УДК 004.65:004.75 DOI: 10.31673/2412-4338.2024.019904

Zhebka Serhii
State university of information and communication technologies, Kyiv
ORCID 0009-0007-4620-9888

Vlasenko Vadym
State university of information and communication technologies, Kyiv
ORCID 0000-0002-9329-5914

Aronov Andrii
State university of information and communication technologies, Kyiv
ORCID 0009-0000-7868-8341

Kolodiuk Andrii
State university of information and communication technologies, Kyiv
ORCID 0009-0001-1724-7531

ADDRESSING THE SELECTION DILEMMA OF CONSENSUS ALGORITHM IN DISTRIBUTED SYSTEMS

Abstract. *Consensus algorithms serve as the backbone of distributed systems, enabling agreement among participants in decentralized environments. Fault tolerance, ensuring system resilience in the face of participant failures or malicious activities, stands as a cornerstone for these algorithms. In contrast to centralized systems where decision-making authority rests with a single entity, decentralized systems, like blockchain, introduce unique challenges in achieving consensus among disparate and potentially untrustworthy participants. This article conducts an exhaustive exploration of consensus algorithms, focusing primarily on Proof of Work (PoW), Proof of Stake (PoS), and Delegated Proof of Stake (DPoS). A thorough analysis of the advantages, disadvantages, and operational intricacies of each algorithm is provided, shedding light on their applicability across various use cases. Practical examples and optimization strategies are delineated to elucidate the operational nuances and aid stakeholders in algorithm selection. Additionally, a comprehensive methodology for consensus algorithm selection is outlined, emphasizing the paramount importance of considering specific criteria to ensure optimal performance in decentralized ecosystems. Supplementary figures depicting the selection process and decision tree for consensus algorithm determination accompany the analysis, serving as valuable resources for researchers, developers, and stakeholders navigating the complexities of decentralized consensus mechanisms. This article aims to provide a holistic understanding of consensus algorithms, empowering stakeholders to make informed decisions and foster innovation in decentralized systems.*

Keywords: *decentralized systems, consensus algorithms, blockchain, fault tolerance, energy efficiency, distributed network, information technologies.*

Жебка Сергій Валентинович
Державний університет інформаційно-комунікаційних технологій, Київ
ORCID 0009-0007-4620-9888

Власенко Вадим Олександрович
Державний університет інформаційно-комунікаційних технологій, Київ
ORCID 0000-0002-9329-5914

Аронов Андрій Олексійович
Державний університет інформаційно-комунікаційних технологій, Київ
ORCID 0009-0000-7868-8341

Колодюк Андрій Васильович
Державний університет інформаційно-комунікаційних технологій, Київ
ORCID 0009-0001-1724-7531

ВИРІШЕННЯ ДИЛЕМИ ВИБОРУ АЛГОРИТМУ КОНСЕНСУСУ У РОЗПОДІЛЕНИХ СИСТЕМАХ

Анотація. *Алгоритми консенсусу слугують основою розподілених систем, уможливлюючи досягнення згоди між учасниками в децентралізованих середовищах. Відмовостійкість, що забезпечує стійкість системи до збоїв або зловмисних дій учасників, є наріжним каменем цих алгоритмів. На відміну від централізованих систем, де повноваження щодо прийняття рішень належать одній особі, децентралізовані системи, такі як блокчейн, створюють унікальні проблеми в досягненні консенсусу між розрізненими і потенційно ненадійними учасниками. У цій статті проводиться вичерпне дослідження алгоритмів консенсусу, зосереджуючись насамперед на доказах роботи (PoW), доказах частки (PoS) та делегованих доказах частки (DPoS). Надається ретельний аналіз переваг, недоліків і операційних тонкощів кожного алгоритму, що проливає світло на їх застосовність у різних випадках використання. Наведено практичні приклади та стратегії оптимізації, щоб прояснити операційні нюанси та допомогти зацікавленим сторонам у виборі алгоритму. Крім того, описано комплексну методологію консенсусного вибору алгоритму, що підкреслює першорядну важливість врахування конкретних критеріїв для забезпечення оптимальної продуктивності в децентралізованих екосистемах. Аналіз супроводжується додатковими рисунками, що відображають процес вибору та дерево рішень для визначення алгоритму консенсусу, які слугують цінним ресурсом для дослідників, розробників та зацікавлених сторін, які орієнтуються в складнощах децентралізованих механізмів консенсусу. Ця стаття має на меті надати цілісне розуміння алгоритмів консенсусу, що дозволить зацікавленим сторонам приймати обґрунтовані рішення та сприятиме інноваціям у децентралізованих системах.*

Ключові слова: *децентралізовані системи, алгоритми консенсусу, блокчейн, відмовостійкість, енергоефективність, розподілена мережа, інформаційні технології.*

1. Introduction.

In recent years, the proliferation of distributed systems, particularly blockchain technology, has revolutionized the landscape of digital transactions and decentralized applications. At the heart of these systems lies the concept of consensus algorithms, which serve as the cornerstone for achieving agreement among participants in a decentralized environment. Consensus algorithms play a vital role in ensuring the integrity, security, and reliability of distributed systems by facilitating agreement on the validity of transactions and the state of the network.

The significance of consensus algorithms becomes particularly pronounced in decentralized systems, where there is no central authority to arbitrate disputes or enforce rules. Instead, consensus mechanisms enable participants, often operating in an adversarial and untrusting environment, to collectively validate transactions and agree on the state of the ledger. This decentralized consensus forms the basis of trust in blockchain networks, allowing them to function effectively without the need for intermediaries.

This article aims to provide a comprehensive overview of consensus algorithms, delving into their underlying principles, operational mechanisms, and comparative analysis. We will explore three prominent consensus algorithms: Proof of Work (PoW), Proof of Stake (PoS), and Delegated Proof of Stake (DPoS). Each algorithm presents unique advantages and challenges, catering to different use cases and operational requirements.

Through a thorough examination of these consensus algorithms, along with practical examples and optimization strategies, this article seeks to empower readers with the knowledge and insights

necessary to navigate the complexities of decentralized systems. By understanding the intricacies of consensus mechanisms, stakeholders can make informed decisions, drive innovation, and contribute to the advancement of decentralized technologies.

2. Research results.

The consensus algorithm is a fundamental mechanism in distributed systems, allowing users or machines to reach agreement in a decentralised environment. For these algorithms, it is very important to maintain fault tolerance - that is, the system remains functional even if some participants fail or act maliciously.

In a centralised system, decision-making and control are vested in a single authority. This central authority has the power to make unilateral changes without the need for a complex consensus process involving many stakeholders.

However, in a decentralised system such as blockchain, the dynamics change significantly. Here, the challenge is to achieve consensus in a distributed network, especially when the participants are unknown to each other and may be inherently distrustful. The need for consensus is particularly important when deciding which entries to make in a distributed ledger or database.

Table 1

Advantages and disadvantages of consensus algorithms

	Proof of Work (PoW)	**Proof of Stake (PoS)**	**Delegated Proof of Stake (DPoS)**
Advantages			
Decentralization	High	High	High
Security	High	High	High
Absence of "alienation"	Yes	Yes	Yes
Reliability	High	High	High
Efficiency	Can be energy-efficient	High	High
Scalability	Low	High	High
Disadvantages			
Energy Consumption	High	Low	Low
Hardware Costs	High	Low	Low
51% Attacks	Yes	Less likely	Less likely
Complexity	High	Low	Low
Promotes centralization	Yes	No	Yes

The main types of consensus algorithms:

Proof of Work (PoW) is a consensus algorithm employed to designate a miner for the subsequent block generation. Bitcoin relies on this PoW consensus algorithm. The fundamental concept of this algorithm involves resolving a intricate mathematical puzzle and swiftly providing the solution. Solving this mathematical puzzle demands significant computational resources, hence the node that achieves the solution promptly earns the privilege to mine the next block.

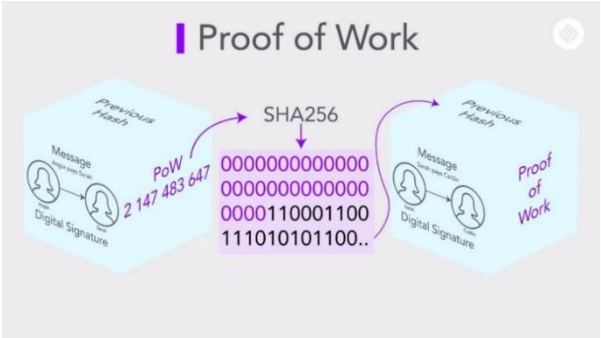

Fig.1. An example of the POW algorithm

Proof of Stake (PoS) stands out as the most prevalent alternative to PoW. Ethereum has transitioned from PoW consensus to PoS consensus. In this consensus algorithm variant, instead of investing in costly hardware to tackle a complex puzzle, validators commit a portion of their coins to the system by staking them. Subsequently, all validators commence block validation. They verify blocks by staking their tokens on those they deem suitable for addition to the chain. Depending on the blocks actually incorporated into the blockchain, validators receive rewards commensurate with their stakes, thus augmenting their stakes accordingly. Ultimately, a validator is selected to generate a new block based on their economic stake in the network. This way, PoS incentivizes validators through a reward mechanism to achieve consensus.

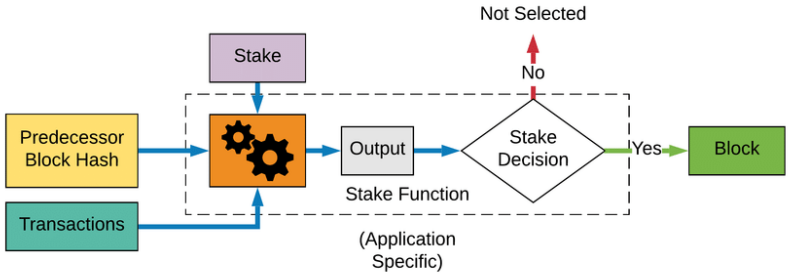

Fig.2. Example of PoS algorithm

Delegated Proof of Stake (DPoS) represents an alternative form of the Proof of Stake consensus algorithm. This particular consensus mechanism operates on the principle of vote delegation. Users transfer their voting rights to other users. Subsequently, the user responsible for block mining distributes rewards among those users who delegated their votes to them.

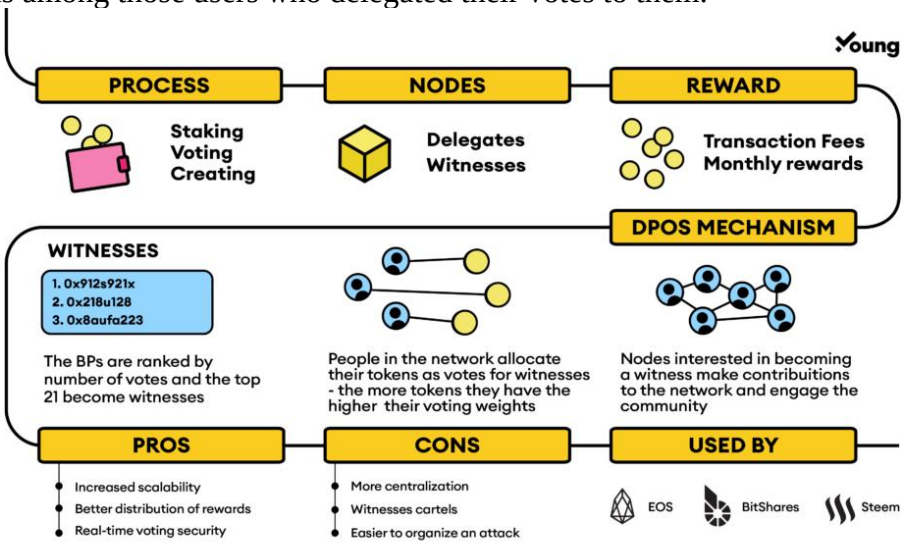

Fig.3. An example of DPoS algorithm

Proof of Work requires miners to perform complex computational tasks to validate new blocks. The most famous example of PoW is Bitcoin.

The formula for calculating the reward:

Block reward = Fixed block reward + Transaction fees

For Bitcoin, the fixed reward is halved every 210,000 blocks.

Optimising energy costs

You can optimise your energy costs by switching to energy-efficient hardware, such as ASIC miners that specialise in mining a specific cryptocurrency, reducing overall power consumption compared to general-purpose GPUs.

An example of a solvable algorithm for mining in the Bitcoin network:

$$Ch(X,Y,Z) = (X \wedge Y) \oplus (\bar{X} \wedge Z)$$

$$Maj(X,Y,Z) = (X \wedge Y) \oplus (X \wedge Z) \oplus (Y \wedge Z)$$

$$\sum_0 (X) = RotR(X,2) \oplus RotR(X,13) \oplus RotR(X,22)$$

$$\sum_1 (X) = RotR(X,6) \oplus RotR(X,11) \oplus RotR(X,25)$$

$$\sigma_0 (X) = RotR(X,7) \oplus RotR(X,18) \oplus RotR(X,3)$$

$$\sigma_1 (X) = RotR(X,17) \oplus RotR(X,19) \oplus RotR(X,10)$$

$RotR(A,n)$ denotes a circular right shift of n bits of binary word A

$ShR(A,n)$ denotes the right shift of n bits of binary word A.

$A \| B$ denotes the concatenation of binary words A and B.

Proof of Stake does not require miners to perform computational tasks, instead, the choice of a block for validation depends on the amount of cryptocurrency that the participant has blocked as collateral.

Reward calculation formula:

Reward per block=(Total blocked funds × Annual percentage)/Number of blocks per year

This formula may vary depending on the specific cryptocurrency, but the basic idea is to provide rewards according to the amount of funds blocked.

Since PoS does not require intensive computing, it is significantly more energy efficient than PoW. The optimisation consists in choosing cryptocurrencies that use PoS or its variations for mining or investing.

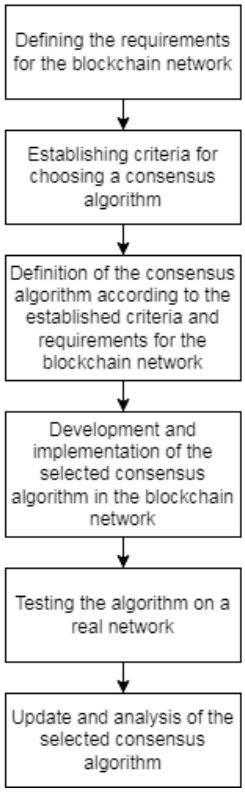

Fig. 4. Methodology for choosing a consensus algorithm

The process of selecting the consensus algorithm based on specified criteria is outlined in Figure 4.

The third block of the methodology for selecting a consensus algorithm can be visualized as a decision tree, guiding the selection of the most suitable algorithm according to all the criteria outlined in the problem statement. A simplified version of this decision tree is depicted in Figure 5.

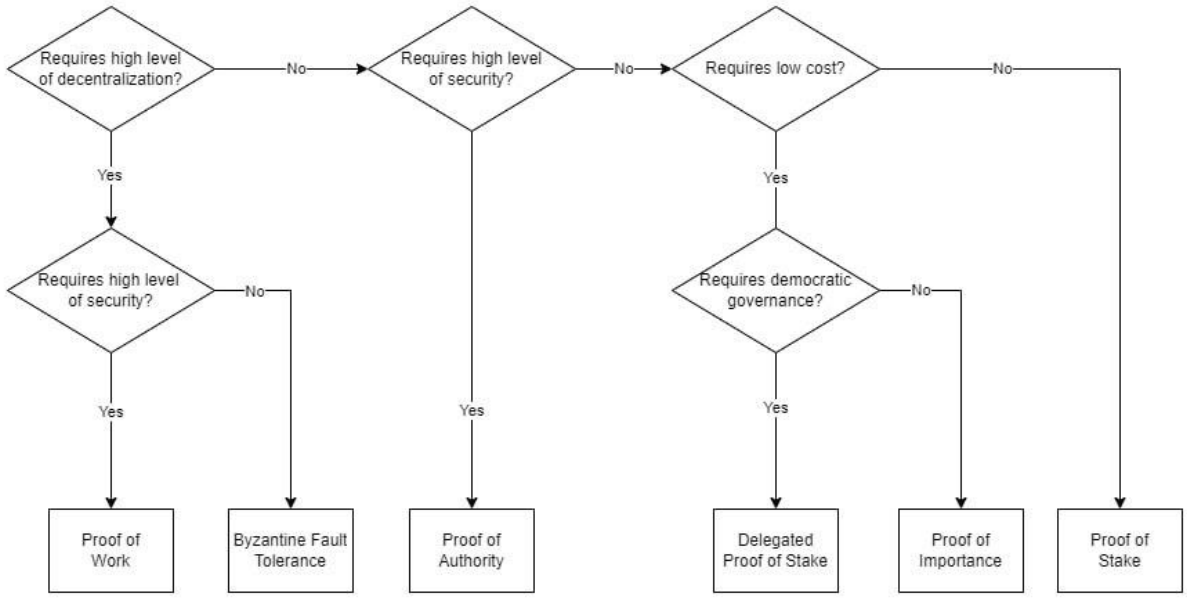

Fig. 5. Block three. Definition of the consensus algorithm

3. Conclusions.

An analysis of consensus methods such as Proof of Work (PoW), Proof of Stake (PoS), and Delegated Proof of Stake (DPoS) indicates the importance of understanding and considering the

trade-offs that arise when using them. Making informed decisions based on the specifics of a particular task allows you to ensure the optimal choice of a consensus algorithm for the task at hand.

Optimising and improving the effectiveness of consensus algorithms is a key task for ensuring the efficiency and stability of decentralised systems. The study and implementation of optimisation strategies aimed at reducing energy consumption, improving scalability, and ensuring security has significant potential to improve the functionality and efficiency of distributed networks.

There is a need for further research and innovation in the field of consensus algorithms in decentralised systems. Consistent efforts to develop scientific knowledge, identify new approaches, and develop technological innovations can help achieve significant improvements in decentralised technologies and expand their application.

References

1. B. Sriman, et al. “Blockchain Technology: Consensus Protocol Proof of Work and Proof of Stake.” Intelligent Computing and Applications, 2020, pp. 395–406, doi:10.1007/978-981-15-5566-4_34.

2. Bamakan, Seyed Mojtaba, et al. “A Survey of Blockchain Consensus Algorithms Performance Evaluation Criteria.” Expert Systems with Applications, vol. 154, 2020, p. 113385,

3. Cho, Hyungmin. “ASIC-Resistance of Multi-Hash Proof-of-Work Mechanisms for Blockchain Consensus Protocols.” IEEE Access, vol. 6, 2018, pp. 66210–66222

4. Duong, Tuyet, et al. “2-Hop Blockchain: Combining Proof-of-Work and Proof-of-Stake Securely.” Computer Security – ESORICS 2020, 2020, pp.

5. Guru, Abhishek, et al. “A Survey on Consensus Protocols and Attacks on Blockchain Technology.” Applied Sciences, vol. 13, no. 4, 2023, p. 2604.

6. King, Sunny, and Scott Nadal. PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake, 2012, pp. 1–6

7. Liu, Yu, et al. “Hybrid Consensus Protocols and Security Analysis for Blockchain.” 2022 International Conference on Data Analytics, Computing and Artificial Intelligence (ICDACAI), 2022

8. Lucas, Bouvarel, and Rafael V. Paez. “Consensus Algorithm for a Private Blockchain.” 2019 IEEE 9th International Conference on Electronics Information and Emergency Communication (ICEIEC), 2019

9. Mackenzie, Adam. Memcoin2: A Hybrid Proof-of-Work, Proof-of-Stake Crypto-Currency, 2013

10. Malinov V., Zhebka V., Zolotukhina O., Franchuk T., Chubaievskyi V. Biomining as an Effective Mechanism for Utilizing the Bioenergy Potential of Processing Enterprises in the Agricultural Sector //CEUR Workshop Proceedings, 2023, 3421, p. 223–230

11. Zhebka V., Gertsiuk M., Sokolov V., Malinov V.Sablina M. Optimization of Machine Learning Method to Improve the Management Efficiency of Heterogeneous Telecommunication Network // CEUR Workshop Proceedings, 2022, 3288, p. 149–155

12. Zheng, Zibin, et al. “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends.” 2017 IEEE International Congress on Big Data (BigData Congress), 2017