DOI: https://doi.org/10.15276/hait.07.2024.9
UDC 004.75

Research into the possibilities of improving Proof-of-Work blockchain technology

Diana V. Soloviova[1)]
ORCID: https://orcid.org/0009-0007-5253-8848; dianochkasolo1@gmail.com.
Svitlana G. Antoshchuk[1)]
ORCID: https://orcid.org/0000-0002-9346-145X; asg@op.edu.ua. Scopus Author ID: 8393582500
Viktor O. Boltenkov[1)]
ORCID: https://orcid.org/0000-0003-3366-974X; vaboltenkov@gmail.com. Scopus Author ID: 8575846900
[1)] Odessa Polytechnic National University, 1, Shevchenko Ave. Odessa, 65044, Ukraine

ABSTRACT

This work is devoted to to the research into the possibilities of improving Proof-of-Work blockchain technology based on dynamic clustering of nodes to reduce transaction time.To eliminate the problem with the Proof-of-Work mechanism, which is considered in this work, it is necessary to solve the problem of reducing the amount of time spent on a transaction. It is proposed to implement this by dividing the system into subnets: when the consensus is not accepted by the entire community, but it is accepted by groups separately – thus minimizing the transaction time in the Proof-of-State algorithm. There is no ready-made solution for the Proof-of-Work dynamic consensus mechanism that would be successfully applied in blockchain technologies. All existing algorithms for dividing the blockchain network into subgroups are used only for static algorithms, but Proof-of-Work is dynamic and has certain features: there is no scope; the user does not see the list of nodes. These features greatly complicate the implementation of clustering for the Proof-of-Work consensus mechanism. The task of this study is the formulation of hypotheses and the verification of the formulated hypotheses, which are aimed at increasing the speed of the transaction. For verification, it is proposed to simulate a blockchain network to conduct experiments and test hypotheses that can potentially solve the Proof-of-Work problem. To develop a way for improving the Proof-of-Work consensus mechanism by implementing dynamic clustering of network nodes, flexibility and scalability, minimal impact on the existing blockchain protocol are taken into account, security issues are also important, management of the process of accepting new nodes to avoid possible attacks and ensure integrity and network security. Existing methods of improving Proof-of-Work technology, clustering methods that can be applied to the network are analyzed; problems that arise when developing a new technique are identified. A blockchain network modeling system has been developed and implemented, with the help of which the approach of dynamic grouping of nodes of the blockchain network, in which the system is divided into subsystems, is implemented. The results of the study allow us to conclude: the cluster system gives improved values of the number of transactions per second (by two hundredths transactions), average transaction time (by one and sixty-seven hundredthsseconds), throughput (by two tenthstransactions), transaction delay (by one and six hundred sixty-seven thousandths seconds) and significantly reduces the total energy consumption of the system (a difference of five thousand, one hundred twenty-two units). This indicates the potential of the proposed method in various practical applications.

Keywords: Blockchain technology; Proof-of-Work; Proof-of-Work consensus; consensus mechanism; blockchain simulation; blockchain mining; transaction time; time minimization; mining synchronization; dynamic clustering; blockchain modelling.
Proof-of-State

***For citation*: Soloviova D. V., Antoshchuk S. H., Boltenkov V. O. "Research into the possibilities of improving Proof-of-Work blockchain technology". *Herald of Advanced Information Technology.* 2024; Vol. 7 No. 2: 131–146. DOI: https://doi.org/10.15276/hait.07.2024.9**

INTRODUCTION

The modern world sets before itself both the goal of further development of progress and the goal of solving the problems that this irreversible progress creates. Both are extremely important today.

Blockchain technology plays the role of both one of the engines of progress and a method of solving specific problems. This distributed ledger technology has found applications in various industries due to its unique characteristics such as decentralization, transparency, immutability and high security. However, along with the rapid expansion of the use of blockchain, new challenges and problems arise that require immediate solutions [1].

The consensus mechanism is a necessary process in the blockchain that ensures that new blocks are attached to the chain. It can be said that it is a cornerstone process in the functioning of the entire blockchain.

The basis of the functioning of many blockchains is the Proof-of-Work (PoW) consensus mechanism, it has become a cornerstone in the evolution of blockchain technologies and plays a key role in ensuring the reliability and security of digital transactions. The importance of PoW is manifested in its ability to prevent many types of attacks, such as double spending and transaction order

manipulation [2].This mechanism creates an economic incentive for miners, forcing them to invest significant resources in computing power to validate blocks. Despite its effectiveness, this mechanism is not without its drawbacks, an important one being the long time required to confirm transactions. Significant time delays in the PoW mechanism create problems in ensuring the speed and scalability of blockchain systems. These delays can affect user expectations, system performance, and overall network bandwidth. Therefore, there is a need to find ways to reduce transaction processing time within the Proof-of-Work mechanism [3].

Proof-of-Work remains indispensable in the context of ensuring decentralization and protection against abuse. Improving the PoW mechanism aims to preserve these fundamental principles, while reducing time delays and increasing the efficiency of the system [4]. That is why the topic of work related to the improvement of PoW while preserving its inviolable advantages is relevant.

The purpose of the study is to develop the possibilities for improving the Proof-of-Work consensus mechanism by implementing dynamic clustering of network nodes, which will increase the efficiency of the data transfer process, namely reduce the time spent on a transaction [5].

ANALYSIS OF LITERARY DATA

The biggest problem that makes the Proof-of-Work mechanism less profitable is the long transaction time. This time interval is not only reflected in the percentage of global electricity used to verify transactions, but also requires recipients to wait a significant period of time for transaction confirmation. This problem becomes central to our research, as our work is aimed at solving this challenge in the development of blockchain technologies.

The problem of a long transaction time is easier to solve in the Proof-of-State (PoS) mechanism, where the use of sharding, for example, allows you to distribute the load on the network, increasing the speed of transaction processing [6, 7]. Proof-of-State uses a static system where the choice of persistence depends on the number of coins owned by the participant, not on computing power.

However, Proof-of-Work cannot implement such a mechanism because it is dynamic in nature. It is based on the work of miners, who spend significant computing resources to find new blocks, and does not have the simple ability to divide the work between different shards, as it is done in PoS [13]. Thus, the advantages of sharding, which helps to reduce the transaction time in PoS, are not available for the Proof-of-Work mechanism [8, 9].

Proof-of-Work is considered dynamic because miners compete with each other for the right to add a block to the blockchain [14]. This process requires constant solving of complex computing tasks. Participants can join and leave the network, and the difficulty of the task can change depending on the total computing power of the network [10].

Proof-of-State is considered static because instead of using computing power like PoW, it is based on ownership of cryptocurrency. Participants with more cryptocurrency have a higher chance of being selected to create a block and receive a reward. The PoS framework assumes that participants with more funds are more likely to be selected to create blocks [12]. This creates a more static system compared to PoW [11]. For a dynamic consensus mechanism, there is no ready-made implemented solution that would be successfully applied in blockchain technologies. The static mechanism of consensus (Proof-of-State) differs from the dynamic one (Proof-of-Work) by a number of key features that demonstrate the differences in solutions that can be applied to them. Let's summarize in Table 1 the result of the analysis of the comparison of these two mechanisms (static and dynamic).

Table 1. **Comparison table of Proof-of-State and Proof-of-Work consensus mechanisms**

Comparison parameter	The name of the consensus mechanism	
	Proof-of-State	Proof-of-Work
Field of view	The system has a list of nodes and it is clear which nodes are further and closer	The user does not see the entire network, this information is not available
Availability of metrics	In fact, the system stores a table of PoS pseudometrics	In PoW, it is more difficult: you cannot track users, measure the distance
Possibility of mining	The possibility of mining is determined by the number of tokens of this currency in the user's possession	The ability to mine a block is determined by the computing power of each miner

Source: **compiled by the authors**

So we can see their particularly distinctive characteristics, which are interesting in the course of the study and which influence the further development of the way for improving the Proof-of-Work blockchain technology.

It is clear that these differences of the Proof-of-Work mechanism are some challenges for us. Based on these challenges, the goal of our work is to develop and implement dynamic clustering for a blockchain network with a PoW mechanism. This will reduce transaction time and increase network efficiency, given the specifics and challenges associated with this consensus mechanism.

But not the usual clustering, but an algorithm that would take into account the listed features of the mechanism.

FORMAL PROBLEM STATEMENT

To eliminate the problem with the Proof-of-Work mechanism, which is considered in this work, it is necessary to solve the problem of reducing the amount of time spent on a transaction. It is proposed to implement this by dividing the system into subnets: when the consensus is not accepted by the entire community, but it is accepted by groups separately – thus minimizing the transaction time in the PoS algorithm. There is no ready-made solution for the PoW dynamic consensus mechanism that would be successfully applied in blockchain technologies. All existing algorithms for dividing the blockchain network into subgroups are used only for static algorithms, but PoW is dynamic and has certain features: there is no scope, the user does not see the list of nodes. These features greatly complicate the implementation of clustering for the PoW consensus mechanism. The task of this study is the formulation of hypotheses and the verification of the formulated hypotheses, which are aimed at increasing the speed of the transaction. For verification, it is proposed to simulate a blockchain network to conduct experiments and test hypotheses that can potentially solve the PoW problem.

To develop the possibilities for improving the Proof-of-Work consensus mechanism by implementing dynamic clustering of network nodes, flexibility and scalability, minimal impact on the existing blockchain protocol are taken into account, security issues are also important, management of the process of accepting new nodes to avoid possible attacks and ensure integrity and network security [15].

The goal of the work is to improve metrics such as the number of transactions per second, reduce transaction latency, increase throughput (or at least not degrade it), not degrade energy efficiency, and not increase lock time.

The primary task that appears in this work is to develop an algorithm for solving the problem, model the system and test the proposed hypotheses. The first stage of modeling is the creation of a network model. The model should be flexible to vary distances, power while testing hypotheses and running experiments to minimize transaction times. As part of this study, a network model of 100 nodes will be created in order to conduct experiments to test the hypothesis, where the idea of dynamic clustering of nodes will be implemented.

Thus, in the course of this study, the development of a way for improving PoW blockchain technology will be carried out in order to reduce the time spent on a transaction, testing the relevant hypotheses. A simulation of the blockchain system will be carried out, the behavior of real nodes will be simulated and how the processes affect the distributed consensus of the system as a whole will be simulated, and the results will be measured accordingly in order to obtain the necessary conclusions regarding hypothesis testing.

The paper proposes a dynamic grouping approach, which aims to reduce transaction time in the PoW mechanism. By dividing the system into subsystems depending on the capacity and relationships between nodes, it is proposed to improve the efficiency of the transaction confirmation process and reduce their processing time. To achieve this goal, an algorithm is developed and experiments are carried out to measure the results. The obtained results will allow us to draw conclusions about the effectiveness of the proposed approach and the possibility of its implementation in real blockchain systems with the PoW mechanism.

STUDY OF PROOF-OF-WORK BLOCKCHAIN TECHNOLOGY IMPROVEMENT POSSIBILITIES

We will determine the main goals and objectives of the study for improving the Proof-of-Work consensus mechanism by implementing dynamic clustering of blockchain network nodes, such as reducing data transmission time and evenly distributing nodes by group [16, 17].

One of the main aspects of clustering in a PoW and blockchain network is the reduction of transmission times. Clustering allows you to group nodes that are “closer” to each other or have more reliable connections into one cluster. This can reduce data transmission delays and provide faster communication between nodes.

An important task of the study for improving the Proof-of-Work consensus mechanism by implementing dynamic clustering of blockchain network nodes is to achieve an even distribution of nodes by groups or clusters [18]. This provides load balancing and reduces the possibility of network bottlenecks. Even distribution can increase network security by distributing computing power and reducing the risk of a 51 % attack.

A graph model was chosen as a data representation model, and the clustering criterion was the power of nodes [27].

It was established that formal clustering algorithms have vulnerability in this context – insufficient uniformity of clusters [21, 22]. Therefore, based on K-means and OPTICS algorithms, as the most optimal formal clustering algorithms, clustering will be implemented, where the problem of uneven distribution of nodes will be solved and the vulnerability of clustering algorithms will be eliminated [19, 20].

SOLUTION OF THE PROBLEM OF ENERGY CONSUMPTION

One of the most important aspects during the research is maintaining the balance between the minimum power of the system and the growth of consumed energy. The task of the algorithm is not only to reduce the transaction processing time, but also to save computing power.

From the previous subsection, we trace three possible states of the node:

a) peak power, where he directly performs complex mathematical calculations;

b) synchronization, as a partial transition;

c) rest, which minimizes the activity of nodes before the next phase of the cycle.

Therefore, these states will be implemented in the simulation, that is, the operation of nodes will be divided into phases as a solution to the problem. Since the cluster approach is based on the integration of certain nodes into small subsystems, which leads not only to the optimization of the synchronization speed of individual clusters, but also introduces additional principles of control over points – the speed and quality of the overall synchronization of the network increases, reducing the percentage of “lagging” nodes that is even more fundamental [28].

Thus, if, for example, the time of the general synchronization phase used to take 2 minutes, now each individual cluster will perform it, for example, in an average of 1 minute, which reduces the energy consumption of this phase by half.

However, the key advantages are the second part: the blockchain principle itself, in its real dimension, is an example of an absolutely terrible optimization of the network interaction process. A significant segment of nodes not only does not participate in reaching a collective consensus, but also does not even know at all about the current state of such a system and the example of the latest blockchain chain. This leads to calculations that do not make any sense for this period of time, and therefore energy consumption increases not by a few percent, but by multiples. Therefore, clustering is an additional mechanism that helps prevent the formation of such conditions.

DEVELOPMENT OF A BLOCKCHAIN NETWORK SIMULATION SYSTEM AND SOFTWARE IMPLEMENTATION OF PROOF-OF-WORK BLOCKCHAIN IMPROVEMENT STUDY

The clustering method, which is the basis of the work, deliberately involves the analysis of the design, which from a higher degree reconfiguration of the network and the basic algorithm is able to give a minimal increase, because by obtaining a real network in the sense of the overall computing power, it achieves an increase in speed due to the optimization of the design of the synchronization structure.

Therefore, the thesis can be properly proved only by its more actual implementation. Since the PoW process, in its real expression, involves several thousand to tens of thousands of machines with a colossal computing power, synchronization algorithms and a consensus method in millions of lines of code, based on a higher degree of chaos of the network connecting them together (various countries/providers/machines/DDoS-attacks) and others [33]. The construction of a system for its correct imitation would take, one person probably many years, and it still could not be applied in practice, and even despite the fact that by now billions of dollars and years have already been invested in the technology – its implementation is still quite conditional Therefore, the theory can be correctly proven only from the design level of a high degree of abstraction [23, 32].

However, of course, the created simulation should reflect all the processes necessary for modeling the blockchain system, in order to be able to conduct real experiments and obtain reliable, from the point of view of logic, indicators [24, 25].

These are processes such as:

– transaction creation processes and necessary actions on them;

– the process of forming blocks and their

publication;

– processes of building a network of machines and interaction between them;

– the process of building connections between nodes;

– block hashing process;

– mining process;

– the process of adopting a consensus in the PoW system.

The software (software) is a simulation of the blockchain system.

Additionally, the software should implement the processes for the improved PoW blockchain network proposed in this paper:

– cluster formation process;

– processes of transition of nodes from one cluster to another;

– the process of joining a node to a group;

– the process of synchronizing mining results by cluster method and cascade by default.

Also, the software must provide the functions necessary for the analysis of the created system:

– output system parameters;

– visualize the system (dynamically).

And most importantly, the functionality must provide the ability to launch two networks, classic PoW and improved, to actually compare the results of their work efficiency.

The software is internal, intended for the researcher. External use is not provided, because the software is created for the purpose of testing the hypothesis of the developed study, and not for use by a random user. The task of the software is to implement an abstract model of the system with the classic PoW algorithm and improved for the purpose of hypothesis testing.

Therefore, a blockchain network simulation system with a PoW mechanism is being developed, which allows to reproduce new algorithms of consensus adoption and details of system construction, which contribute to reducing the time spent on transaction processing. To achieve the goal, it is necessary to update the structure of the blockchain by adding new components, updating the mechanism for establishing connections between nodes, and the mechanism for synchronizing mining results [26, 29]. Such a structure will allow the dynamic distribution of the blockchain network into subnets. There is no ready-made simulator for reproducing and testing the PoW dynamic consensus mechanism, which would be successfully applied in blockchain technologies. The developed simulation model of the blockchain network with the Proof-of-Work consensus mechanism was implemented using the Python programming language, which contains the following classes, which are presented in the UML class diagram in Fig. 1.

The blue color shows the classes that have been added to the classic blockchain structure, which are such additional classes Cluster, Synchronizer, Analyzer and Vizualizer. Attributes and methods added to the classic network structure that improve the blockchain structure to implement the dynamic node grouping algorithm are highlighted in italics. In particular, these are methods of establishing connections between nodes, implementing the process of synchronizing nodes to transfer mining results, presenting the system in a graphical model, and implementing clustering of nodes. For the simulator of the blockchain system, we will describe the main process of interaction with the user, that is, the researcher. All the main processes take place inside the system classes – this is described in the previous subsections. Inside is a simulation of the blockchain system. The user only runs this simulation and receives the results of analytics. So, let's look at the scenario of running a blockchain simulator and getting an analysis of its effectiveness. The process is as follows: first, the user (researcher, administrator) starts the network simulation and chooses its size. The user also chooses the type of system (classic or cluster) in the simulator.

After the user starts the simulator, the signal is transmitted directly to the network, which transmits the signal to the nodes for their creation (the number of nodes is set by the user). Also, in parallel with the creation of the network, the blockchain and the generation of transactions are launched (this point is omitted in the diagram to simplify and visualize the processes). Transactions from the pool go to a new block, which is mined by nodes. Finally, one of the miners finds the hash of the block and sends a synchronization request to the Synchronizer. The process of network synchronization takes place – the status of finding a hash is transmitted to all nodes, that is, the adoption of consensus. This synchronization result is then transmitted to the block such that the block is considered published and added to the blockchain as a new block (the blockchain will thus also receive a synchronization signal). This signal is then transmitted to the nodes, that is, they are informed about the end of mining and the publication of a new block, which in turn, after their complete synchronization, transmit the signal to the network. The network transmits all information to the Analyzer, which in turn displays the simulation results to the user – system efficiency parameters and dynamically visualizes the system (using the Visualizer). An example of visualization is presented in Fig. 2.

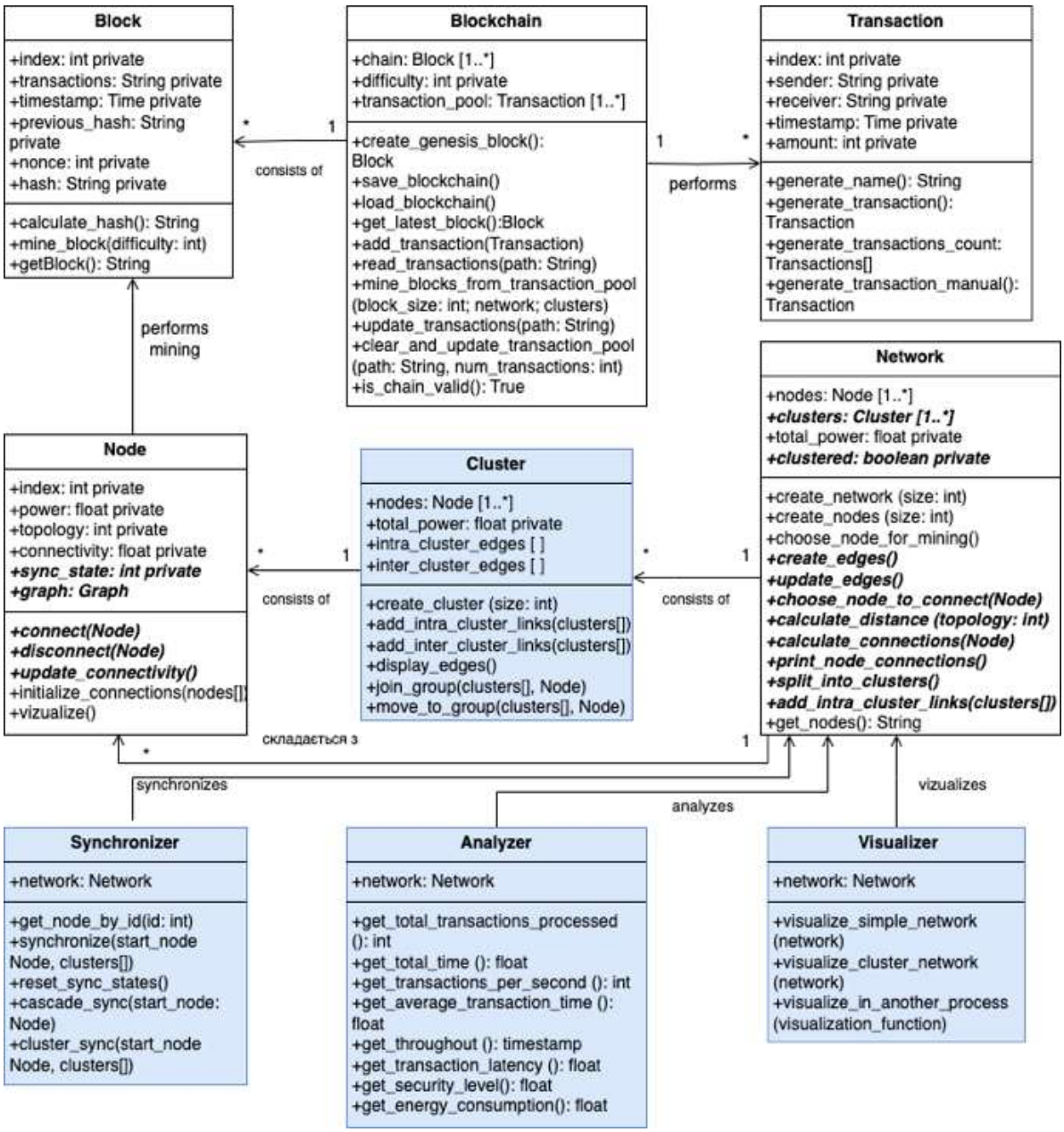

Fig. 1. **Simulator class diagram**

Source: **compiled by the authors**

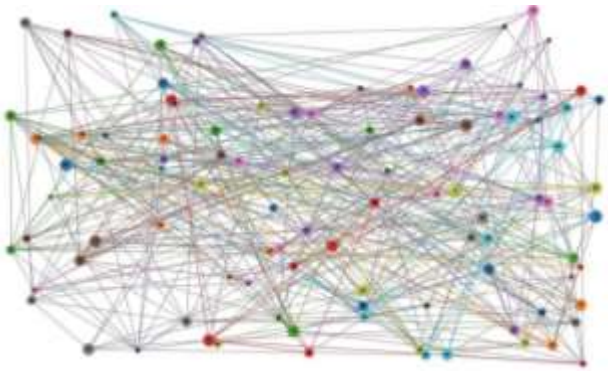

Fig. 2. **Visualization of the clustered network**

Source: **compiled by the authors**

After each stage of mining, the reconfiguration of the system takes place – this is an important component of realizing the dynamic nature of clustering and visualization. Because certain nodes could "split" – log out of the system, have poor access to the network, etc [30].

OPTIMIZATION OF BLOCKCHAIN NETWORK SIMULATOR PARAMETERS

During the implementation of this system – a simulator of the blockchain network, the optimal values of the parameters that affect the further operation of the system and its efficiency were determined. This is due to the fact that the blockchain system is a structure endowed with a

large number of connections between various processes and objects, so they influence each other in a certain way.

So, in this subsection, we will describe the optimization of some parameters that most affected the result of the simulation and justify their values.

The first parameter that was optimized is the number of clusters into which the network of nodes is divided during their dynamic grouping. In order to find out the optimal value, experiments were conducted and it was established that the most effective and reasonable value of the number of clusters is calculated according to the formula, namely, depending on another parameter of the system. It is clear that the number of clusters depends most on the number of nodes in the network.

Thus, the following dependence of the number of clusters on the number of nodes in the system was established, which turned out to be the most optimal for this system:

$$N_{clust.} = \sqrt{N_{nodes.}}, \quad (1)$$

where N_{clust} is number of clusters; N_{nodes} is the number of nodes in the network.

The result of the calculation is rounded to a whole number and at the output we get the optimal value of the number of clusters. The square root was taken, because it is a fairly accurate pattern based on the potential connectivity of the point, its possibilities.

The next parameter that was optimized is the number of transactions in one block, that is, the block size. The number of transactions per block in a blockchain network depends on the purpose of the network. Sometimes it is 100 or 1000 transactions – in this case the transaction pool is emptied very quickly. It depends on the scale of the network. But since the purpose of the work was to test the hypothesis, for which it was necessary to see the processes more slowly and under the focus of approximation, and because this simulation is an abstract model of a blockchain with 100 nodes, the number of transactions per block was set to 3. This value of the number of transactions turned out to be the most suitable for the methodology of conducting experiments. Choosing such a number of transactions allows you to easily manually fill in and hash block hashes, that is, reproduce mining, look at the results of mining, draw the necessary conclusions within the reproduced system.

An optimized time parameter between block publications has been set. The total time between mining blocks should be constant. This is necessary to ensure stable operation of the network (to retain control of the stability of the network) and to prevent both overloading and unnecessary downtime. The difficulty of this task is automatically regulated by the protocol so that the average time between the creations of new blocks remains constant.

Since the blocks are mined randomly – the gap can vary – in one interval it will be 2 minutes, and in another – 10 minutes. This entails the consequence that the process turns into chaos. We must ensure that the network has time to synchronize as a whole, and that the next block does not appear too early, that is, before the previous one has been fully accepted as a general consensus. But we have the ability to relatively "plan" the time, in the range of which we are able to "play" with this meaning. If the structure of the investigated network becomes more connected, responsive, we can afford to shorten it. Therefore, this time was set to 30 seconds for the classic network. 30 seconds turned out to be the optimal value for the effective operation of the simulation.

The optimal value of the hashing difficulty was chosen. The difficulty parameter is set by the blockchain protocol, and its change occurs dynamically, depending on the total power of the computing network. The correct value of the hashing difficulty helps to ensure a stable and secure operation of the network by adjusting the rate of creation of new blocks according to the total computing power of the network. Additionally, hashing complexity directly affects system security – high complexity increases system security. However, with the increase in complexity, the power consumption of the network increases. So, taking into account all the parameters affected by the hashing difficulty, the optimal hashing difficulty of 5 was set for this 100-node simulator system.

The next parameter is a coefficient that determines and affects the connectivity of a node. It takes part in the connectivity calculation. We will describe the principle by which its optimal value was determined.

The number of connections is calculated taking into account the node connectivity property – its product by the coefficient:

$$N = C \times k, \quad (2)$$

where N is the number of node connections; C is the value of the node connectivity feature; k is the coefficient of connectivity.

The value of the number of connections is rounded to an integer. It was necessary to establish the value of the coefficient k. The

number of connections affects the speed of the node synchronization process. The idea behind implementing the program and structure is that while maintaining the overall weight of the edges, we reduce the relative share of intercluster connections at the expense of intracluster connections, as if "pulling the blanket" in the direction we need. The coefficient for the normal network was set to 3, since this value is approximately compensated by the new type of connections. For the cluster network, the coefficient is set to 6: with an average connectivity of 0.5, it gives 3 edges per node, that is, 300 edges per 100 nodes used in the simulation. This is almost bordering on optimal network synchronization (90%+), but keeps the speed within acceptable limits. About 150 connections are created by the cluster itself – but strictly within the cluster, due to which acceleration of the synchronization stage is achieved.

ANALYSIS OF THE EFFICIENCY INDICATORS OF THE DEVELOPED STUDY

In order to analyze the effectiveness of the developed study, it is necessary to study the performance indicators of the blockchain system with the implementation of dynamic clustering and compare it with the classic base system. Since the indicators in cycles (1 cycle – 1 mining) of the program are very variable, we will go through 10 mining cycles to obtain results. That is, we will preload 30 transactions into the pool for testing the classic Proof-of-Work model and 30 transactions for testing the cluster model. Then the performance indicators will be more average.

So, the program for the classic and cluster network was launched. Both types of networks were launched to mine 30 transactions. That is, the conditions are the same. At the output, after testing both models, the following results of the blockchain system efficiency indicators were obtained, and specifically those related to the topic – that is, the time of transactions, because the goal of the work was to reduce the transaction time. Program output of efficiency indicators was obtained for the classic PoW network and for the cluster network, respectively.

The results of the analysis and comparison of performance indicators, which were obtained at the end of the experiments, are presented in Table 2. So, the results of the simulation of two types of blockchain network systems and the output of indicators clearly demonstrate that the cluster model is indeed better in terms of the speed of transactions. Let's analyze each indicator.

The number of transactions processed by the systems is the same because it was set by the user specifically for the purpose of setting the same conditions for running the two models and comparing the results of their work. The total system operation time was equal to 300 s in the classic Proof-of-Work network and 250 s in the network with the implementation of dynamic clustering. This time consists of performing 10 mining iterations. One mining iteration is the time between block publications. For a classic network, it is 30 s, and for a cluster network – 25 s. This time must be constant to ensure network stability. We have the opportunity to relatively "plan" the time in which we are able to interact with this value. If the construction of our network becomes more connected, responsive, we can afford to reduce this time. In this way, we achieve shorter intervals between blocks and, therefore, a reduction in transaction time. The synchronization time that was shortened is minimal in the system, since the time was changed only for intracluster connections, which are about 10 % of the standard generation, or even less.

Table 2. **Comparison of metrics in two types of blockchain network**

The name of the metric	Basic network	A network with dynamic clustering
Number of transactions processed	30 transactions	30 transactions
Total system uptime	300 s	250 s
Number of transactions per second	0.1 transactions	0.12 transactions
Average transaction time	10 s	8.33 s
Capacity	1 transaction	1.2 transactions
Transaction delay	10 s	8.333 s
Total energy consumption	9980.36 units	4858.29 units
Security level	25 units	7.9 units

Source: **compiled by the authors**

If the network were reconfigured (with dynamic clustering), giving the lion's share (2/3, for example) only to intra-cluster connections in advance, keeping a third to inter-cluster connections, the synchronization time would be reduced by half or even by 2/3 under ideal conditions structures of the cluster itself. But in this version, in the implementation of the simulation of the implementation of the dynamic grouping algorithm, there is another available and significant advantage – a higher total number of synchronized nodes, higher connectivity and stability from attacks, therefore, that is why the time between block publications for the cluster network is set to 25 s. and for the usual one – 35, because it is theoretically justified.

The number of transactions per second was also higher in the dynamic clustering model (0.12 transactions per second for the clustered model compared to 0.1 transactions per second for the classic model). This is due to the fact that mining is faster in the cluster model, and the time between blocks is shorter.

The average transaction time for the classic network is 10 s, and for the cluster network – 8.3 s. On a larger scale of transactions, this difference in time will turn out to be extremely significant. So, for 1000 transactions, this difference will be 1700 seconds, which is 28.3 minutes.

The throughput of the model with dynamic clustering is 1.2 transactions, for the classic one – 1 transaction. This parameter characterizes the ratio of the total number of transactions to the mining interval. Its difference is caused by a decrease in the mining interval for the cluster system, which is a consequence of its increased connectivity.

The transaction delay for the classical network is 10 s, and for the cluster network – 8.33 s. This small difference in the scale of the real network gives very important results. For 10,000 transactions, this difference will be almost 47 hours. And 10,000 transactions are the usual conditions for a day's blockchain work.

For the classic blockchain system with the Proof-of-Work mechanism, we obtained a total energy consumption of 9980.36 units, and for the cluster model – a total energy consumption of 4858.29 units. The difference is very big, it is 5121.07 units of energy and this is only for 30 transactions. Thus, it can be concluded that the developed model is extremely efficient from the point of view of energy consumption.

This is due to the fact that the time of mining and synchronization for the cluster network is reduced, compared to the classic one – it affected the result of energy consumption indicators. It was deduced that energy consumption depends on the time spent on mining and synchronization, as well as on the power of the system. But the power of the classical system and the cluster system is the same, equal to 51.8 units within the framework of this experiment.

Thus, it was the mining and synchronization time, namely the accelerated synchronization time for the cluster network that influenced this result. This time is really shorter for a cluster network: since a number of nodes are inside the cluster, the nature of their communication can be initiated by additional security protocols, fewer conditions and delays, therefore, by more optimal methods of their synchronization. This happens by reducing the overall network security and delegating part of the authority within the cluster.

The result of reducing energy consumption is a consequence of the implementation of the idea of using “rest phases”, which is described in subsection 2.5.4. Due to the reduction of the synchronization time, in the time scheduled for mining, "extra" time appeared, free time, during which the system is not busy mining blocks (because mining has already ended, and a new one has not yet started), but rests. This phase is set specifically to reduce power consumption, as this is also one of the most important problems of Proof-of-Work.

The security level of the cluster network is 7.9 units, while that of the classic network is 25 units. This is due to the fact that when the network is divided into clusters, the possibility of taking it under your control also increases, because the main attack that a decentralized network faces is a 51 % attack. After all, this is exactly what the idea of decentralization itself was originally: everyone is equal to everyone; transparency and equal proof are preserved. It's like any currency, in general – it arose in opposition to control by the banking system, centralization of the state, issuer, exchange rate, demand, etc. Clustering, in fact, is a regressive movement – we return to the concentration of capital, therefore, the control of the crowd over the life of such a currency falls. But as far as the economic aspect is concerned, there is also a program aspect.

If in network A (full decentralization), strictly speaking, the entire set of miners and holders participates in maintaining the primary status quo, then for clustering/grouping, we purely conceptually transfer this responsibility to small groups. And since we all understand the rules of the game (if there is a possibility of fraud, it will happen), we

only encourage big capital to find a solution to this problem. Thus, clustering provides a number of advantages in terms of segmentation and specialization, additional consensus patterns. But everything has its price; the price in this case is safety.

ANALYSIS OF DEPENDENCES OF NETWORK PARAMETERS

During the research and implementation of the simulator system, certain dependences of the parameters on each other were revealed. They were displayed as formulas in the 2nd chapter. But in this subsection, their nature will be considered and justified in more detail.

First, it is energy consumption. The value of this parameter, as it was found during the research, depends on the power of the system and the time spent on mining and synchronization [31]. If we consider this process comprehensively and deeply, the formula for the dependence of energy consumption turns out to be more complex.

It looks like this:

$$E = \frac{S\times(t_{mine.}+t_{sych.})\times P}{100} + \frac{(100-S)\times t_{cycle.}\times P}{100}, \quad (3)$$

where E is the energy consumption of the system; S is the percentage of system synchronization; t_{mine} is time spent by the system on mining; t_{sync} is time spent by the system on synchronizing mining results; P is the total power of the system; t_{cycle} is the time spent on one cycle, the time between publications of new blocks.

The sum of the synchronization time and the mining time can actually be called the network activity time, while the cycle time also consists of the rest phase of the nodes.

This extended formula reflects the relationship with the percentage of network synchronization, because it gives information about the number of "lagging" nodes: if the synchronization is 100 %, there are no lagging nodes.

The power of the system at the time directly depends on the complexity of calculations, the complexity of the hash, which needs to be found in mining. From this it can be concluded that the energy consumption of the system depends directly on the complexity of hashing.

So, power consumption depends on 2 main factors – hashing complexity and system synchronization. It does not make any sense to change the hashing complexity within the framework of this study, because this is not the task of the study. Complexity is an independent factor that we cannot influence. It is an independent factor from the structure of the network, it is a rule that implementers of the blockchain network set for practice.

Network synchronization, in turn, is a variable in this study. Synchronization depends directly on network connectivity, which is higher in a cluster because of its greater efficiency, establishing cluster control. In a cluster network, the level of connectivity is higher, because additional cluster control protocols appear in clusters. Acceleration of synchronization, which is achieved, is also achieved in this way, in particular. Synchronization restores peace to the nodes, it turns off the machines before a new cycle, therefore, the more effective the network synchronization is, the lower the energy consumption, respectively. Thus, the energy consumption in the created cluster model is significantly reduced. The dependence of energy consumption on network activity for the case of cascade and cluster synchronization is shown in Figure 3 and Figure 4, respectively.

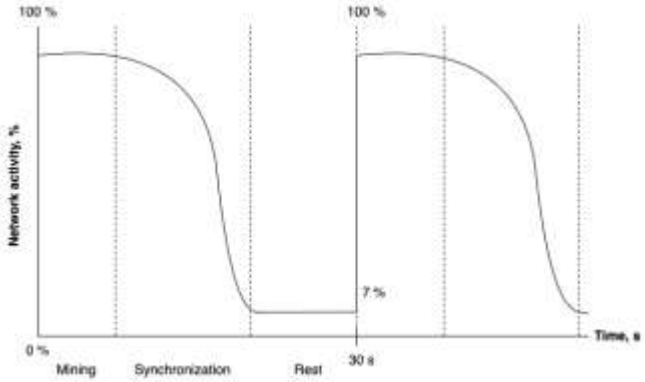

Fig. 3. **Graph of the dependence of network activity on time in the case of cascade synchronization**
Source: **compiled by the authors**

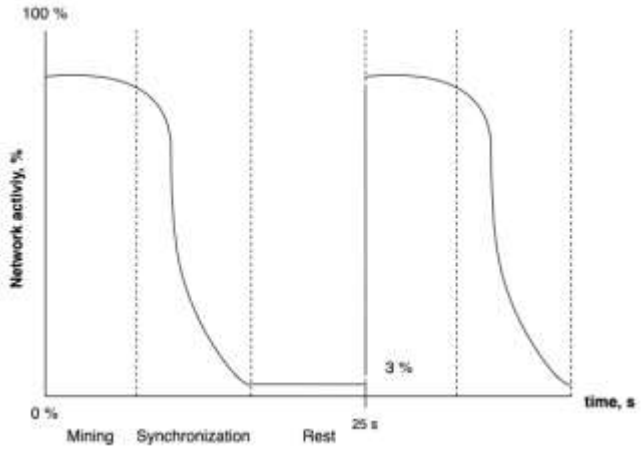

Fig. 4. **Graph of network activity versus time in the case of cluster synchronization**
Source: **compiled by the authors**

These graphs show the dependence of network activity and energy consumption over time, that is, how it changes during the block mining cycle. The top of the "wave" of the graph is mining, when 100 % of the power is spent, the decline of the wave is synchronization. The decay is smoother for cascade synchronization and a sharp drop is observed in the case of cluster synchronization. The bottom of the wave is the resting state of the nodes. The overall synchronization in the cluster is higher, so the third segment (idle state) falls lower, which means less power consumption. The total power is the integral of the function (the area of the volume under the waves of the graph). Thus, energy consumption directly depends on network activity, which is shown in the graph.

Let's look at the dependence of the network security level on other parameters.

First, the level of security depends on the complexity of hashing the network. This is a quadratic dependence, the increase in complexity occurs in a non-linear way, it is explained by a complex of factors, including an increase in computational complexity, increased protection against attacks and increased reliability of the blockchain.

Secondly, the research revealed that the level of security depends on the number of clusters. It is strictly logical that the number of clusters is inversely proportional to security.

But the complexity of hashing grows exponentially, so with a complexity of 10 units and 10 clusters, we have a security level of 10 ($10^2/10$), that is, still 10 times higher than a clusterless network with a security of 1. And the root of the number nodes in this sense are a reflection of the same idea, but in the opposite direction. After all, for 1,000,000 nodes, the number of clusters is only a thousand (which is still not so many), but for 4 points there are 2 groups, the consequence of this is that the distribution is completely uniform. The root of a number is a similar mathematical method to the derivative, which softens the dynamics of the number, preserving it in some sense, simplifying the trend. Since the cluster is not a direct threat, but a potential danger, we must represent it in a similar way mathematically. Therefore, in this dependence, we do not take the number of clusters itself, but the root of such a dependence of the number. The graph of the dependence of the network security level on the number of clusters is presented in Fig. 5.

With the following parameters, we will see how the time of transactions directly depends on the time of synchronization. Because the goal of the work was precisely to minimize the time spent on executing a transaction in the network, and this goal was achieved by dividing the system into clusters.

Let's consider what kind of dependence these parameters are related to each other. Synchronization facilitates the transition to the next states of the cycle. Nodes that have not been properly connected and notified of the latest state of the network and blockchain continue to mine hashes for out-of-date data. In this way, the network not only contributes to the growth of empty calculations, but also deprives the unsynchronized segment of the opportunity to search for a solution to the task in a timely manner.

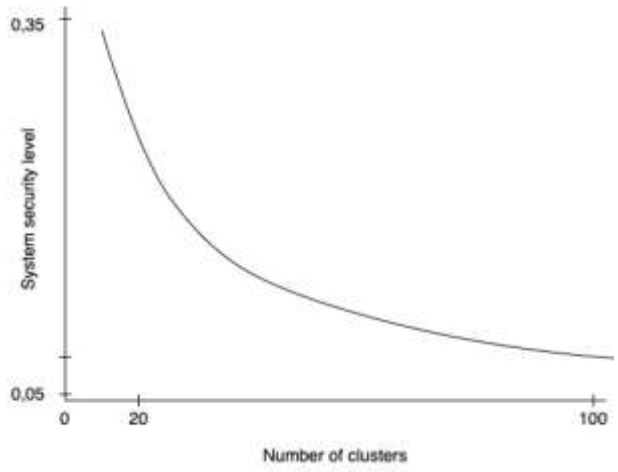

Fig. 5. **The graph of the dependence of the system security level on the number of clusters**

Source: **compiled by the authors**

Thus, if a part of the nodes goes beyond the time limit of the block, remaining part of the wrong sequence, the system becomes chaotic. The network is built on the primary principle of admissibility of the degree of such chaos, therefore time is also calculated. The more time we lose control over the network, the more time we have to keep in the loop to rebalance it, and therefore slow down the flow of transaction processing in general.

The model used does not assume a direct relationship between network synchronization and development execution speed. But it can be developed and provided by the architect of a similar structure in the future. Like, for example, the ratio of the amount of network asynchronization/individual clusters, as a coefficient of the temporal parameter. Where, for example, a network synchronization value of 90 % will be taken as a sample reference value, and when it falls below 89 %, the time is multiplied by a number greater than one. If it is

higher than 91 %, then the number is less than one, if 90% – then by one. In this way, the network would regulate the time between block publications independently, depending on the degree of connectivity and overall responsiveness, because the parameters of the mining iteration and the synchronization level have the described dependence.

ANALYSIS OF THE RESEARCH RESULTS

Therefore, the ways for improving the Proof-of-Work consensus mechanism by implementing dynamic clustering of network nodes have been studied. For a deeper understanding of the characteristics of the technique and potential limitations, we present a table detailing the key aspects of this technique.

Let's look at the advantages of the research results:

– reducing the time spent on network synchronization;

– reduction of the total cycle time between block publications;

– significant reduction in energy consumption;

– adaptability of the proposed technique.

In the technique of improving the Proof-of-Work consensus mechanism by implementing dynamic clustering of nodes of the blockchain network, synchronization occurs faster due to the distribution of the network into clusters, where synchronization occurs within the cluster. This means that each cluster has its own information exchange system, and when a block is replaced in one cluster, other nodes of this cluster instantly receive information about this block, which significantly speeds up synchronization within the cluster. Then only one signal needs to be sent to synchronize between clusters, which is also fast. Therefore, thanks to the technique of dynamic grouping of the blockchain network, a significant reduction in the time required for all network nodes to receive information about a new block after its successful mining is achieved.

The advantage of reducing system energy consumption is due to the following factors. First, this is achieved by reducing the synchronization time. The cluster model of the blockchain network allows to reduce the synchronization time between nodes due to more efficient information transfer within the cluster. This allows you to reduce the amount of energy spent on data transmission and confirmation of new blocks between network nodes. Rest phases for nodes were also introduced. The rest phase allows nodes to temporarily go into a low-power mode during the intervals between mining and synchronization. This allows you to reduce the load on the power system and reduce the overall energy consumption of the network.

Next, we will consider the shortcomings of the improving for improving the Proof-of-Work consensus mechanism by implementing dynamic clustering of network nodes, which arise from the development, implementation, testing and analysis of results.

These shortcomings, which were discovered, are ways to further improve the the studied rechnique and its implementation:

– decrease in the level of network security;
– increasing the risk of centralization;
– complexity of implementation;
– the need to optimize parameters;
– the possibility of failures;
– the need for a large amount of data.

We will explain ways to improve centralization and reduce security. Decentralization was based on the principle of network divergence, fragmentation of convergence centers. Clustering implies a movement in the reverse order, in which control over clusters becomes easier to establish than without them. For example, if the network has no groups and is built on the principle of equality, it is necessary to gain control over 51 % of the machines that process the flow of transactions and data. But if the cluster is, for example, 3, it would be enough to establish control over 2/3 of these clusters. And to gain control over each cluster separately is 51 percent for each. Thus, it is enough to control 51% of 2/3 of the network. If there are 100 clusters, 51% control must be established over 51 clusters. And this is about a quarter of all cars in general. Moreover, some clusters can be disabled due to DDos attacks and spam. And such an attack requires only a few percent of the entire cluster. The clusters themselves, with such a discrepancy, lose their coherence/complicate the construction. This means that they are more vulnerable in themselves - that's why the increase in their number is so dangerous for security.

We will also explain the possible methods of overcoming the listed shortcomings and overcoming the challenges facing further research. First, to improve the level of security, it is possible to work into the system to periodically change the structure and composition of clusters in order to reduce the risk of attacks, that is, so that attackers do not have information about the location of the most powerful nodes in specific clusters. This can be done by reconfiguring the cluster composition

through a random number of mining iterations. In this way, the system will periodically randomly "shake" the nodes.

Second, in order to solve the security problem, it is absolutely necessary to introduce into the network appropriate large-scale penalties for attacks on mining nodes. Third, the number of clusters can also be set randomly (up to a certain limit) so that attackers cannot calculate a pattern. And the clustering method can be studied more deeply and optimized taking into account the testing of various target functions of clustering, but those that necessarily ensure the absolute uniformity of the distribution of nodes by clusters.

CONCLUSION

In this work, the ways of improving the Proof-of-Work blockchain technology by implementing dynamic clustering of network nodes in order to reduce the time spent on the transaction, i.e. the goal of the work has been achieved, have been developed and researched.

A technique for improving the blockchain technology with the PoW consensus mechanism and software for its implementation have been developed.

A technique for improving the blockchain technology with the PoW consensus mechanism and software for its implementation have been developed.

The technique of improving the Proof-of-Work consensus mechanism by implementing dynamic clustering of network nodes was studied and analyzed in detail. Optimization of the system parameters is described, experiments are planned to establish the efficiency of the rechnique, system efficiency indicators are analyzed, and an in-depth analysis of the dependencies of the network parameters is carried out. It is found that the cluster system gives improved values of number of transactions per second (by 0.02 transactions), average transaction time (by 1.67 s), throughput (by 0.2 transactions), transaction latency (by 1.667 s) and significantly reduces the total energy consumption of the system (a difference of 5122.07 units). And these values were obtained only for the processing of 30 transactions, which means that when processing more transactions, this positive difference in parameters will only grow. However, it was established that an increase in the number of clusters in the system leads to a decrease in its overall security level and an increase in the risk of an attack by 51 %. So, this study really proves the hypothesis of reducing the time spent on the transaction for the cluster model, this is achieved due to the reduction of the network synchronization time (transmitting the signal to the nodes about the end of mining), but this hypothesis leads to certain security problems that require additional work if it will be decided to implement this technique in a real blockchain network.

REFERENCES

1. Krichen, M. & Ammi, M. "Blockchain for modern applications: A Survey". *Sensors*. 2022; 22 (14): 5274. DOI: https://doi.org/10.3390/s22145274.

2. Sapra, N. & Shaikh, I. "Impact of Proof of Work (PoW) – based blockchain applications on the environment: A systematic review and research agenda". *Journal of Risk and Financial Management*. 2023; 16 (4): 218. DOI: https://doi.org/10.3390/jrfm16040218.

3. Solovyova, D. V. & Antoshchuk, S. G. "Development and research of a simulator for advanced Proof-of-Work blockchain technology". *Thirteenth International Scientific Conference of Students and Young Scientists "Current Information Technology"*. 2023. p. 41–43.

4. Solovyova, D. V. & Antoshchuk, S. G. "Useful blockchain technologies for monitoring climate change". *First International Scientific and Practical Conference "Prospects for the Development of Geoinformation Technologies in the Minds of Climate Change"*. 2023. p. 132–137.

5. Soloviova, D., Antoshchuk, S. & Boltenkov, V. "Development and research of a simulator to improve Proof-of-Work blockchain technology". *IEEE First Ukrainian Distributed Ledger Technology Forum» (UADLTF).* 2023.

6. Saad, S. M. S. & Radzi, R. Z. R. M. "Comparative review of the blockchain consensus algorithm be-tween proof of stake (pos) and delegated proof of stake (dpos)". *International Journal of Innovative Computing.* 2020. DOI: https://doi.org/10.11113/ijic.v10n2.272.

7. Khare, S. & Ashraf, A. et al. "Blockchain: Structure, uses and applications in IoT". In: *Baalamurugan, K., Kumar, S. R., Kumar, A., Kumar, V., Padmanaban, S. (eds). "Blockchain Security in Cloud Computing. EAI/Springer Innovations in Communication and Computing" . Springer, Cham*. 2022. p. 131–144. DOI: https://doi.org/10.1007/978-3-030-70501-5_6.

8. Sriman, B. & Kumar, S. & Shamili, P. “Blockchain technology: Consensus protocol proof of work and proof of stake”. In: *Dash, S. S., Das, S., Panigrahi, B.K. (eds). “Intelligent Computing and Applications. Advances in Intelligent Systems and Computing”*. 2020; 1172. DOI: https://doi.org/10.1007/978-981-15-5566-4_34.

9. Mechkaroska, D. & Dimitrova, V. “Analysis of the possibilities for improvement of blockhain technology”. *26th Telecommunications Forum (TELFOR)*. Belgrade: Serbia. 2018. p. 1–4. DOI: https://doi.org/10.1109/TELFOR.2018.8612034.

10. Kim, J., et al. “Anomaly detection based on traffic monitoring for secure blockchain networking”. *IEEE International Conference on Blockchain and Cryptocurrency (ICBC).* Sydney: Australia. 2021. p. 1–9. DOI: https://doi.org/10.1109/ICBC51069.2021.9461119.

11. Gervais, A. & Ghassan, A. K. “On the security and performance of proof of work blockchains”. In: *ACM SIGSAC Conference*. 2016. p. 3–16.

12. Lee, D. R. & Jang, Y. A. “Proof-of-Stake (PoS) blockchain protocol using fair and dynamic sharding management”. *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS ’19).* London: United Kingdom. 2019. p. 2553–2555. DOI: https://doi.org/10.1145/3319535.3363254.

13. Wendl, M. & Doan, M. H. “The environmental impact of cryptocurrencies using proof of work and proof of stake consensus algorithms: A systematic review”. *Journal of Environmental Management*. 2023. p. 326–328. DOI: https://doi.org/10.1016/j.jenvman.2022.116530.

14. Król, M. & Sonnin, M. A. “Proof-of-Prestige: A useful work reward system for unverifiable tasks”. *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC).* Seoul: Korea (South). 2019. p. 293–301. DOI: https://doi.org/10.1109/BLOC.2019.8751406.

15. Soesanto, D. & Adji, T. B. “Adaptive proof of work architecture design by implementing multiple mempool”. *International Conference on Advanced Creative Networks and Intelligent Systems (ICACNIS).* Bandung: Indonesia. 2022. p. 1–8. DOI: https://doi.org/10.1109/ICACNIS57039.2022.10054940.

16. Arslan, S. & Goker, T. “Compress-store on blockchain: A decentralized data processing and immutable storage for multimedia streaming”. 2019. – Available from: https://www.researchgate.net/publication/333418470_Compress-Store_on_Blockchain_A_Decentralized_Data_Processing_and_Immutable_Storage_for_Multimedia_Streaming. – [Accessed: Dec, 2023].

17. Mahony, A. O. & Popovici, E. A. “Systematic review of blockchain hardware acceleration architectures”. *30th Irish Signals and Systems Conference (ISSC*). Maynooth: Ireland. 2019. p. 1–6. DOI: https://doi.org/10.1109/ISSC.2019.8904936.

18. Hazari, S. & Mahmoud, Q. “Improving transaction speed and scalability of blockchain systems via parallel proof of work”. *Future Internet*. 2020; 12: 125. DOI: https://doi.org/10.3390/fi12080125.

19. Das, D. & Kayal, P. “A k-means clustering model for analyzing the Bitcoin extreme value returns”. *Decision Analytics Journal*. 2023; 6: 100152. DOI: https://doi.org/10.1016/j.dajour.2022.100152.

20. Qin, J. & Fu, W. “Distributed k-means algorithm and fuzzy c-means algorithm for sensor networks based on multiagent consensus theory”. *IEEE Transactions on Cybernetics.* 2017; 47 (3): 772–783. DOI: https://doi.org/10.1109/TCYB.2016.2526683.

21. Dokuz, A., Çelik, A. & Ecemiş, A. “Anomaly detection in bitcoin prices using DBSCAN algorithm”. *Avrupa Bilim ve Teknoloji Dergisi*. 2020. p. 436–443. DOI: https://doi.org/10.31590/ejosat.araconf57.

22. Babichev, S., Durnyak, B. & Zhydetskyy, V. “Application of optics density-based clustering algorithm using inductive methods of complex system analysis”. *IEEE 14th International Conference on Computer Sciences and Information Technologies (CSIT).* Lviv: Ukraine. 2019. p. 169–172. DOI: https://doi.org/10.1109/STC-CSIT.2019.8929869.

23. Dong, S. & Abbas, K. “Blockchain technology and application: an overview”. *PeerJ Computer Science*. 2023; 9: e1705. DOI: https://doi.org/10.7717/peerj-cs.1705.

24. Filtz, E. & Polleres, E. A. “Evolution of the bitcoin address graph”. *Data Science – Analytics and Applications*. 2017. p. 77–82. DOI: https://doi.org/10.1007/978-3-658-19287-7_11.

25. Cachin, C. & Caro, A. “The transaction graph for modeling blockchain semantics. cryptoeconomic systems”. *Cryptoeconomic Systems.* 2020. DOI: https://doi.org/10.21428/58320208.a12c57e6.

26. Li, J. & Ning, Y. “Blockchain transaction sharding algorithm based on account-weighted graph”. In: *IEEE Access.* 2024; 12: 24672–24684. DOI: https://doi.org/10.1109/ACCESS.2024.3365510.

27. Smirnov, A. “The optimized algorithm of finding the shortest path in a multiple graph. modeling and analysis of information systems”. *Modeling and Analysis of Information Systems.* 2020; 30: 6–15. DOI: https://doi.org/10.18255/1818-1015-2023-1-6-15.

28. Frolov, D. “Blockchain and institutional complexity: an extended institutional approach”. *Journal of Institutional Economics*. 2020; 17: 1–16. DOI: https://doi.org/10.1017/S1744137420000272.

29. Amelin, V. S. & Gatiyatullin, E. “Black-Box for blockchain parameters adjustment”. *IEEE Access*. 2022; 10: 101795–101802. DOI: https://doi.org/10.1109/ACCESS.2022.3208702.

30. Milligan, G. W. & Soon, S. C. “The effect of cluster size, dimensionality, and the number of clusters on recovery of true cluster structure”. In: *IEEE Transactions on Pattern Analysis and Machine Intelligence.* 1983; PAMI-5 (1): 40–47. DOI: https://doi.org/10.1109/TPAMI.1983.4767342.

31. Ghosh, E & Das, B. “A study on the issue of blockchain’s energy consumption”. *Proceedings of International Ethical Hacking Conference. eHaCON 2019. Advances in Intelligent Systems and Computing*. 2020. 1065. DOI: https://doi.org/10.1007/978-981-15-0361-0_5.

32. Wuthier, S. & Chang, S. “Demo: Proof-of-Work network simulator for blockchain and cryptocurrency research”. *IEEE 41st International Conference on Distributed Computing Systems (ICDCS).* DC: USA. 2021. p. 1098–1101.

33. Alzhrani, F. & Saeedi, K. Zhao. “Architectural patterns for blockchain systems and application design”. *Appl. Sci*. 2023; 13: 11533. DOI: https://doi.org/10.3390/app132011533.

Conflicts of Interest: the authors declare no conflict of interest

Received 05.03.2024
Received after revision 10.05.2024
Accepted 15.05.2024

DOI: https://doi.org/10.15276/hait.07.2024.9
УДК 004.75

Дослідження можливостей вдосконалення технології блокчейну Proof-of-Work

Соловйова Діана Вячеславівна[1)]
ORCID: https://orcid.org/0009-0007-5253-8848; dianochkasolo1@gmail.com
Антощук Світлана Григорівна[1)]
ORCID: https://orcid.org/0000-0002-9346-145X; asg@op.edu.ua. Scopus Author ID: 8393582500
Болтьонков Віктор Олексійович[1)]
ORCID: https://orcid.org/0000-0003-3366-974X; vaboltenkov@gmail.com. Scopus Author ID: 8575846900
[1)] Національний університет «Одеська політехніка», пр. Шевченка, 1. Одеса, 65044, Україна

АНОТАЦІЯ

Для усунення проблеми з механізмом Proof-of-Work, який розглядається в цій роботі, необхідно вирішити проблему зменшення кількості часу, що витрачається на транзакцію. Це пропонується реалізувати шляхом поділу системи на підмережі: коли консенсус приймається не всією спільнотою, а приймається групами окремо – таким чином мінімізується час транзакції в алгоритмі Proof-of-State. Немає готового рішення для механізму динамічного консенсусу Proof-of-Work, яке було б успішно застосоване в технологіях блокчейн. Всі існуючі алгоритми поділу мережі блокчейн на підгрупи використовуються тільки для статичних алгоритмів, але Proof-of-Work динамічний і має певні особливості: немає області дії, користувач не бачить список вузлів. Ці особливості значно ускладнюють реалізацію кластеризації для механізму консенсусу Proof-of-Work. Завданням даного дослідження є формулювання гіпотез і перевірка сформульованих гіпотез, які спрямовані на підвищення швидкості проведення транзакції. Для перевірки пропонується змоделювати мережу блокчейн для проведення експериментів і перевірки гіпотез, які потенційно можуть вирішити проблему Proof-of-Work. Для удосконалення вдосконалення механізму консенсусу Proof-of-Work шляхом реалізації динамічної кластеризації вузлів мережі враховуються гнучкість і масштабованість, мінімальний вплив на існуючий протокол блокчейну, питання безпеки також важливі, управління процесом прийняття нові вузли, щоб уникнути можливих атак і забезпечити цілісність і безпеку мережі. Проаналізовано існуючі шляхи вдосконалення технології Proof-of-Work, методи кластеризації, які можна застосувати в мережі, виявлено проблеми, які виникають при цьому. Розроблено та впроваджено систему моделювання блокчейн-мережі, за допомогою якої реалізовано підхід динамічного групування вузлів блокчейн-мережі, при якому

система розбита на підсистеми. Результати дослідження дозволяють зробити висновок: кластерна система дає покращені значення кількості транзакцій в секунду (на дві сотих транзакцій), середнього часу транзакцій (на одну і шістдесят сім сотих секунд), пропускної здатності (на дві десяті транзакцій), затримки транзакції (на одну шістсот шістдесят сім тисячних секунди) і істотно знижує загальне енергоспоживання системи (різниця в п'ять тисяч сто двадцять дві одиниці). Це свідчить про потенціал запропонованого методу в різних практичних застосуваннях.

Ключові слова: технологія блокчейн; Proof-of-Work; консенсус Proof-of-Work; механізм консенсусу; симуляція блокчейна; майнінг блокчейнів; час транзакції; мінімізація часу; синхронізація майнінгу; динамічна кластеризація; блокчейн моделювання

ABOUT THE AUTHORS

Diana V. Soloviova – student, Computer Science. Odessa Polytechnic National University, 1, Shevchenko Ave. Odessa, 65044, Ukraine
ORCID: https://orcid.org/0009-0007-5253-8848; dianochkasolo1@gmail.com.
***Research field*:** Blockchain technologies

Соловйова Діана Вячеславівна - магістр, спеціальність «Комп'ютерні науки». Національний університет «Одеська політехніка», пр. Шевченка, 1. Одеса, 65044, Україна

Svitlana G. Antoshchuk – Doctor of Engineering Sciences, Professor, Department Information Systems. Odessa Polytechnic National University, 1, Shevchenko Ave. Odessa, 65044, Ukraine
ORCID: https://orcid.org/0000-0002-9346-145X; asg@op.edu.ua. Scopus Author ID: 8393582500
***Research field*:** Automated management systems and progressive information technologies; information technology; theoretical and applied aspects of multimedia data processing

Антощук Світлана Григорівна – доктор технічних наук, професор кафедри Інформаційних систем. Національний університет «Одеська політехніка», пр. Шевченка, 1, Одеса, 65044, Україна

Viktor O. Boltenkov - PhD, Associate Professor, Information System Department. Odessa Polytechnic National University, 1, Shevchenko Ave. Odessa, 65044, Ukraine
ORCID: http://orcid.org/0000-0003-2777-3137; vaboltenkov@gmail.com. Scopus Author ID: 57203623617
Research field: Blockchain technologies; signal processing

Болтьонков Віктор Олексійович – кандидат технічних наук, доцент кафедри Інформаційних систем. Національний університет «Одеська політехніка», пр. Шевченка, 1. Одеса, 65044, Україна