AUTOMATA MODEL OF A SYSTEM WITH DISTRIBUTED LEDGER TECHNOLOGY BASED ON A BLOCKCHAIN

O.Ja. Kravets(1), Ali Husein(1), D.V. Getmanskaia(1), Mustafa Jaafar Baqer Al-Imari(1), I. A. Chernoivanenko(1), Yu.V. Redkin(2), O.O. Varlamov(3)*

(1) Voronezh State Technical University, Voronezh; (2) Admiral Ushakov Maritime State University, Novorossiysk; (3) Bauman Moscow State Technical University
Russian Federation

* Corresponding Author, e-mail: csit@bk.ru

Abstract: The article discussed an automata model of the functioning process of a system with distributed ledger technology based on a blockchain. The goal is to develop a special mathematical system with a distributed ledger based on a blockchain, taking into account the specifics of implementing algorithms for mutual information coordination, the possibility of combining individual nodes into groups, and implementing alternative strategies based on the development of appropriate models and algorithms that ensure increased stability in their operation. Automata theory was used, theory and methods of mutual coordination were applied, and the mechanism of the functioning process of a system with a distributed register was implemented. An automata model has been obtained and investigated. Thus, an automata model of the distributed ledger technology blockchain system node functioning process has been developed, which differs from the node representation by a finite state machine with a variable structure and a linear tactic with the possibility of implementing non-standard functions: the formation of a branch of processed data and a temporary blockage attack, and provides for obtaining the dependence of the sequence of changing the node's behavior strategy options on the conditions of the environment it interacts with.

Key words: Automata model, blockchain, mutual information coordination, temporary blockage attack, node's behaviour strategy options.

1. INTRODUCTION

An important area of improvement for distributed software systems is the use of distributed ledger technology (DLT) concepts and solutions in their architecture. DLT is a decentralized approach to data storage, creating multiple copies of data and synchronizing them using mutual information coordination (MIC) algorithms. The article expands on the research in [1] by clarifying the state transition order of the automata model of a blockchain-based distributed registry system.

MIC algorithms are subject to requirements for fault tolerance and account for the

possibility of abnormal operation of individual nodes. The software of practical implementations of DLT systems, such as peer-to-peer payment systems [2], uses blockchain technology (in the terms of DLT systems – blockchain; DLT BC), which generally satisfies the requirements listed above.

However, most of the research results in this area do not fully take into account the simultaneous implementation of several non-standard functions by the nodes, such as the formation of a branch of processed data (fork version) and a time-lock attack [3] (hiding the generated block from other system nodes).

The goal of the paper is to examine existing protocols for achieving mutual information agreement between DLT system nodes, which are aimed at solving the FLP problem using synchronization and non-determinism (considering BC-based DLT systems) in the event of system node failures and the implementation of abnormal functions. The paper highlights the advantages and disadvantages of these solutions. In this reason a review of related works is discussed in the next section and approach for organization of investigation and analysis is presented in the Section 3. The results obtained are presented in Section 4.

2. RELATED WORK

Thus, in the software of payment peer-to-peer systems [4], nodes seek to increase their efficiency in performing the MIC algorithm by changing their behavior: choosing between working according to the specified rules and abnormal functioning, thus defining the strategy of behavior. In this case, the options of strategies of behavior of nodes are either not taken into account or proprietary algorithms [5] are used for them, specific to a particular implementation of the DLT BC system and taking into account the options of the strategy of the node's behavior only separately. In addition, the ability to combine nodes into groups leads to the centralization of the distributed system, which negatively affects its stability and increases the likelihood of a single BC. Centralization also increases the likelihood of individual nodes or groups of nodes implementing non-standard functions [6], which can lead to the formation of an alternative BC. This approach necessitates the improvement of the mathematical software of DLT BC systems to implement various MIC algorithms.

Thus, it is necessary to formalize the process of functioning of a distributed registry system node based on a block chain in the form of a finite-state model that allows for modeling the variability of its behavior strategy.

The purpose of this work is to develop a special mathematical system with a distributed ledger based on a blockchain, taking into account the specifics of implementing algorithms for mutual information coordination, the possibility of combining individual nodes into groups, and implementing alternative strategies based on the development of appropriate models and algorithms that ensure increased stability in their operation.

A study of existing approaches to the management of DLT-systems when achieving mutual information agreement between their nodes.

The analysis of the properties of DLP-systems is carried out: parallel execution of processes [7], the absence of global clocks [8], resistance to failures [9], asynchronous

transmission of messages. Formulated the definition of mutual information agreement, considered the conditions for achieving mutual information agreement between the nodes of a DLT-system. Fig. 1 shows the generalized architecture of the network of the considered DLT-systems.

There is a problem of the impossibility of achieving MIC between deterministic asynchronous processes in a fixed time with one process that is not working (FLP problem), and approaches to its solution have also been developed: synchronization or the use of non-determinism. The stability of DLT systems to failures is considered, and the classification of violations in the operation of system nodes when achieving mutual information agreement is carried out: failure (failure) of the node, implementation of abnormal functions (Byzantine attack [10], Sybil attack [11], time delay attacks [12]).

3. INVESTIGATION ORGANIZATION

The structure of a DLT-system based on BC was analyzed when achieving mutual information agreement between its nodes, and the theoretical principles aimed at solving the problems of failures and the implementation of abnormal functions by the system nodes were considered. The conditions were determined and the possibility of implementing attacks of temporary blocking and the formation of branches of processed data was concluded.

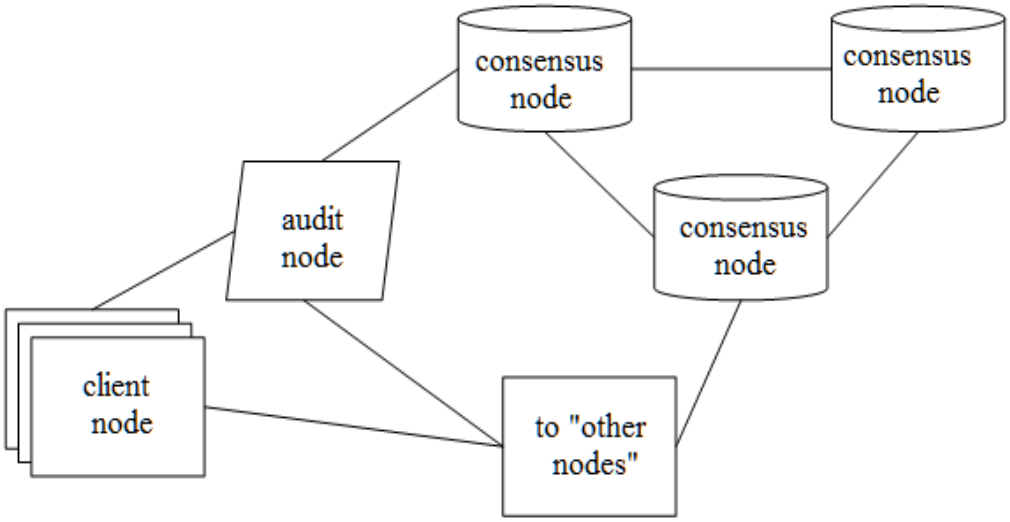

Figure 1. Generalized architecture of a DLT system network

The analysis of existing models of peer-to-peer systems based on Nakamoto and GHOST algorithms for achieving mutual information agreement was carried out [13].

Automata model of the functioning process of a system with a distributed register is given on the Fig. 2 [1].

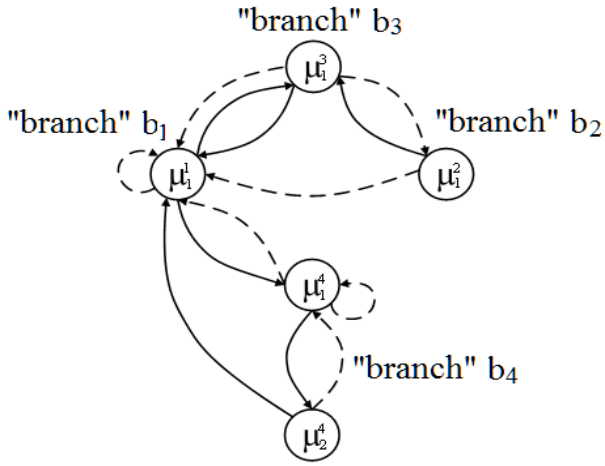

Figure 2. Automata model of the DLT BC system node, taking into account the variability of its behavior strategy

4. THE ORDER OF STATE CHANGES IN AN AUTOMATA MODEL OF A SYSTEM WITH A DISTRIBUTED REGISTRY BASED ON A BLOCKCHAIN

The stable states μ_j^i included in the b_1 behavior strategy options of the am automata determine the execution of actions aimed at achieving the MIC. As mentioned above, for the MIC algorithm of the abstract DLT BC system, the branches of the B tree will have one stable state each (except for b_4). Let's define the functions, output signals of the automata a_i, environmental reactions, and the order of state transitions.

Let's define the initial state as μ_1^1. When starting the MIC algorithm or returning to the initial state μ_1^1, the a_i automata must check the presence of connections with neighboring automata from the set A, the relevance of its BC, and, if necessary, adjust the state matrix $\|a_{ij}(X^m(t_n))\|$. After these actions, the automata executes the MIC algorithm, solving the Proof-of-X problem to find the next block.

According to the rules for adding a block to a single BC of various MIC algorithms (Nakamoto, GHOST, etc.), the next block may be considered to be the block that forms the most "long" (the number of blocks before the Genesis block), "heavy" (the number of blocks, including "uncles"), etc. BC. Let's introduce a rule for determining the block that should be added to a single BC according to the requirements of the abstract algorithm for achieving MIC in a DLT BC system: let's call the block that meets all security requirements and is the next block to be added to a single BC according to the MIC algorithm rules, the block with the highest value. The concept of "value" will mean the longest length for MIC Nakamoto, the heaviest weight for MIC GHOST, etc.

The functions performed by the automata in the states of branch 1 will be defined as:

a) creating and maintaining a minimum number of connections with other automata in set A;

b) updating or rewriting (if necessary) the BC;

c) checking the main BC;

d) adjusting the state matrix $\| a_{ij}(X^m(t_n)) \|$;

e) executing the Proof-of-X algorithm.

The need to perform the functions of points a and b will be determined by the failure mechanism. Let's define the output signal y_1 of the am automata in state μ_1^1 as a request for the main block of the unified BC. The reaction x_k of the environment E to the output signal y_1 can be:

- a favorable reaction $X^m(t_n)[+1]$ expressed by confirming that the block found by the a_m automata, which satisfies all the security and DLT algorithm criteria, can be accepted next, since the head block in a single BC is, for example, "parent" for the Nakamoto algorithm or "smaller" for the GHOST algorithm. Let's call such blocks "previous";

- an adverse reaction $X^m(t_n)[-1]$ can manifest itself as a failure (lack of connection with neighboring automata or other technical issues) or as confirmation that another block based on the previous one has been accepted into the unified BC.

The output signal y_1 is a request from the head block of the unified BC, caused by the unsuccessful execution of the Proof-of-X algorithm. This will result in a reaction x_k from the environment E, which is classified as unfavorable $X^m(t_n)[-1]$, but it will not affect the state matrix $\| a_{ij}(X^m(t_n)) \|$. If the Proof-of-X algorithm fails, the a_m automata remains in the state μ_1^1 and sends the output signal y_1 until it finds a new block that meets all the criteria.

In the event of a favorable response $X^m(t_n)[+1]$ to the output signal y_1, the single BC request for the header block is processed by the BC automata a_m, which, depending on the probability values in the state matrix $\| a_{ij}(X^m(t_n)) \|$, either transitions to the μ_1^3 of b_3 branch to publish the found block or to the b_4 branch to attempt a time-lock attack.

In the event of an unfavorable reaction $X^m(t_n)[-1]$ to the output signal y_1, the a_m automata, depending on the probability values of the state matrix $\| a_{ij}(X^m(t_n)) \|^-$, either transitions to the b_2 branch state μ_1^2 to attempt to form a branch of the processed data (fork version BC), or remains in the initial b_1 branch state μ_1^1.

After entering the state μ_1^3 of branch b_3, the automata "honestly" publish the found block in order to add it to the unified BC. Thus, the reactions x_k of the environment E to the output signal y_1 - the found block will be:

- a favorable reaction $X^m(t_n)[+1]$: the block is accepted by the majority of the network's automata, i.e., it is added to the unified BC;

- an unfavorable reaction $X^m(t_n)[-1]$: the alternative block is accepted.

In the case of a favorable reaction $X^m(t_n)[+1]$, the a_i automata receives a reward, increases the probability of transition to branch b_3 in the state matrix $\| a_{ij}(X^m(t)) \|^+$, and transitions to state μ_1^1 for further execution of the DLT algorithm.

In the case of an unfavorable reaction from the environment E, the automata, depending on the values of the state matrix probabilities $\| a_{ij}(X^m(t_n)) \|^-$, will either transition to state μ_1^2 of branch b_2 to attempt to form a fork version of BC, or return to state μ_1^1 of branch 1 and continue searching for a new block.

The states of branch 2 are characterized by the choice of a strategy for forming a branch of processed data (a fork of the unified BC). At the moment of transition of the a_m automata from the states of branch 3 to the states of branch 2, the published block was not accepted by the majority of DLT BC system automata, but has the same rights (fulfills the requirements of the DLT algorithm) as the alternative block accepted into the unified BC. Consequently, when generating the next block by the a_m automata, it is possible to create a fork version of the unified BC.

Since the automata has a linear tactic, it will learn during its operation with the external environment E, and its behavior will become appropriate due to the constant correction of the system of two state matrices $\| a_{ij}(X(t_n)) \|^+$ and $\| a_{ij}(X^m(t_n)) \|^-$. As a result, matrices will be formed and the most probable variants of the strategy of the automata's behavior depending on the conditions of the state of the environment will be determined.

5. CONCLUSION

1. An automata model of the DLT BC system node functioning process has been developed, which differs from the node representation by a finite state machine with a variable structure and a linear tactic with the possibility of implementing non-standard functions: the formation of a branch of processed data and a temporary blockage attack.

2. The process of functioning of a node of a system with a distributed registry based on a block chain is formalized in the form of a finite state machine with a variable structure and a linear tactic, which ensures that the sequence of changing the node's behaviour strategy depends on the state conditions of the environment it interacts with, by constructing state matrices.

3. The order of changing the states of the automata model of a system node with a distributed registry based on a blockchain chain is determined, depending on the environment's reactions.

The continuation of research is related to the development of an algorithm for the functioning of a blockchain-based distributed registry system that ensures a specified average block generation delay time, depending on the node behavior strategies and the

system's centralization ratio. The implementation of special software elements for managing the operation of a distributed registry system based on a blockchain will also be carried out, which ensures that the stability of the system's operation is assessed based on factors that influence the likelihood of alternative blockchain formations.

REFERENCES

[1] Kravets O. Ja., Almusawi O. A. R., Doroshenko Ju. N. et al. Security management of the functioning of a multi-node mobile cyber-physical system with a distributed registry based on an automatic model. *Journal of Physics: Conference Series*, vol. 2094, art. no. 042040, 2021. https://doi.org/10.1088/1742-6596/2094/4/042040.

[2] Reddy A., Banda G. ElasticPay: Instant Peer-to-Peer Offline Extended Digital Payment System. *Sensors*, vol. 24, art. No. 8034, 2024. DOI: 10.3390/s24248034.

[3] Heisel L., Weber M. Acid attacks on pin-tumbler locks. *Journal of forensic sciences*, vol. 70, 2024. DOI: 10.1111/1556-4029.15647.

[4] Mai X., Nguyen T. Switching behaviors in peer-to-peer mobile payment applications: the role of sociability. *Journal of Systems and Information Technology*, 2023, vol. 26. DOI: 10.1108/JSIT-05-2023-0082.

[5] Wallace L. Cracking the code-matching a proprietary algorithm for a low-cost sensor measuring PM1 and PM2.5. *Science of The Total Environment*, vol. 893, 2023, art No. 164874. DOI: 10.1016/j.scitotenv.2023.164874.

[6] Chithra P.L., Aparna R. Blockchain enabled dual level security scheme with spiral shuffling and hashing technique for secret video transmission. *International Journal on Information Technologies and Security*, vol. 15, no. 2, 2023, pp. 97-108. DOI: 10.59035/UBSN9044.

[7] Yu B., Zhao H., Zhou T. et al. TCHAO: parallelism with transaction classification and grouping by historical access objects to scale blockchain. *Journal of King Saud University Computer and Information Sciences*, vol. 37, 2025. DOI: 10.1007/s44443-025-00090-7.

[8] Guo W., Zhu M., Shengfeng G. et al. Linear quadratic Gaussian-based clock steering system for GNSS real-time precise point positioning timing receiver. *GPS Solutions*, vol. 28, no. 1, 2023. DOI: 10.1007/s10291-023-01592-5.

[9] Fernández-Bravo P., Javier F., Arjona A. et al. DELTA: A Modular, Transparent, and Efficient Synchronization of DLTs and Databases. *International Journal of Network Management*, vol. 34, no. 5, 2024. DOI: 10.1002/nem.2293.

[10] Long G., Zhang Z. Adaptive Update Distribution Estimation under Probability Byzantine Attack. *Computers, Materials & Continua*, vol. 81, no. 1, 2024, pp. 1667-1685. DOI: 10.32604/cmc.2024.052082.

11. Vijayalakshmi D.M. Securing DSR protocol defending against sybil attack in MANET. *International journal of scientific research in engineering and management*, vol. 07, no. 04, 2023. 10.55041/IJSREM19009.

12. Ramani S., Jhaveri R.. SDN Framework for Mitigating Time-Based Delay Attack. *Journal of Circuits, Systems and Computers*, vol. 31, no. 15, 2022. DOI: 10.1142/S0218126622502644.

[13] Kang Y., Hailey C., Liu B., Zhang D. Ghost Key Distribution under Mutual Authentication Mechanism. *Information Sciences*, vol. 640, no. 2, art. no119025, 2023. DOI: 10.1016/j.ins.2023.119025.

[14] Zetzsche D., Anker-Sørensen L., Passador M., Wehrli A. DLT-based enhancement of cross-border payment efficiency – a legal and regulatory perspective. *Law and Financial Markets Review*, vol. 15, no 1-2, 2022, pp. 1-46. DOI: 10.1080/17521440.2022.2065809.

Information about the authors:

Oleg Jakovlevich Kravets – Dr. Sci (IT), professor of Voronezh State Technical University, areas of scientific research - system analysis, optimization, simulation of complex objects

Ali Husein – postgraduate student of of Voronezh State Technical University, areas of scientific research – system analysis, optimization, simulation of complex objects

Diana Viktorovna Getmanskaia - postgraduate student of of Voronezh State Technical University, areas of scientific research – information technology, system analysis, modeling

Mustafa Jaafar Baqer Al-Imari – postgraduate student of of Voronezh State Technical University, areas of scientific research – system analysis, optimization, simulation of complex objects

Igor Aleksandrovich Chernoivanenko – postgraduate student of of Voronezh State Technical University, areas of scientific research - system analysis, optimization, simulation of complex objects

Yuriy Viktorovich Redkin – PhD, associate professor of Admiral Ushakov Maritime State University, Novorossiysk, areas of scientific research - wireless networks, digital signal processing, control and data processing systems

Oleg Olegovich Varlamov – Dr. Sci (IT), professor of Bauman Moscow State Technical University, areas of scientific research - artificial intelligence, decision-making systems, optimization, simulation of complex objects

Manuscript received on 05 September 2025