

ALGORITHMS FOR ACHIEVING MUTUAL INFORMATION COORDINATION

O. Ja. Kravets (1), B. V. Martynenkov (1), A. V. Tsvetkov (1), E. O. Puzhanova (1), D. I. Mutin (2), P. V. Bespalov (1), Yu. V. Redkin (3)*

⁽¹⁾Voronezh State Technical University, Voronezh; ⁽²⁾Moscow State University of Technology “STANKIN”, Moscow; ⁽³⁾Admiral Ushakov Maritime State University, Novorossiysk, Russian Federation

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

Abstract: The article discussed an algorithm for achieving mutual information coordination for a system with distributed ledger technology based on a blockchain. The goal is to develop a generalized approach to formalizing the operation of the distributed ledger technology blockchain system in the course of achieving mutual coordination, including taking into account the possibilities of implementing abnormal functions by the distributed ledger technology blockchain node of the system and grouping nodes. The rules of block chain formation in algorithms for achieving mutual information coordination are proposed. The process of achieving mutual information coordination is described. A mathematical model of the process of achieving mutual information coordination between the nodes of the distributed ledger technology blockchain system is proposed, which differs in the representation of the system by a team of finite automata with the possibility of creating associations (pools) and providing an assessment of the centralization of the system in the conditions of choosing different variants of behaviour strategy by automata.

Key words: implementing abnormal functions, blockchain, mutual information coordination, representation of the system, team of finite automata.

1. INTRODUCTION

Currently, few works are devoted to the development of models of the process of achieving mutual coordination (MIC) in distributed ledger technology (DLT) blockchain (BC) systems based on empirical justification of their adequacy. In addition, most of the well-known theoretical models only takes into account the hash rate and the influence of time parameters, while the possibility of implementing abnormal functions of the system node behaviour strategy, such as a time lock attack and the formation of a fork of processed data, is not taken into account. The aim is to develop a generalized approach to formalizing the operation of the DLT BC system in the course of achieving MIC, including taking into account the possibilities of implementing abnormal functions by the DLT BC node of the system and grouping nodes.

2. EXISTING APPROACHES TO MODELING THE OPERATION OF A DISTRIBUTED LEDGER SYSTEM

This article continues the research [1].

The first and most well-known approaches devoted to assessing the stability of DLT BC systems using the MIC Nakamoto algorithm were proposed in [2, 3]. An approach to assessing the stability of DLT BC systems using the MIC GHOST algorithm was proposed in [4] and implemented as a model in [5, 6]. These approaches provide approximate estimates of the probability of alternative BC formation due to assumptions and significant simplifications. In addition, they are divorced from the real processes taking place in the MS, i.e. they are not realistic. In particular:

- it is assumed that the values of the probabilities of block generation by the nodes of the system do not change over time, however, in real DLT BC systems, nodes can adjust the probability of generation by changing their resource capacities [7];

- the economic feasibility of conducting attacks by a group of attacking nodes is not taken into account. The resources of the attacking node group are considered limitless, which is not true [7];

- the accepted assumption of generating a block with an average waiting time is not always correct [2];

- the assumption made by M that the block propagation time in the system is zero is also not always correct, it is necessary to take into account the network synchronization time [3].

Many works refine and supplement the obtained approaches and estimates for various special cases, without significantly improving the practical suitability of the estimates obtained. Empirical approaches to evaluating the effectiveness of the proposed methods [6, 7] are based on the model of player ruin, verified by Monte Carlo methods. The player's ruin model allows us to obtain a formula for calculating the probability of forming an alternative BC.

3. COMPARATIVE ANALYSIS OF ALGORITHMS FOR ACHIEVING MUTUAL INFORMATION COORDINATION BETWEEN NAKAMOTO AND GHOST

Analysing the two payment systems Ethereum and Bitcoin for algorithms to achieve MIC, the following differences and general principles can be identified. Messages (transactions) in Ethereum are more variable (sending messages, creating a contract) compared to the Bitcoin system, but the data has the same structure: they are grouped into blocks, which in turn form a BC. The node that adds the next block to BC is also determined during the mining process (Proof-of-X algorithms). The algorithm for determining the node forming the next block in both Ethereum and Bitcoin is of the PoW type [8]. Currently, Ethereum uses a PoW algorithm called Ethash [9], and in the future, it is planned to switch to the Prof-of-Stake (PoSt) protocol. We assume that differences in hashing protocols, cryptographic encoding, transaction fields and blocks, as well as the exchange of service data between network nodes will not be taken into account due to the indirect impact on non-determinism.

In Ethereum, when a new block is found, a node receives an incentive reward, the so-called "fuel" measured in "gwei". The price of "fuel" is the number of digital tokens, called Ether, equal to one "gwei". Each of the miners strives to receive a reward – to add their generated block to BC. During this race, it is possible that some nodes accept block number 1, and another block number 2. A "fork" of BC occurs. To combat this phenomenon, Ethereum uses the GHOST (Greedy Heaviest Observed Subtree) protocol [6].

The main distinguishing features of the MIC GHOST algorithm from the Nakamoto algorithm in BC formation are:

- the ability to add headers of "ommer" blocks, the parent of which is the parent element of the current block.
- the principle of formation of the main block chain. The main block chain is not the "longest" BC, but the "heaviest" one.
- as a result, there is a shorter delay time for generating blocks approximately every 15 s.

If the block validation was performed in a shorter period of time than T , the system adjusts (increases) the complexity of the subsequent block S_{block} . In turn, the complexity of the block affects the corresponding field, for example, "nonce" in the block header [10]. This dependence is expressed by the formula:

$$\text{Com}_{\text{nonce}} = \frac{2^{256}}{S_{\text{block}}}, \quad (1)$$

where $\text{Com}_{\text{nonce}}$ is the complexity of calculating the hash field "nonce".

The motivation for nodes to include "ommer" blocks is an additional reward in the form of 1/32 of the total payment for the current block. There are two main requirements for "ommer" blocks: the block must have a valid header and be no higher than the sixth descendant of the current block.

This leads to differences in the rules for determining the validity and order of adding blocks to BC:

- a valid block is considered to be a block that not only refers to the previous valid block, but also to blocks no older than the 6th generation;
- the block with the highest "weight" is added to BC, not the length,
- that is, with the largest number of blocks preceding it, including "ommer".

4. RULES FOR THE FORMATION OF A BLOCK CHAIN IN ALGORITHMS FOR ACHIEVING MUTUAL INFORMATION COORDINATION

To describe the structure of algorithms for achieving MIC in various DLT BC systems, we decompose the algorithm into the following stages: determining the leader node that generates the next block and accepting the new block by the nodes of the DLT BC system.

At the stage of determining the leader, the MIC achievement algorithms use the "Proof-of-X" class of algorithms. We formalize protocols for determining the sequence of block formation in the form of functions $P(t_n, A)$, where t_n is the n th time interval,

and A is the set of automata involved in the MIC achievement algorithm. The function $P(t_n, A)$ generates a slot machine number $a_z \in A$ with some probability. The probability $p_{t_n}^z$ of generating the z -th number of the machine in the time interval t_n is determined by the following expression:

$$p_{t_n}^z = \frac{1}{T} \frac{h_z}{\sum_{i=1}^{|A|} h_i}, \tag{2}$$

where T is the specified delay time interval for generating blocks, which is determined by the security requirements of a specific implementation of the MIC algorithm, h_z is the resource capacity (hash power, machine share, etc.) a_i , $\sum_{i=1}^{|A|} h_i$ is the total resource capacity of the entire set of automata A .

5. THE PROCESS OF ACHIEVING MUTUAL INFORMATION COORDINATION

Based on the automatic model of the functioning of the DLT BC node of the system, let's consider the process of achieving MIC in the DLT BC system. Structurally, the DLT BC system will be represented by a decentralized peer-to-peer network consisting of peer nodes. In DLT systems, the locations and times of adding or removing nodes from the network are random, therefore, the connections formed between the machines will also be random. At the same time, the list of address information of the machine should be formed taking into account the minimum number of outgoing connections for various algorithms for achieving MIC specific DLT BC systems. From this we can conclude that the environment E in which the automaton operates should be represented by a stochastic switchable environment.

Let us consider an abstract DLT BC system represented by a set A (collective) of automata $a_1 - a_k$ interacting with a stochastic switchable medium E , which for each m -th automaton is represented by a subset $A' \subset A$ such that $a_m \in A'$, Figure 1.

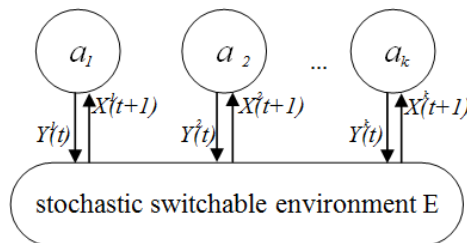


Figure 1. The structure of the DLT BC system in the form of a collective of automata

Since various operations, such as verifying transactions and blocks, have well-defined computational and time costs, and adding a new block to BC is performed at discrete intervals on average, we assume that the DLT BC system operates in discrete time $t \in N_0$.

To describe the structure of MIC achievement protocols in DLT BC systems, we decompose the algorithm into the following stages: determining the leader node that generates the next block and accepting the new block by the nodes.

At the stage of determining the leader, the "Proof-of-X" class of proof algorithms is used in MIC achievement algorithms. We formalize the protocols for determining the sequence of block formation in the form of a function $P(t_n, A)$, where t_n is the n -th time interval, A is the set of automata involved in the MIC achievement algorithm. The function $P(t_n, A)$ generates the number of the slot machine $a_m \in A$ with some probability $p_{t_n}^m$:

$$p_{t_n}^m = \frac{1}{T} * \frac{h_m}{\sum_{z=1}^{|A|} h_z} \tag{3}$$

where T is the specified delay time interval for generating blocks, determined by the security requirements of a specific implementation of the MIC algorithm, h_m is the resource capacity of the machine a_m , and $\sum_{z=1}^{|A|} h_z$ is the total resource capacity of the entire set of machines.

At the stage of acceptance of a new block by the DLT BC nodes of the system, the order of BC formation must be determined. In the course of the work, the most common protocols for its formation were considered: according to the Nakamoto MIC rule and protocols based on the rule of the "heaviest" GHOST tree. Figure 2 shows an example of determining a valid BC system by DLT BC nodes for various MIC achievement algorithms.

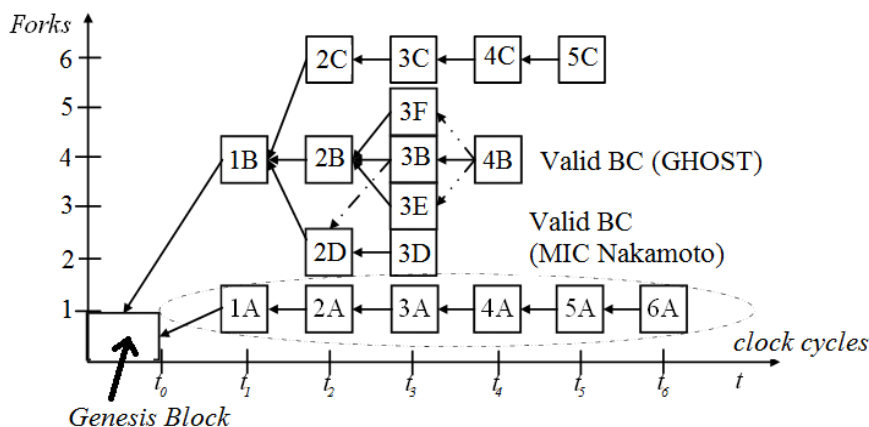


Figure 2. Determination of a valid BC system by DLT BC nodes during MIC achievement

Let's imagine the process of achieving a DLT BC MIC system by a collective game Γ of slot machines. Then the set of output signals $Y(t_n) = (Y^1(t_n), Y^2(t_n), \dots, Y^{|A|}(t_n))$ at a time t_n , where $Y^m(t_n)$ is the output signal of

the m -th node of the DLT BC system at a time t_n , let's call the game party Γ . The set of values $X(t_{n+1}) = (X^1(t_{n+1}), X^2(t_{n+1}), \dots, X^{|A|}(t_{n+1}))$ of the input variables $X^m(t_{n+1})$ at a given time t_{n+1} , assigned to classes $X(t_n)[+1]$ or $X(t_n)[-1]$, let's call the outcome of the batch $Y(t_n)$.

Let's set the game Γ with the probabilities $P(Y(t_n), X(t_{n+1}))$ of the outcome $X(t_{n+1})$ of each game $Y(t_n)$ for each machine from the set A . At the same time

$$\sum_{z=1}^{|A|} P(Y(t_n), X^z(t_{n+1})) = 1 \tag{4}$$

for anyone $Y(t_n)$. Then the probability system $P(Y(t_n), X^z(t_{n+1}))$ will set the game of $|A|$ faces.

In the course of constant adjustment to changing conditions, each m th automaton strives to increase the profitability of the MIC algorithm, i.e. it strives to obtain such sets $X(t_{n+1})$ so that the input variable $X^m(t_{n+1})$ belongs to the class $X(t_n)[+1]$ as often as possible.

Let's define the mathematical expectation $M^m(t_n)$ of obtaining sets $X(t_{n+1})$ assigned to $X(t_{n+1})$ for the m -th automaton in a batch $Y(t_n)$ and set it by the formula:

$$M^m(t_n) = \sum_{X^1(t_{n+1}), \dots, X^{m-1}(t_{n+1}), X^{m+1}(t_{n+1}), \dots, X^{|A|}(t_{n+1})} [P(Y(t_n), X^1(t_{n+1}), \dots, X^{m-1}(t_{n+1}), +1, X^{m+1}(t_{n+1}), \dots, X^{|A|}(t_{n+1})) - X^1(t_{n+1}), \dots, X^{m-1}(t_{n+1}), -1, X^{m+1}(t_{n+1}), \dots, X^{|A|}(t_{n+1}))] \tag{5}$$

The desire to increase the profitability of the MIC algorithm by each individual node of the DLT BC system leads to the appearance of the effect of groups (joint behaviour) through structural and parametric modifications, such as combining several nodes into groups (pool). This approach leads to centralization and an increase in the share of generated blocks by a certain group of nodes, which increases the likelihood of individual nodes or their groups performing abnormal functions and negatively affects the stability of the entire system. Figure 3 shows the structure of the DLT BC system, which takes into account the possibility of combining individual nodes into groups through an information exchange mechanism.

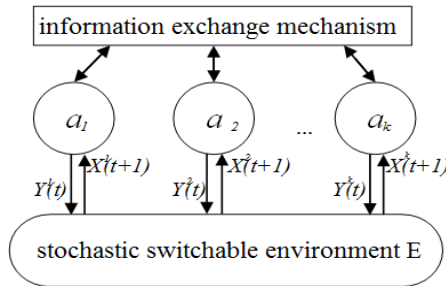


Figure 3. The structure of the DLT BC system in the form of a collective of automata with the possibility of grouping

To assess the centralization of the system, we introduce the indicator w , which reflects the ratio of the maximum value of resource capacities h_z concentrated in one group (pool) or DLT BC node of the system to the total value of the resource capacity of the entire system $\sum_{z=1}^M h_z$, where M is the number of groups and individual nodes in the system: $W = \frac{\text{Max}(h_z)}{\sum_{z=1}^M h_z}$. The probability of the formation of an alternative BC as a

result of the implementation of one or more variants of the node's abnormal functioning strategy increases with increasing centralization of the system.

6. CONCLUSION

The rules of block chain formation in algorithms for achieving mutual information coordination are proposed.

The process of achieving mutual information coordination is described.

A mathematical model of the process of achieving mutual information coordination between the nodes of the DLT BC system is proposed, which differs in the representation of the system by a team of finite automata with the possibility of creating associations (pools) and providing an assessment of the centralization of the system in the conditions of choosing different variants of behaviour strategy by automata.

REFERENCES

- [1] Kravets O. Ja. et al. Automata model of a system with distributed ledger technology based on a blockchain. *International Journal on Information Technologies and Security*, vol. 17, no. 4, 2025, pp. 79-86.
- [2] Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System, 2008. <https://nakamotoinstitute.org/library/bitcoin/>.
- [3] Rosenfeld, M. Analysis of hashrate-based double-spending. <https://arxiv.org/abs/1402.2009>.
- [4] Sompolinsky, Y., Zohar, A. Secure high-rate transaction processing in bitcoin. *Lecture Notes in Computer Science*, vol 8975, 2015. https://doi.org/10.1007/978-3-662-47854-7_32.
- [5] Bartoletti, M., Galletta, L., Murgia, M. A true concurrent model of smart contracts executions. <https://arxiv.org/abs/1905.04366>.
- [6] Zhu H. et al. Is stubborn mining severe in imperfect GHOST bitcoin-like blockchains? Quantitative analysis. *IEEE Transactions on Services Computing*, vol. 99, 2024, pp. 1-14. DOI: 10.1109/TSC.2024.3428329.
- [7] Georgiades, Y. et al. Majority is not required: A rational analysis of the private double-spend attack from a sub-majority adversary. *Distributed Ledger Technologies: Research and Practice*, 2025. DOI: 10.1145/3722126.

- [8] Hashemi S.M., Botez R.M., Ghazi G. Blockchain PoS and PoW consensus algorithms for airspace management application to the UAS-S4 Ehécatl. *Algorithms*, vol. 16, no. 10, 2023. Art No 472. DOI: 10.3390/a16100472.
- [9] Kim J.-Y., Lee J., Moon S.-M. Trie-Hashimoto: State Trie-based proof-of work mining for optimizing blockchain storage. *IEEE Access*, vol. 99, 2024, art. no 20241-1. DOI: 10.1109/ACCESS.2024.3360379.
- [10] Target. <https://en.bitcoin.it/wiki/Target>.

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

Boris Vitalievich Martynenkov– postgraduate student of of Voronezh State Technical University, areas of scientific research – system analysis, optimization, simulation of complex objects

Alexander Vasilyevich Tsvetkov - Dr. Sci (IT), professor of Voronezh State Technical University, areas of scientific research – system analysis, project management

Ekaterina Olegovna Puzhanova– postgraduate student of Voronezh State Technical University, areas of scientific research – system analysis, project management

Denis Igorevich Mutin – Dr. Sci (IT), professor of Moscow State University of Technology “STANKIN”, Moscow, areas of scientific research – system analysis, optimization, simulation of complex objects

Pavel Viktorovich Bespalov– 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

Manuscript received on 07 October 2025