**S. S. Grybniak**

# DOUBLE-LAYER MODEL OF THE SCALABLE DISTRIBUTED DECENTRALIZED LEDGER

*In spite of the wide application of the distributed decentralized ledgers, in particular, in the popular platforms Bitcoin and Etherium, they inherent major faults. Their main drawback is low speed of transactions processing. To eliminate this drawback, in the given research two-layer model of the distributed decentralized ledger is suggested, this enables not only to increase the speed of transactions processing but increase the scalability. Each of the model layers differs both in the functions, to be performed and in the principle of the network creation. First – it is a network, constructed on the architecture using the directed acyclic graph – DSGChain, which itself creates the blocks. The second – it is a network that is classic blockchain. In this network the formulation of consensus Proof of Stake for the validation and finalization of blocks occurs. Within the frame of the suggested model the method of DAG blocks arrangement has been developed. The given method is based on the introduced notion of the skeletal blocks. The method enables to reduce substantially the traffic between two networks. Method of the optimistic (probabilistic) consensus formation has been developed. Probabilistic consensus enables to reduce the time of blocks finalization. In the process of the coteries formation for PoS consensus new method of mixing on the base of Tent transformation is suggested to use, this method increases the level of ledger security on the whole. On the base of the suggested model its program realization has been created in the form of the Waterfall platform. Loading experiments with the testing network demonstrated that it provides the rate of transactions processing of more than 2000 tps at a high level of scalability. Thus, the combination of the blockchain technologies and DAGChain in one model of the distributed ledger enables to increase the rate of transactions processing by orders. Further direction of the data processing acceleration is the application of sharding in DAGChain network, this can improve the efficiency indices of the distributed ledger.*

***Key words:*** *distributed decentralized ledger, DAGChain, skeletal block, probabilistic PoS consensus.*

## Introduction

Distributed Ledger Technology (DLT) nowadays is one of the most advanced technologies in the sphere of the development of the distributed systems of data processing. First and classic case of DLT became the blockchain technology and Bitcoin cryptocurrency, developed on its base. In recent decade the sphere of blockchain and other DLT applications is rapidly spreading. This causes certain problems, connected with the operation speed and scalability of the distributed ledgers, that is, with the problem of saving of the needed characteristics in case of drastic growth of the number of users. In this aspect, the subject of the given paper, devoted to the construction of the model of the distributed ledger with the increased rate of data processing and high scalability is rather relevant.

## Relevancy

DLT become more and more popular due to the safe and transparent transactions and lack of the mediators or central control organs [1]. It is expected that as a result of growing demand for digital services decentralized technologies will continue gaining popularity in the coming years. Blockchain technology can be used practically in all spheres of human activity. They include first of all various financial services and payment systems [2, 3], medicine [4, 5], support of IoT [6, 7] and many other branches. Distributed system must have scalability mechanism for the adaptation to the change of working load in the wide ranges [8, 9]. However, rate of data processing in the known popular systems Bitcoin and Etherium is not high – these systems process approximately 7 and 15 transactions per second (tps), correspondingly. These indices are incomparable with the conventional centralized systems, which process thousands of transactions per second [10]. There appears the problem of increasing the data processing performance. There exists several options of its solution, one of them is

the increase of the block size (number of the transactions in it), that leads to the problem, connected with the size of the block, namely – blocks of larger size noticeably slower propagate in the network [11]. Another approach is connected with the decrease of the slot duration – time, set for the creation of the block. In this case, it is not excluded, that the block fails to propagate in the network during the set time – such blocks, as a rule, are declined [12]. The third approach to the problem of increasing the performance is parallel creation of several blocks which are sent to several previous blocks, thus forming directed acyclic graph, further DAG. On the base of DAG the accelerated DLT is constructed, it is called BlockDAG [13]. Within the frame on this research it is proposed to combine BlockDAG and Blockchain technologies, in future this will result in the increase of the data processing rate in the distributed ledger and scalability enlargement. This enables to solve the problem, formulated above.

## Objective

**Objective of the paper** – is the construction of the distributed ledger with the increased scalability and increased rate of transactions processing.

## Tasks

1. Creation of the two-layer model of the distributed ledger on the base of two networks with functions distribution.
2. Development of the method of DAG blocks arrangement, taking into account the concept of the structural units.
3. Improvement of the method of the probabilistic consensus formation for the suggested two-layer model.
4. Experimental proof of the improved characteristics of the suggested model.

## Two-layer model of the distributed ledger

For the enhancement of the data processing rate in the distributed ledger and increase of its scalability two-layer model of the distributed ledger, which combines BlockDAG and blockchain technologies and consists of two networks has been suggested.

Basic structural technical element of the network is a node – it is a server, registered in the network, it stores all the corresponding notations in the form of the ledger. At each node certain number of logic structures can be deployed, they are conventionally called Workers, their accounts have necessary data for the participation in the protocol of PoS consensus [14]. Each Worker consists of two components with the independent addresses – Validator and Coordinator.

For the division of the functions of the operation optimization and storage the suggested model of the distributed ledger contains two layers: DAGChain network and coordination network (Fig. 1).

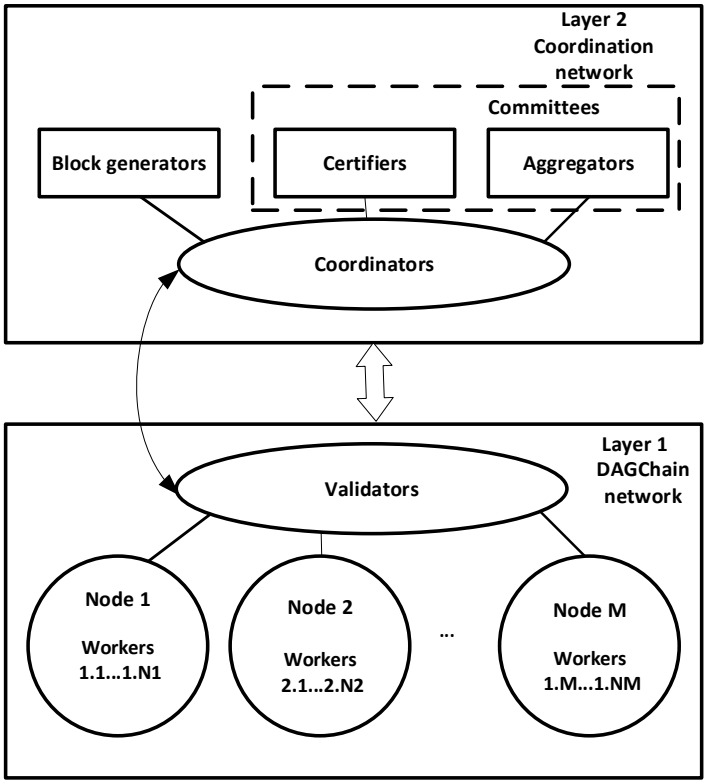


Fig. 1. Two-layer model of the distributed ledger

DAGChain network is constructed on the base of the directed acyclic graph DAG, it can accept the transactions combine them in blocks and create reference DAG.

Coordination network is constructed on the base of the blockchain, it is responsible for the linearization of DAG, finalization of the blocks and selection of the validators, which create blocks at certain time interval.

These two networks will be called layers of the model (in some sources [14] the term «levels» is used).

Time scale in both networks is divided into time intervals – slots of 4 sec, duration during which the actions are synchronized. Validators must create and distribute their block during the slot. Slots are united into the epochs. Epochs are intended for the tabulation of the intermediate results of the network. In the suggested model the epoch consists of 32 slots. The coteries of the validators are appointed for the approval of the blocks for each following slot.

Functions of DAGChain network and coordination network are basically different.

DAGChain network has the following functions:

1. Search of the other nodes and connection with them.

2. Acceptance of the transactions from the users, placement into transaction pool and transmission of the transactions in the network.

3. Determination on the base of the perturbation method, which of the validators creates block in each slot. It should be noted that in the given model the improved perturbation method is used, this enables to increase the speed of the selection of the corresponding validator and improve the cryptosecurity of the system [15].

4. Elimination of the transactions from the pool, adding them to the block, transfer of this block to other participants of the network.

5. Validation of the obtained blocks.

6. Arrangement of the blocks, determination of the so-called skeleton blocks in each slot.

7. Transfer to its coordinating node the order of the skeleton blocks, which are the elements of this node.

8. Obtaining from its coordinating node the order of the skeleton blocks for the finalization. Under the term finalization (or completeness) the process is meant, after the termination of which the transaction in the network is considered to be final and there is no risk of the falsification (change) of the transaction or the block in the arranged chain.

9. Arrangement of the transactions, using the obtained skeleton blocks from the coordinating node and finalization of blocks.

10. Storage of the history of blocks and transactions in the nodes of the ledger.

11. Participation in the synchronization of blocks and transactions.

12. Processing of the special transactions for the activation / deactivation of the validators, saving of the current list of validators, which is used for the determination of the block creation in each slot.

Coordination network is constructed on the basic of the blockchain, in the network the coordinators may perform the following roles:

– creator of the block;

– attestator that signs the last, in its opinion, valid block in the slot;

– aggregator, that combines the results of the attestation by one signature.

Coordinating network performs following functions:

1. Determination by quasi -random method (by means of the improved randomizing algorithm) in each slot of the epoch the composition of the coteries and roles of the coordinators in them (creator, attestator, aggregator).

2. Acceptance of the results of the attestation from other nodes and its transfer across the network.

3. Adding by the block creator of the order of the skeleton blocks, which it obtained from its node, also adding the attestations to the block, which were not added to the block.

4. Transfer by the attestators of their signature of the last block which contains skeleton blocks, with which they agree. This block in its past has the first block of the past epoch with the result of the finalization.

5. Uniting by the aggregators of the attestations in one signature to decrease the number of messages to be transferred between the nodes.

6. According to the obtained attestations and the consensus algorithm of the formation of the skeletal blocks chain to be finalized.

7. Transfer of the final chain of the skeletal blocks in its node of DAGChain network for the finalization.

8. Synchronization of the consensus results with DAGChain network.

9. Obtaining of the information from the DAGChain network about the start of the activation/deactivation of the validators, sending of the information in response, when the validator will be activated / disactivated.

10. Charge of the reward and fees for the coordinators on the base of the obtained attestations.

11. Storage of the history of the blocks and attestations.

12. Storage of the coordinators state (balances, status) in the general state of the network.

## Method of DAG blocks arrangement

To reduce the traffic between DAGChain network and coordinating network the method of DAG blocks arrangement is suggested in the given study, taking into account the concept of the structural blocks.

Let us define the notion of the skeletal blocks and characteristic features of their application. In DAGChain each block is referred to (by the directed edges) all previously formed (parent) blocks. Sometimes the total set of the parent blocks is called «past» of this block. The height of the block is called the number of all parent blocks this block refers to.

*Definition*. Skeletal block – is the block of the slot, which meets the requirement of the following rules:

1) It has the greatest height.

2) If there are several such blocks, the block which refers to the greater number of the previous

blocks is taken.

3) If there are several such blocks, the block which has the smallest hash-code or the block allocated after the randomization procedure is taken.

As each block saves Merkle tree, actually skeletal block saves in the «packed» form all the "past" of the blocks of this slot. That is why, not all the blocks of the slot can be transferred to the coordinating network but only skeletal blocks. This enables to reduce the traffic between DAGChain network and coordinating network *n* times, where *n* – is a number of blocks, formed in the slot.

This allowed to suggest the method of DAG blocks arrangement, using the skeletal blocks, the given method is realized by the following algorithm:

1. Skeletal block of each non-finalized slot is determined, skeletal blocks are arranged in the order of their direction from the least number of the slot to greater.

2. First skeletal block is selected.

3. Non- finalized parent blocks of this block are taken and arranged by the height (by the principle «the more, the earlier»); if the height is the same, the blocks are arranged by the number of the references to the previous blocks (parents); if the number of references is the same, the blocks are arranged by the smallest hash-code or applying the randomization procedure. This block is installed in the list before the skeletal block.

4. Point 3 is repeated recursively for the inclusion of the parents blocks until all the parents blocks are either finalized or are already in the arranged list. Parents blocks are included in the list before the selected block.

5. Points 3 – 4 are repeated with all the skeletal blocks in order.

As a result, the arranged succession of all DAG blocks is formed.

## PoS consensus in the two-layer model

Main task, performed by the participants of the coordinating network (coordinators) – is the formation of the agreed common thought about the state of the network, which will not change but will be supplemented with new data. There exists two approaches regarding the formation of the consensus, their selection is stipulated by the relation of the «probability of the correct decision / time of the decision taking (finalization of the decision): complete (final) PoS consensus or optimistic (probabilistic) consensus.

In the suggested model, as a rule, the complete (final) PoS consensus is used for the coordination of the network state, it operates according to the following algorithm:

1. For the complete consensus each coordinator during the epoch votes for the first valid block of the previous epoch.

2. If the block got more than 2/3 of votes of all the coordinators, then the block is considered to be finalized, and, as the result, the chain of the skeletal blocks of DAGchain network from the past finalized block is also considered to be finalized and is sent into DAGchain network as finally approved.

3. If in the epoch there are 32 slots and the duration of the slot is 4 seconds then the transaction will pass in 2*32*4=256 seconds = 4 min 16 seconds.

But for the numerous practical applications, to reduce the finalization time, in the given research the improvement of PoS consensus method by means of the formation of the optimistic (probabilistic) consensus is suggested, it is realized in the following way:

1. Attestators of the slot in the previous slot exchange skeletal blocks, which they see in the DAGchain. The author of the coordinating block uses this information to indicate optimal chain of the skeletal blocks and increase the chances that the majority will vote for it.

2. Attestators vote not only for the first block of the previous epoch but also for the last block of the coordinating network (in the ideal variant, for the block, created in the same seat), which contains the chain of the skeletal blocks, which it sees in its DAGchain node and agrees with the available sequence.

3. If the initial part of the chain of the skeletal blocks repeated *m* times and more than half of the participants of the corresponding slots voted for these blocks, then this chain is the candidate for the

finalization and is sent to DAGchain node for the prefinalization.

4. After finalization of the chain of the skeletal blocks into DAGchain network it is written in the block of the coordinating network and these skeletal blocks further are not suggested as the candidates.

Such an approach enables to reduce considerable the time of decision finalization at sufficient probability of the correct decision. Simulation of the suggested method of consensus formation (jointly with the randomization) was performed and it was established that the obtained at the final consensus arrangement will not change with the probability non less than 0.9. But the forecast of the possible finalization can be obtained during 3*4=12 seconds. Further acceleration can be achieved by decreasing the slot duration.

## Experimental verification of the quality indices of the developed model

Nowadays basic elements of the suggested model of the two-layer distributed scalable ledger, using the above-mentioned methods of data processing are realized in programming language Golang [16]. Test network is constructed on the base of the servers Amazon Elastic Compute Cloud compute cloud. Loading experiments have been carried out. For the laboratory studies test network operated on 64 samples t3.small (with double core central processor and 2 GB memory) Amazon EC2.

In the process of the experiment the pool with approximately 100 000 transactions was generated, the time, during which the last of the transactions will be written in the ledger is recorded. Significant growth of the transactions processing speed is registered, in this way the test network demonstrated average speed of 2234 tps.

## Conclusions and directions of further research

As a result of the studies, carried out the problem of increasing the scalability and transactions processing speed was solved after the realization of the following tasks:

1. Two-layer model of the distributed ledger, combining basic network, constructed using DAGChain technology and coordination network, based on the conventional blockchain technology has been suggested. Tasks, to be solved by the networks, are divided according to the functional characteristic.

2. Method of the accelerated arrangement of DAG blocks, taking into account the concept of structural blocks has been developed.

3. Method of the formation of the probabilistic PoS consensus within the frame of the suggested two-layer model has been improved.

4. Two-layer model, which realizes the distributed ledger with the average rate of the transactions processing that exceeds 2000 tps at rather high scalability has been created.

This experimentally proves the improvement of the characteristics of the suggested model. Thus, all the tasks, put forward, have been solved, the objective of the study has been achieved. As the direction of the further study the construction of DAGChain network with the sharding, with the usage of the subnetworks is considered, this can improve the quality indices of the distributed ledger.

## REFERENCES

1. Decentralized platforms: Goals, challenges, and solutions / S. Grybniak, Y. Leonchyk, R. Masalskyi [et al.] // IEEE 7th Forum on Research and Technologies for Society and Industry Innovation (RTSI). – 2022. – P. 62 – 67. DOI : 10.1109/RTSI55261.2022.9905225.

2. Trivedi S. Systematic Literature Review on Application of Blockchain Technology in E-Finance and Financial Services / S. Trivedi, K. Mehta, R Sharma // Journal of Technology Management & Innovation. – 2021. – Vol. 16, № 3. – P. 89 – 102. DOI:10.4067/S0718-27242021000300089.

3. Mihus I. Evolution of practical use of blockchain technologies by companies / I. Mihus // Economics, Finance and Management Review. – 2022. – Vol. 1. – P. 42 – 50. DOI:10.36690/2674-5208-2022-1-42.

4. Applications of Blockchain in the Medical Field : Narrative Review / Y. Xie, J. Zhang, H. Wang [et al.] // J. Med. Internet Res. – 2021. – Vol. 23, № 10. – P. 286 – 294. DOI: 10.2196/28613.

5. Blockchain Technology Applications in Healthcare : An Overview / A. Haleem, M. Javaid, R. Pratap [et al.] // International Journal of Intelligent Networks. – 2021. – Vol. 2. – P. 130 – 139. DOI:10.1016/j.ijin.2021.09.005.

6. Moudoud H. Towards a Scalable and Trustworthy Blockchain : IoT Use Case / H. Moudoud, S. Cherkaoui, L. Khoukhi // IEEE International Conference on Communications, Montreal, QC, Canada. – 2021. – P. 1 – 6. DOI : 10.1109/ICC42927.2021.9500535.

7. Abbassi Y. IoT and Blockchain combined : for decentralized security / Y. Abbassi, H. Benlahmer // Procedia Computer Science. – 2021. – Vol. 191. – P. 337 – 342. https://doi.org/10.1016/j.procs.2021.07.045.

8. Solutions to Scalability of Blockchain : A Survey / Q. Zhou, H. Huang, Z. Zheng [et al.] // IEEE Access. – 2020. – Vol. 8. – P. 16440 – 16455. DOI: 10.1109/ACCESS.2020.2967218.

9. A Survey on the Scalability of Blockchain Systems / J. Xie, F. R. Yu, T. Huang [et al.] // IEEE Network. – 2019. – Vol. 33, № 5. – P. 166 – 173. DOI: 10.1109/MNET.001.1800290.

10. Hafid A. Scaling Blockchains: A Comprehensive Survey / A. Hafid, A. S. Hafid, M. Samih // IEEE Access. – 2020. – Vol. 8. – P. 125244 – 125262. DOI: 10.1109/ACCESS.2020.3007251.

11. Brilliantova V. Blockchain and the future of energy / V. Brilliantova, T. W. Thurner // Technology in Society. – 2019. – Vol. 57. – P. 38 – 45. DOI:10.1016/j.techsoc.2018.11.001.

12. Comparison of block expectation time for various consensus algorithms / D. S. Kaidalov, L. V. Kovalchuk, A. O. Nastenko [et al.] // Radio Electronics, Computer Science, Control. – 2019. – Vol. 4. – P. 159 – 171. DOI:10.15588/1607-3274-2018-4-15.

13. Swaroopa Reddy B. UL-blockDAG : Unsupervised Learning based Consensus Protocol for Blockchain / B. Swaroopa Reddy, G. V. V. Sharma // IEEE 40th International Conference on Distributed Computing Systems (ICDCS), Singapore, Singapore. – 2020. – P. 1243 – 1248. DOI: 10.1109/ICDCS47774.2020.00159.

14. Understanding Ethereum via Graph Analysis / T. Chen, Y. Zhu, Z. Li [et al.] // IEEE INFOCOM 2018 - IEEE Conference on Computer Communications, Honolulu, HI, USA. – 2018. – P. 1484 – 1492. DOI: 10.1109/INFOCOM.2018.8486401.

15. Grybniak S. Basic principles of mixing functions based on the simplest linear and nonlinear mappings / S. Grybniak, D. Dmytryshin // Proceedings of Odessa Polytechnic University. – 2022. – Issue 2 (66). – P. 100 – 109. DOI: 10.15276/opu.2.66.2022.12.

16. Waterfall [Electronic resource] / Access mode : https://waterfall.foundation/.

Editorial office received the paper 15.05.2023.
The paper was reviewed 25.05.2023.

***Grybniak Sergyi*** – Post-Graduate with the Department of Applied Mathematics and Information technologies.
National University «Odeska Polytechnica.