulse to dive deeper and compare performance using benchmarking.

For any future work, it would be interesting to have a study on the selection of a consensus algorithm and it is possible to choose a wider list of criteria or reduce it to a minimum. In addition, the blockchain application industry is developing rapidly and new algorithms are being created that can quickly replace the old ones on the market. There is always a need for future research, so it is a necessity to keep up to date with the latest developments in consensus algorithms and blockchain technology.

References

[1] V. Buriachok, V. Sokolov, P. Skladannyi, Security Rating Metrics for Distributed Wireless Systems, in: Workshop of the 8th Int. Conf. on "Mathematics. Information Techno-logies. Education:" Modern Machine Learning Technologies and Data Science, vol. 2386 (2019) 222–233.

[2] B. Bebeshko, et al., Application of Game Theory, Fuzzy Logic and Neural Networks for Assessing Risks and Forecasting Rates of Digital Currency, Journal of Theoretical and Applied Information Technology 100(24) (2022) 7390–7404.

[3] V. Sokolov, P. Skladannyi, H. Hulak, Stability Verification of Self-Organized Wireless Networks with Block Encryption, in: 5th International Workshop on Computer Modeling and Intelligent Systems, vol. 3137 (2022) 227–237.

[4] F. Kipchuk, et al., Assessing Approaches of IT Infrastructure Audit, in: IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (2021). doi: 10.1109/picst54195.2021.9772181.

[5] B. Sriman, et al., Blockchain Technology: Consensus Protocol Proof of Work and Proof of Stake, Intelligent Computing and Applications (2020) 395–406. doi: 10.1007/978-981-15-5566-4_34.

[6] S. Bamakan, et al., A Survey of Blockchain Consensus Algorithms Performance Evaluation Criteria, Expert Systems with Applications 154 (2020) 113385. doi: 10.1016/j.eswa.2020.113385.

[7] H. Cho, ASIC-Resistance of Multi-Hash Proof-of-Work Mechanisms for Blockchain Consensus Protocols, IEEE Access 6 (2018) 66210–66222. doi: 10.1109/ACCESS.2018.2878895.

[8] T. Duong, et al., 2-Hop Blockchain: Combining Proof-of-Work and Proof-of-Stake Securely, Computer Security – ESORICS 2020 (2020) 697–712. doi: 10.1007/978-3-030-59013-0_34.

[9] A. Guru, et al., A Survey on Consensus Protocols and Attacks on Blockchain Technology, Applied Sci. 13(4) (2023) 2604. doi: 10.3390/app13042604.

[10] S. King, S. Nadal. PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake, (2012) 1–6.

[11] Y. Liu, et al., Hybrid Consensus Protocols and Security Analysis for Blockchain, International Conference on Data Analytics, Computing and Artificial Intelligence (ICDACAI) (2022). doi: 10.1109/ICDACAI57211.2022.00046.

[12] B. Lucas, R. V. Paez, Consensus Algorithm for a Private Blockchain, IEEE 9th International Conference on Electronics Information and Emergency Communication (ICEIEC) (2019). doi: 10.1109/ICEIEC.2019.8784500.

[13] A. Mackenzie, Memcoin2: A Hybrid Proof-of-Work, Proof-of-Stake Crypto-Currency (2013).

[14] V. Malinov, et al., Biomining as an Effective Mechanism for Utilizing the Bioenergy Potential of Processing Enterprises in the Agricultural Sector, Cybersecurity Providing in Information and Telecommunication Systems, Vol. 3421 (2023) 223–230.

[15] D. Mingxiao, et al., A Review on Consensus Algorithm of Blockchain, IEEE International Conference on Systems, Man, and Cybernetics (2017). doi: 10.1109/SMC.2017.8123011.

[16] R. Pass, E. Shi, Hybrid Consensus: Efficient Consensus in the Permissionless Model, Initiative for CryptoCurrency and Contracts (2016) 1–55. doi: 10.4230/LIPIcs.DISC.2017.39.

[17] S. King, S. Nadal, PPCoin: Peer-to-Peer Crypto-Currency with Proof-ofStake (2012).

[18] L. Shi, et al., Pooling Is Not Favorable: Decentralize Mining Power of POW Blockchain Using Age-of-Work, IEEE Transactions on Cloud Computing 11(3) (2022). doi: 10.1109/TCC.2022.3226496.

[19] B. Sriman, et al., Blockchain Technology: Consensus Protocol Proof of Work and Proof of Stake, Intelligent Computing and Applications (2020) 395–406. doi: 10.1007/978-981-15-5566-4_34.

[20] Y. Yu, Analysis of POW in Bitcoin and POS in Peercoin, Highlights in Science, Engineering and Technology 39 (2023) 784–788. doi: 10.54097/hset.v39i.6645.

[21] Q. Zhang, et al., Blockchain Model Testing and Implementation Based on Improved PBFT Consensus, 11th IEEE International Conference on Intelligent DataAcquisition and Advanced Computing Systems: Technology and Applications (IDAACS) (2021). doi: 10.1109/idaacs53288.2021.9660959.

[22] S. Zhang, J.-H. Lee, Analysis of the Main Consensus Protocols of Blockchain, ICT Express 6(2) (2020) 93–97. doi: 10.1016/J.ICTE.2019.08.001.

[23] W. Zhao, et al., On Peercoin Proof of Stake for Blockchain Consensus, 3rd International Conference on Blockchain Technology (2021) 129–134. doi: 10.1145/3460537.3460547.

[24] W. Zhao, et al., On Peercoin Proof of Stake for Blockchain Consensus, 3rd International Conference on Blockchain Technology (2021) 129–134. doi: 10.1145/3460537.3460547.

[25] V. Zhebka, et al., Optimization of Machine Learning Method to Improve the Management Efficiency of

Heterogeneous Telecommunication Network, Cybersecurity Providing in Information and Telecommunication Systems Vol. 3288 (2022) 149–155.

[26] Z. Zheng, et al., An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends, IEEE International Congress on Big Data (BigData Congress) (2017). doi: 10.1109/BIGDATACONGRESS.2017.85.

[27] Z. Zheng, et al., An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends, IEEE International Congress on Big Data (BigData Congress) (2017). doi: 10.1109/BIGDATACONGRESS.2017.85.