ПРОБЛЕМИ ПРИЙНЯТТЯ РІШЕНЬ ТА УПРАВЛІННЯ В ЕКОНОМІЧНИХ, ТЕХНІЧНИХ, ЕКОЛОГІЧНИХ І СОЦІАЛЬНИХ СИСТЕМАХ

UDC 303.732.4
DOI: 10.20535/SRIT.2308-8893.2024.4.01

SYSTEMATIC STUDIES OF CRYPTOCURRENCY USAGE TOOLS FOR FINANCIAL MARKETS

V. ROMANENKO, H. KANTSEDAL

Abstract. The paper analyzes mining processes when using cryptocurrency on financial exchanges. It considers the cognitive map (CM) of the use of cryptocurrency as a complex system. It reveals all functions of mining processes when interacting with speculative instruments under conditions of uncertainties and risks. Digital modeling of impulse processes in the CM was carried out to study the dynamic properties of the free movement of the tops of the CM under random disturbances.

Keywords: cryptocurrency, cognitive map, mining, impulse processes.

INTRODUCTION

During the 1990s and 2000s, there was a need to solve the problems of verifying and signing digital documents (or transactions) in an environment with partial trust, that is, in an environment where one or more agents may not be in good faith [1]. Bitcoin was proposed to solve this problem. In work [2], attention was focused on the exchange of monetary assets, and a workable cryptocurrency prototype was also proposed. This ensured a relatively rapid spread of the idea among cryptographic enthusiasts. In four years, the popularity of the topic of Bitcoin led to a boom in articles aimed at increasing the efficiency of its support (mining) [3], as well as the appearance of a request for specific computing systems aimed only at mining.

Miners, the backbone of the cryptocurrency ecosystem, are responsible for emissioning and maintaining cryptocurrency. Their crucial task is to ensure the recording and execution of transactions by forming digital blocks in a standard chain—blockchain. This blockchain, one of the key concepts that underpin modern cryptographic systems, is a testament to the vital role of miners in the cryptocurrency world.

Mining is a popular way to earn money through cryptocurrency. The blockchain rules require the chain of blocks to be continuous, meaning breaks in the chain are not allowed, but branching is possible. This applies even to traditional cryptocurrencies when creating new ones based on old ones or temporarily until the next block is generated. In addition, blockchain requires the instant execution of events (smart contracts) included in the block. It also prohibits changes to the results and composition of actions in each block.

In a further development, cryptocurrency led to the emergence of specialized cryptocurrencies that can solve specific tasks of cloud computing and data storage. However, Bitcoin continues to occupy a dominant position among other currencies.

In works [4–7], cognitive maps of the use of cryptocurrency in financial markets were developed. These maps were designed based on causal relationships and took into account the main financial indicators of cryptocurrency circulation. However, they did not consider the role of miners as organizers and performers of cryptocurrency exchange by performing transactions outside the banking system.

STATEMENT OF THE PROBLEM

This article examines the problems of researching the processes of using cryptocurrency in financial markets as a complex system, the model of which is developed in the form of a cognitive map (CM).

The first task is devoted to analyzing the functions of mining processes, which help perform cryptocurrency exchange operations by conducting transactions in digital form outside the banking system.

The second task is to analyze the interaction of speculative instruments with the cryptocurrency market. The third task is to analyze the uncertainties and risks of using cryptocurrencies.

In the article we simulate the processes in the CM to study the dynamic properties of the CM's vertexes under random disturbances.

PECULIARITIES OF FUNCTIONING OF DIGITAL CRYPTOCURRENCY LIKE BITCOIN

The nature of using Bitcoin for exchange

The primary purpose of using Bitcoin was to transfer funds between users during trade transactions. In recent years, Bitcoin has gained mostly speculative popularity. To reveal the specifics of using Bitcoin as a means of exchange, let us consider the traditional type of money transfer via a bank (Fig. 1).

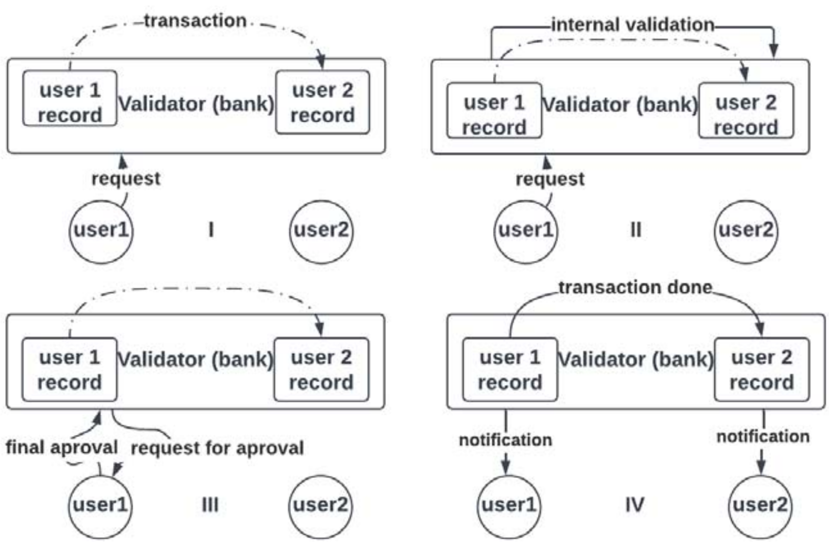

Fig. 1. The sequence of funds transfer in traditional systems is conditionally divided into four stages

There are several stages in the standard options for transferring funds:

- Authorization on the bank's server, sending a request to transfer funds.
- Internal verification of the bank (whether this transaction is possible, whether the recipient's address is valid, whether there are enough funds).
- Transaction authorization/confirmation (more a legal requirement than a necessary step).
- Physical transfer of funds (i.e., changing the balance of two users). Sending a message about a successful transaction.

The considered simple option of transferring funds between two clients of the same bank vividly illustrates the main features of the system, namely:

- The user cannot access his money and the bank's database directly.
- All operations are performed on the bank's side in its single system. The user acts as an external factor.
- The system is centralized.

This approach, of course, has its advantages, particularly for the regulation of funds; however, it also has significant disadvantages, such as limited functionality in the event of system damage (lack of Internet, light, etc.). The Bitcoin system partially solves this problem. Consider an example of Bitcoin transfer between users (Fig. 2):

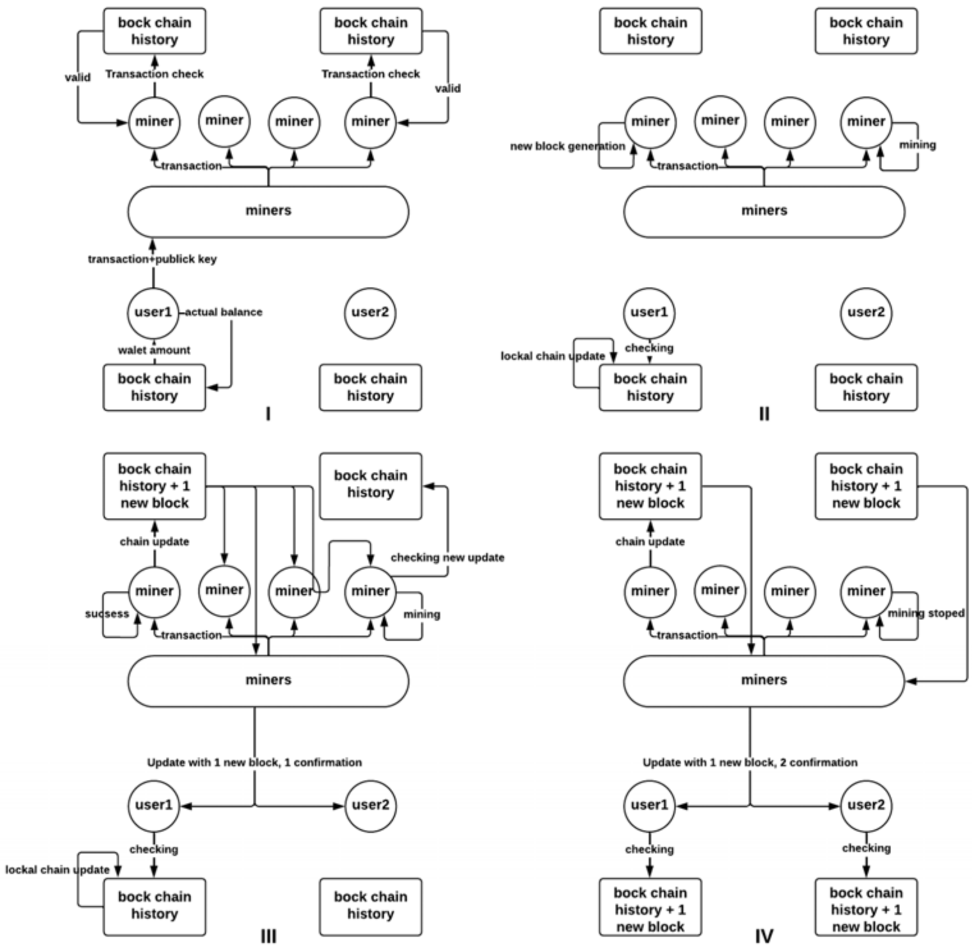

Fig. 2. The transfer of funds between two users in the Bitcoin system is conventionally divided into four sequential stages. In the figure, it is assumed that only two users are actively engaged in mining

During the transfer of bitcoins, several stages can be distinguished:

- The user checks his balance against his own copy of the blockchain (similar to a bank database). According to the verification, he requests to transfer funds to user 2. The request is coded using the user's private key and can be verified by anyone using the public key.
- The request is sent to the system and processed by one of the miners (or several). The possibility of operations is checked according to the miner's local blockchain. After verification, the operation is included in the block and the block generation process begins (that is, the selection and calculation of the hash sum that satisfies certain complexity characteristics).
- One of the miners finds the required hash sum — the new block is considered generated and is sent to other users for confirmation. The user who made the transaction receives an early warning that the transaction is already successful and agreed with one miner.
- Other crypto community users (and other miners) confirm the generation of the block (that is, it does not contradict their transaction history). This transaction is considered complete after receiving confirmation from 51% of users.

An additional requirement for users to accept the generated chain of blocks is its length. Therefore, shorter chains are rejected, and the longest chain takes priority for extension (Fig. 3).

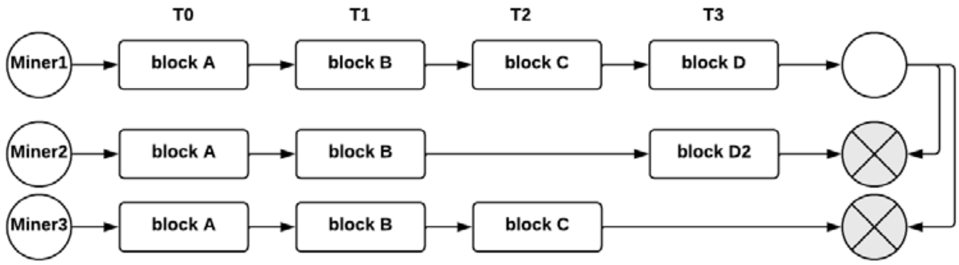

Fig. 3. Example of rejecting blocks based on chain length rule. Miner chain 1 is accepted, while chains 2 and 3 are rejected

In this system, there is no central element that can be replaced with another one. This means that changes in the miners operating the system will not be noticeable to ordinary users, and the loss of a part of the community of miners will not affect the system's operation. To ensure a smooth transition when miners' capacities change, a balancing mechanism is embedded in the blockchain. The complexity of block generation, which involves setting conditions on the selected hash sum, depends on the speed of block generation and is balanced at the level of 1 block per 10 minutes. If there is a sudden increase in the total power of the miners, the selection process may speed up. In response, the system will automatically introduce an additional complication to hash sum generation. This resistance to losing part of the mining capacity also limits the number of transactions that can be included in a block, as block sizes have physical size limits.

Anonymity in the blockchain system and benefits of use

Unlike the traditional banking system, the blockchain system does not allow for transaction cancellations or block alteration. The private key is the sole user identifier, enabling transactions from anywhere with an Internet connection. While it is possible to trace the source of funds, it is impossible to prevent their transfer.

Linking an address to a specific Bitcoin user is another concern. This problem is partly addressed through regulating cryptocurrency exchanges, which oversee real money flow and require user registration. However, a significant loophole for money laundering via cryptocurrency is the process of mining, which effectively converts electricity into cryptocurrency. This process completely anonymizes the recipient of the cryptocurrency, enabling it to be used for criminal purposes. The only way to trace the recipient of the cryptocurrency earned through mining is by locating the connection points of the mining equipment. On average, a miner can earn between $0.7 to $1.4 for every 1kWh of electricity used, depending on the exchange rate and electricity prices. This becomes incredibly profitable when access to free energy is available, such as when an enterprise or government institution covers the electricity costs. Businesses with an average power capacity of 100 kW, benefiting from discounted electricity rates, can generate up to $70.000 in monthly illegal income. This income could be undeclared or even a form of bribery.

Recent events have shown several unusual options for influencing the cryptocurrency exchange rate. Thus, countries that extract raw energy materials (gas and oil) are more prone to the mining process and, therefore, to the emission of bitcoin. As a result of the impact of the sanction, it became a source of capital outflow from the country and black purchase of goods. Bitcoin proved resistant to restrictions, but crypto exchanges, as exchangers of cryptocurrency for real money, came under restrictions and were forced to leave the market of such countries. Despite the stability of the Bitcoin system itself, such a move significantly undermined user confidence in the system. This shows that Bitcoin has not become an independent means of payment and is still perceived as a speculative asset, where the possibility of exchange for real money plays a key role.

CHARACTERISTICS OF MINING AS A DISTINCT PHENOMENON RESULTING FROM THE USE OF CRYPTOCURRENCIES

Mining is the essential link that connects the world of cryptocurrencies with the real-world environment. The concept of rewarding users for utilizing their computing power is at the core of this process. Other users repeatedly verify every action; only the result that aligns with most users (miners) is considered valid.

Initially, mining referred to creating a block in the blockchain by finding the appropriate hash and solving cryptographic tasks. Over time, the term has evolved to encompass any work for which a reward is received in the blockchain. In our context, mining encompasses any computing process that supports the operation of the blockchain system. From the network perspective, all users are integral parts of the system, acting as nodes. Mining is the only chain that connects the environment of cryptocurrencies with the real world. The idea of rewarding some users for using their computing power is fundamental. Each action is repeatedly duplicated and checked by other users. De facto, only the result that coincides with the results of most users (miners) is considered valid.

First and foremost, mining was the process of generating a block in the blockchain, that is, selecting the appropriate hash and solving cryptographic tasks. However, gradually, this term spread to any work for which a reward is received in the blockchain. In our work, mining is any computing process that supports the operation of the blockchain system. From the network point of view, all users are parts of the system — nodes:

- Full nodes are transitional nodes of the blockchain that keep and update all information about users. They require a lot of computing resources. Usually, users who hold a full node are engaged in checking transactions (keys) and the validity of blocks received from miners. Users with full nodes are rewarded for validating transactions and maintaining the network. Direct mining may also be a secondary task for such users.
- Light nodes support only partial information about the blockchain. The majority of users use them for everyday operations—checking the balance and transferring funds. The computing load is minimal, and synchronization delays can be up to several seconds.
- Pruned full nodes — differ from full nodes by the possibility of limiting support resources. Usually, only a certain limited part of the blockchain is stored — for example, the last 10 GB of transactions. Convenient for blockchain research.
- Mining nodes — the most demanding node to support. It requires different resources – from the processor and RAM to graphics processors and special-purpose integrated circuits. Users who deploy this node on their equipment receive a reward directly from the mining process — the process of generating blocks (combining transactions into a group for calculating the cryptographic component of the system — the hash). As a result of successful block generation, a reward is received. In an unsuccessful generation, the user receives nothing (Proof of Work principal).
- Master nodes — a complete analog of the full node but with additional functions — guaranteeing anonymity in the system. Unlike users with full nodes, an additional requirement for master nodes is the presence of significant capital in cryptocurrency. When conducting an anonymous transaction with another user, the capital of the master node will participate in the transaction and dilute the anonymized transaction, among others. This mechanism will make it possible to completely exclude the possibility of tracking the communication between the sender and the recipient. Of course, from the side of ordinary users, this anonymous transaction will have an increased commission, which will go to the reward of the owners of the master node. Officially, the Bitcoin system can work without master nodes, but this mechanism is easily transferred to any cryptocurrency, so it is definitely used.
- Fast nodes (Lightning Network) are nodes whose main goal is to synchronize speed among themselves. Wines act as a kindred nervous system of the blockchain, increasing bandwidth and speeding up the number of transactions in the system. The user receives a reward for transactions and the speed of their execution.

The operation of the blockchain system requires the participation of several types of users. Mining nodes form the system's foundation, but rewards are also distributed to owners of fast nodes, master nodes, and full nodes based on similar principles. Currently, the system involves over 12.000 different nodes. The exchange of information between these nodes is a hidden centralized element of the system, as connecting to nodes requires knowledge of the API address, and the system relies on resources with a list of active nodes.

Understanding the unique aspects of Bitcoin mining emission

The actual mining process simultaneously involves issuing cryptocurrency and supporting its transfers. The miner receives a reward from two sources of income:

- User commissions, a dynamic aspect of the process, are determined by the user's need to transfer Bitcoin quickly. The higher the commission, the greater the motivation of the miner to include the transaction in the block, thus increasing the priority of the transaction. The estimated minimum reward per block is 0.8 bitcoins and depends on user demand for transfers.
- An additional block reward was staked when the cryptocurrency was created. However, the reward is halved every 210.000 blocks. So, in 2032, the additional reward will be 0.78 bitcoins per block, which will be less than the user fee (Fig. 4).

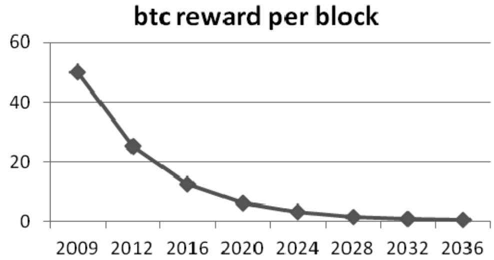

Fig. 4. Decreasing the emission (rewards for mining) of Bitcoin over time

The additional reward acts as a source of creation of new bitcoins (emission of cryptocurrency). At the same time, the commission is charged to users and is not a floating factor on the cryptocurrency rate. This means that the number of bitcoins is limited, and therefore, bitcoin is a unique resource, which gives the right to partially compare it with gold (as a limited resource of exchange). Thus, the number of bitcoins will be at most 21 million coins (Fig. 5). Therefore, considering the loss of wallets, this resource should become more and more unique over time.

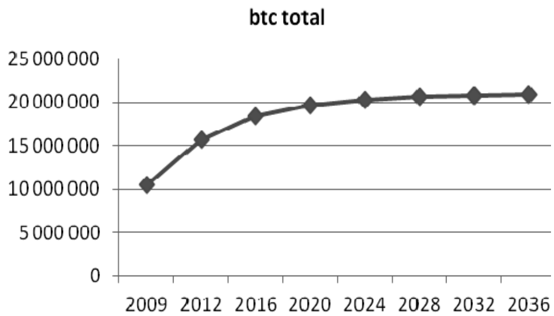

Fig. 5. The increase in the total number of bitcoins

To comprehend another mining issue, one must understand the structure of the primary mining outcome—the block (see Fig. 6).

As mentioned in 2.1, the block generation process does not depend on the number of users involved in the mining process and on their computing power. Theoretically, one user is enough for this. On the other hand, if there are several miners, only one receives a reward for mining. The computing component of mining causes this circumstance. To generate a new block, we need to include user transactions and information about the previous block and generate a hash sum that would meet some complexity rules (that is, it was less than a certain number). With the help of the complexity level, the block's birth time is regulated in 10 minutes, regardless of the computing power of the miners. In the case of low computing power, the block generation time begins to increase, which leads to the inconvenience of ordinary users and the accumulation of transactions. In this case, the condition is gradually softened.

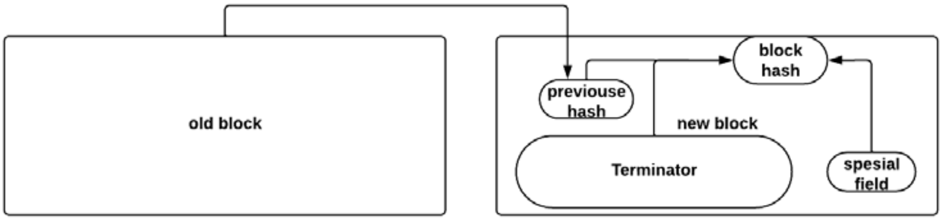

Fig. 6. A simplified Bitcoin block diagram

COGNITIVE MAP AS A MODEL FOR RESEARCHING THE USE OF CRYPTOCURRENCY

The cognitive map for researching the mining process is presented in Fig. 7. The vertices of the CM have the following names:

1. Cryptocurrency rate.
2. Number of active cryptocurrency users.
3. Number of miners.
4. Volume of processed transactions.
5. Performing miner functions.
6. Profitability of mining (profit).
7. User fees for transaction execution.
8. Issuance of cryptocurrency.
9. Amount of capitalization.
10. Indirect profit (circumvention of sanctions, economic restrictions inside of countries).
11. Funding for the development of new mining equipment.
12. Cryptocurrency supply.
13. The price of energy resources when using cryptocurrency.
14. Number of passive users (institutional investors).
15. Mining equipment price.
16. Computing complexity of the network.
17. Safety of using cryptocurrencies.
18. Legality of using cryptocurrencies.
19. Tendency to accumulate cryptocurrencies.
20. Efficiency of miners.
21. Fear of devaluation of cryptocurrency.
22. Belief in the growth of the cryptocurrency rate.
23. Informational and speculative disturbances have the following names.

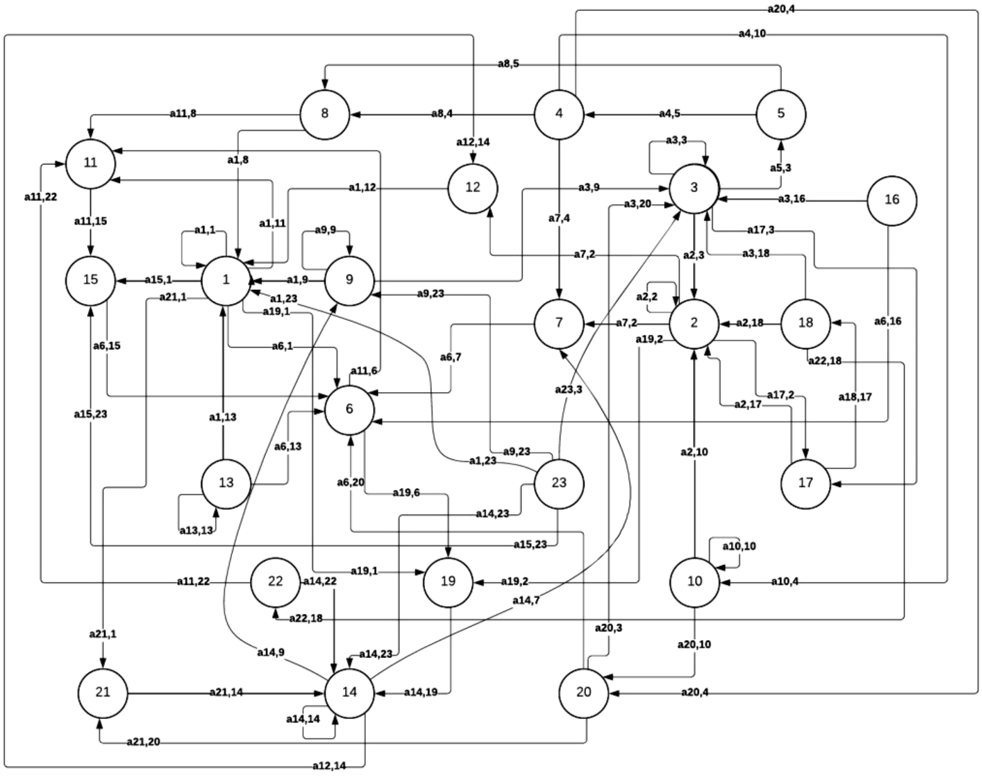

Fig. 7. Cognitive map of cryptocurrency mining

When the perturbations act on the CM vertices, a transient process occurs, which is described by the difference equation [7]:

$$\Delta y_i(k+1) = \sum_{j=1}^{n} a_{ij} \Delta y_j(k) \tag{1}$$

where $\Delta y_i(k) = y_i(k) - y_i(k-1)$, $i = 1,...,n$, a_{ij} — the weight of the edges of the weighted directed graph (CM connects the j-th vertex of the CM with the i-th one. Equation (1), which describes the free movement of the i-th coordinate of the CM, can be written in vector-matrix form for the entire CM:

$$\Delta \overline{y}_i(k+1) = A \Delta \overline{y}(k)\,, \tag{2}$$

where A is the weight matrix of the adjacency of the CM $(n \times n)$, which consists of a_{ij} CM elements.

The first 15 vertices of the CM are measurable. This means that their coordinates can be precisely measured and fixed at discrete moments of time K, starting with the period of discretization T_0.

From the 16th vertex to the 23rd, their coordinates cannot be formalized, and their change is difficult to determine on a real-time scale. To clarify this complexity, the original model of the impulse process (2) is divided into two parts. The first part is dedicated to the measured parameters of the vertices of the original CM (2), ensuring a structured approach to the research. The second part includes the non-measurable parameters of the vertices, acknowledging the inherent challenges in the field:

$$\Delta y_i(k+1) = \sum_{j=1}^{15} a_{ij} \Delta y_j(k) + \sum_{\mu=16}^{23} a_{i\mu} \Delta y_\mu(k), \qquad (3)$$

where y_j — the measured coordinates of the CM; y_μ — unmeasured coordinates of the top of the original CM.

The second model is created to describe the impulse process of the non-measurable parameters of the CM vertices:

$$\Delta y_\mu(k+1) = \sum_{j=16}^{23} a_{\mu j} \Delta y_j(k) + \sum_{j=1}^{15} a_{\mu j} \Delta y_j(k). \qquad (4)$$

At the same time, the unmeasured parameters of the vertices are considered disturbances in the first model (3).

Expressions (3) and (4), respectively, can be written in vector-matrix form:

$$\Delta \overline{Y}_1(k+1) = A_{11} \Delta \overline{Y}_1(k) + A_{12} \Delta \overline{Y}_2(k); \qquad (5)$$

$$\Delta \overline{Y}_2(k+1) = A_{21} \Delta \overline{Y}_1(k) + A_{22} \Delta \overline{Y}_2(k), \qquad (6)$$

where $\overline{Y}_1$ is a vector of measured parameters, and $\overline{Y}_2$ is a vector of non-measurable parameters, and the matrices A_{11}, A_{12}, A_{21}, A_{22} respectively have the dimension (15×15), (15×8), (8×15), (8×8) and are components of the adjacency matrix A in the model (2):

$$A = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix}. \qquad (7)$$

The use of cryptocurrencies is affected by various factors that can reduce trust in their use. As a result, the following risks can occur when dealing with cryptocurrencies:

- Risk of losing users, leading to a decrease in the price of Bitcoin
- Risks associated with incorrect general expectations of many users simultaneously, created by manipulating traders on financial exchanges.
- Risk of a sudden collapse in the cryptocurrency price due to coordinated manipulations on the stock exchanges, including high-frequency trading, where assets are bought and sold at high speeds, potentially leading to investor panic.
- Risks associated with the lack of guarantees for the safety of the capital invested in cryptocurrency, leading to user anxiety when trading on the stock exchange.

It should be noted that the combination of vertices 15-11-6 has an interesting stepped nature and behavior. The process of developing new computing schemes aimed only at solving the mining problem is quite slow and requires a lot of real money. Therefore, it constantly pulls resources away from long-term Bitcoin holders. On the other hand, when the development is completed, and the new equipment is ready for serial production, it causes a significant outflow of capital invested in Bitcoin due to the need to update mining capabilities.

Vertex 13 (the price of energy resources when using cryptocurrency) closely connects the world of miners with the real world. The mining process is extremely energy-consuming, and any fluctuations in the energy market lead to significant problems with mining. In particular, military actions near oil fields traditionally have a negative impact on cryptocurrency.

On the other hand, the presence of conflicts in other regions is a positive incentive for the growth of Bitcoin's price as a source of wealth in unstable conditions or in terms of bypassing traditional financial instruments (bypassing stations, blockades, etc.). Although mining relies increasingly on green energy, its behavior is still sensitive to daily fluctuations.

INTERACTION OF SPECULATIVE INSTRUMENTS WITH THE CRYPTOCURRENCY MARKET

Since the dawn of currency, speculation has been a fundamental part of human society. In the realm of cryptocurrencies, speculation takes on a whole new dimension. Cryptocurrencies, unlike traditional currencies, can be stored indefinitely, with the only limit being the total number of cryptocurrencies in existence. To navigate this unique landscape, many traders turn to mechanisms borrowed from the stock market, such as contracts (futures). These contracts offer the assurance of cryptocurrency redemption at any given time, a stark contrast to the typical trading of cryptocurrencies. In fact, the contract market is currently three times the trading volume of Bitcoin, making it the most popular avenue for speculation.

Contracts are divided into two types—to increase the price (long) of the asset (cryptocurrencies) and decrease it (short). To conclude a contract for an increase, it is necessary to find a counterparty for a similar contract for a price decrease. Currently, exchanges provide the opportunity to conclude contracts without being tied to a specific user and to share them between several counterparties (for ordinary users, the counterparty mechanism looks like the exchange acts as counterparty for all contracts). Thus, the mechanism of contracts on cryptocurrency exchanges is similar to the mechanism of making a bet and is a purely speculative mechanism.

The market of contracts on exchanges is divided into the following categories:

Perpetual contracts: These are derivatives that involve a commission paid depending on the duration of the contract. The commission size is directly related to the imbalance of the number of contracts on the market/exchange.

- Delivery contracts: These are futures with a fixed execution time. Until the execution time, they are similar to perpetual contracts. At the time of execution, holders of long contracts must sell the asset (cryptocurrency) for the amount specified in the contract, and holders of short contracts must buy cryptocurrency at the market price.
- Contracts for cryptocurrency in cryptocurrency: In terms of the execution mechanism, they can be similar to the first two types, but the use of only cryptocurrency expands the possibilities of contracts and allows for the addition of new conditions. These contracts can be applied in decentralized settlements.

Credit funds are widely used for all the speculative assets listed. Under very reasonable conditions, it is possible to borrow up to 124 credit dollars using just one physical dollar. The contract market is seen as a form of speculation that is a significant destabilizing factor in the financial market. Speculative assets are readily accessible and fully integrated into the basic functionality of modern exchanges. Speculation can be categorized as follows:

- Inter-exchange arbitrage involves making a profit from price differences between exchanges. This involves buying and selling assets, but it carries the risk of transferring cryptocurrency between exchanges.
- Cross-currency arbitrage is about profiting from exchange rate differences between interconnected assets. This situation arises when one asset is traded in much smaller volumes than the others, leading to delayed price quotations.
- Cross-product arbitrage is an arbitrage between different products of an exchange or exchanges. It typically involves derivatives, options, and futures.
- Trading based on graphic data analysis is risky for speculation, as it involves a desire to get rich quickly rather than long-term operations. In the short term, the behavior of the cryptocurrency exchange rate is random and has a low, but not zero, chance of success.
- High-speed trading involves short-term transactions and frequent or full automation, which reduces risks due to their short duration.
- Scraping is a speculation strategy based on a stationary cryptocurrency rate assumption. The user engages in the de facto resale of the asset with a minimal markup. This is the least risky strategy among non-arbitrage options for speculation.

On the cognitive map (Fig. 7), speculation is depicted as a disruption, which is considered at the top of 23 CM. Other speculations, in various forms, stem from the above. While most arbitrage strategies enable synchronization of different parts of the system and cryptocurrency markets, scraping introduces white noise. Trading based on graphical analysis and high-speed trading with many users is entirely random.

CHARACTERISTICS OF UNCERTAINTIES WITH CRYPTOCURRENCY USAGE

Uncertainties when using Bitcoin

One of the major issues with blockchain systems in the context of using cryptocurrencies is their reliance on users. Any action or information on the blockchain is considered valid if most users accept it. This vulnerability is exploited in what is known as a “51% attack”. In this attack, the goal is to temporarily control more than 51% of the mining capacity of the entire network. Once this control is achieved, false data can be entered into the generation of the current block and validated. The false data is considered valid because the remaining 49% of users cannot reverse this. However, it is essential to note that the current power of the Bitcoin blockchain is substantial, and the network of miners is extensive, making this type of attack unlikely, given the current number of users and the advancement of computing technology.

Another drawback is the potential for the blockchain network to become overloaded due to the volume of transactions. An attack with a high volume of transactions could potentially cripple the blockchain for some time, resulting in the isolation of cryptocurrency exchanges. In theory, this could lead to a loss of user confidence and a significant drop in the price of the cryptocurrency.

Uncertainties inherent in the characteristics of Bitcoin as a digital currency

One of the significant issues with cryptocurrencies today is their reliance on the Proof of Work (PoW) algorithm to a certain extent. The global economy heavily depends on digital signature technology, with most digital signatures being created using a few simple numbers. This uneven distribution of operations reduces cryptographic stability and poses a potential challenge to economic activities in the next 50 years, not just for Bitcoin.

Another concern is the need for more decentralization and the need to store node addresses. In the event of a 51% attack on Bitcoin services, control over approximately 8.000 nodes could allow fake transactions to be introduced into the system. If most users are successfully redirected to fake nodes within 10 minutes, significant damage could be done to the system.

Additionally, the implementation of the Proof of Work protocol in mining, where the mining reward goes to only one successful miner, has led to the unification of miners in mining pools. While this makes the mining process more predictable, it makes the system less resistant to a 51% attack.

A more immediate challenge for Bitcoin is the issue of limiting both the number of coins and the number of transactions per second. As the world evolves, it's increasingly likely that cryptocurrency may no longer be a convenient medium of exchange due to its price or exchange speed. This could lead to a collapse of the industry in the future.

Furthermore, future mining limitations may lead to a significant amount of equipment being released on the market, which could be used for fraudulent actions with cryptocurrency. The same equipment used for mining can also be used to hack wallets successfully. Considering the dormant wallets with significant funds stored since the beginning of the cryptocurrency era, this may lead to a collapse of the cryptocurrency rate as early as 2040.

Uncertainties arise from speculative phenomena in the cryptocurrency market

Speculation and leverage pose potential problems for cryptocurrency markets. The most significant issue is the synchronization of speculators' actions at certain times, leading to significant market fluctuations. This is further exacerbated by the introduction of copy trading, which enables traders to share strategies with others at the exchange level, making synchronization even easier.

Another risk is the accumulation of substantial finances in speculative assets, potentially leading to a stock market crash. Currently, there is no legal regulation of cryptocurrency exchanges, and tracking the amount of collateral on the exchanges is challenging. Additionally, part of the collateral is always in cryptocurrency, the exchange rate of which can fluctuate significantly, especially when funds need to be transferred through the exchange into real money. These transaction volumes can significantly impact the cryptocurrency market and the pricing mechanism for cryptocurrency.

MODELING OF IMPULSE PROCESSES OF THE COORDINATES OF THE CM VERTICES OF THE USE OF CRYPTOCURRENCY

Based on cause-and-effect relationships, the adjacency matrix A of the impulse process of the cognitive map (7) was developed, which has the following components A_{11}, A_{12}, A_{21}, A_{22}:

$$A_{11} = \begin{bmatrix} 0.4 & 0 & 0 & 0 & 0 & 0 & 0 & -0.4 & 0.15 & 0 & 0 & 0.2 & -0.25 & 0 & 0 \\ 0 & 0.3 & 0.15 & 0 & 0 & 0 & 0 & 0 & 0 & 0.1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0.4 & 0 & 0 & 0 & 0 & 0 & 0.3 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0.3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0.7 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0.3 & 0 & 0 & 0 & 0 & 0 & 0.6 & 0.4 & 0 & 0 & 0 & 0 & -0.4 & 0 & -0.3 \\ 0 & 0.5 & 0 & 0.3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -0.5 & 0 \\ 0 & 0 & 0 & 0.25 & 0.3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.8 & 0 & 0 & 0 & 0 & 0.7 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.7 & 0 & 0 & 0 & 0 & 0 \\ 0.7 & 0 & 0 & 0 & 0 & 0.4 & 0 & 0.3 & 0 & 0 & 0 & 0.2 & 0 & 0 & 0 \\ 0 & 0.6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.8 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.8 & 0 \\ 0.5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.4 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$A_{12} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & -0.7 \\ 0 & 0.5 & 0.2 & 0 & 0 & 0 & 0 & -0.3 \\ -0.2 & 0 & 0.15 & 0 & 0.15 & 0 & 0 & -0.2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -0.2 & 0 & 0 & 0 & 0.3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -0.2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0.4 & 0 & -0.3 & 0.15 & -0.25 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.3 \end{bmatrix}$$

$$A_{21} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -0.1 & 0.2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -0.2 & 0 & 0 & 0 & 0 & 0 \\ 0.3 & 0.1 & 0 & 0 & 0 & 0.2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0.5 & 0 & 0 & 0 & 0 & 0 & 0.3 & 0 & 0 & -0.15 & 0 & 0 \\ -0.1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$A_{22} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0.4 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0.3 & 0 \\ 0 & 0 & 0 & 0 & -0.15 & 0 & 0 & 0 \\ 0 & 0 & 0.3 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

The eigenvalues of the matrix A are $0.989+0i$, $0.592+0.282i$, $0.489+0i$, $0.22+0.333i$, $0.22-0.333i$, $0.08+0.336i$, $-0.334+0i$, $-0.188+0.13i$, $-0.188-0.13i$, $0.142+0i$, $0.064+0.102i$, $0.064-0.102i$, $-0.122+0i$, $0i$, $0i$, $0i$, $0i$, $0.7+0i$, $0.8+0i$, $0i$, $0i$. The eigenvalues of the matrix are smaller than one by module. Therefore, the impulse responses of the closed-loop control for models (5) and (6) are stable.

Modeling the impulse processes of the coordinates of the CM vertices is carried out to examine the movement of critical vertices 1, 2, 3, 6, and 20 under the influence of random disturbances applied to vertices 18, 22, and 23.

Figs. 8–12 display graphs of the CM coordinates' free movement, including the cryptocurrency exchange rate, the number of active cryptocurrency users, the amount of mining, and the efficiency of miners.

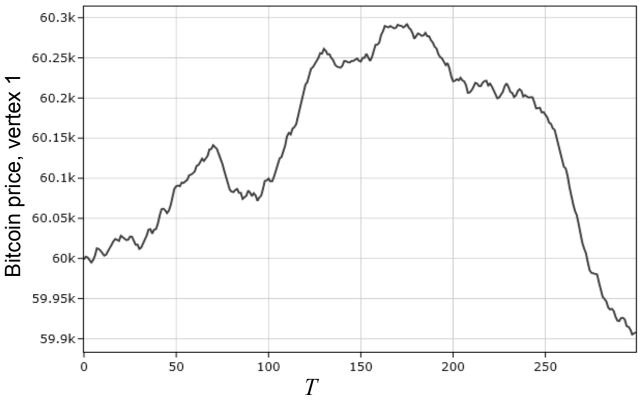

Fig. 8. Free movement of the exchange rate of cryptocurrencies (vertex 1)

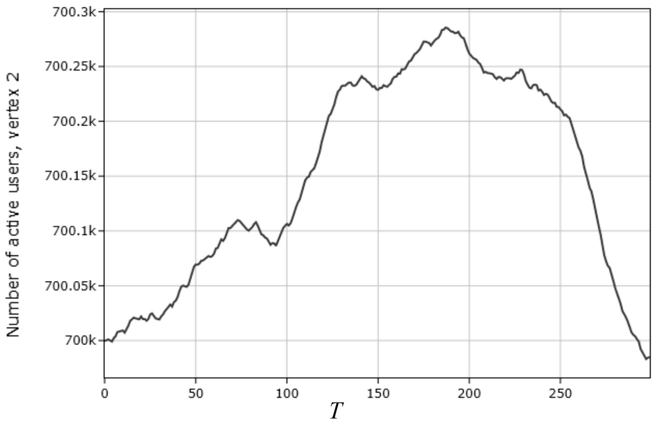

Fig. 9. Free movement of the number of active users (vertex 2)

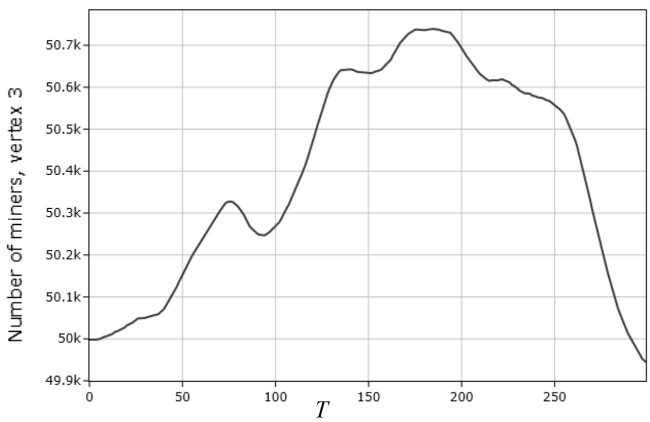

Fig. 10. Free movement of the number of miners (vertex 3)

Fig. 11. Free fluctuations of mining profitability (vertex 6)

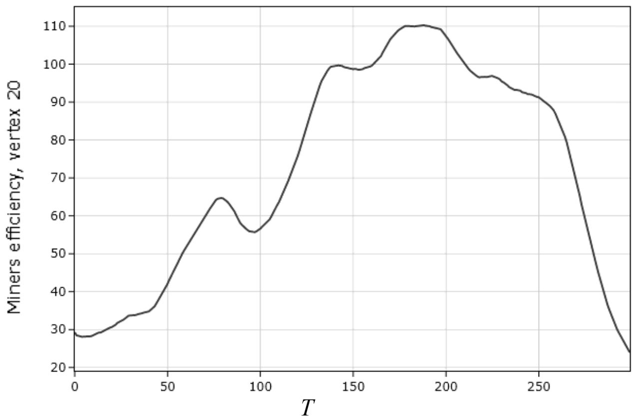

Fig. 12. Free fluctuations of mining efficiency (vertex 20)

For a clearer simulation, initial values of 60000, 700000, 50000, 3000, and 30 were set as the system's starting point for vertices 1, 2, 3, 6, and 20. The most significant changes affected the profitability of mining and cryptocurrency's rate while other changes occurred gradually and were highly correlated. There patterns closely mirror real marked behavior. Specifically, as the number of diskettes increases, the behavior of the cryptocurrency exchange rate closely resembles that of the real market (Fig. 13)

Fig. 13. The behavior of the cryptocurrency exchange rate over an extended period

Therefore, these graphs comprehensively describe the dynamic properties of the cryptocurrency circulation's CM. The model built reflects the primary interactions of cryptocurrencies in financial markets and corresponds to the simulated phenomenon.

CONCLUSION

The work performs a systematic study of the dynamic properties of mining principles when using cryptocurrency on financial exchanges, which are used to perform cryptocurrency exchange operations by conducting transactions in digital form outside the banking system. For this, a cognitive map of the use of cryptocurrency as a complex system was developed, in which all the functions of mining processes in interaction with speculative instruments in conditions of uncertainties and risks are revealed.

In the article, the digital simulation of impulse processes in the CM was carried out while investigating the dynamic properties of the free movement of the tops of the CM under the action of random disturbances.

REFERENCES

1. H. Massias, X. Serret Avila, and Quisquater Jean-Jacques, "Design Of A Secure Timestamping Service With Minimal Trust Requirement," in *20th Symposium on Information Theory in the Benelux, Citeseer, May, 1999*.
2. Satoshi Nakamoto, *Bitcoin: A peer-to-peer electronic cash system*. 2008. Accessed on: May 2, 2024. [Online]. Available: https://git.dhimmel.com/bitcoin-whitepaper/
3. Meni Rosenfeld, "Analysis of bitcoin pooled mining reward systems," *arXiv preprint, arXiv:1112.4980.* 2011. doi: https://doi.org/10.48550/arXiv.1112.4980
4. V. Romanenko, Yu. Miliavskyi, and G. Kantsedal, "An adaptive system for stabilizing unstable cryptocurrency rate based on a cognitive map impulse process model," *International Scientific Technical Journal "Problems of Control and Informatics,"* 66(2), pp. 11–23. doi: 10.34229/1028-0979-2021-2-2
5. V. Romanenko, Y. Miliavskyi, and H. Kantsedal, "Application of Impulse Process Models with Multirate Sampling in Cognitive Maps of Cryptocurrency for Dynamic Decision Making," in M. Zgurovsky and N. Pankratova (eds.) *System Analysis & Intelligent Computing: Theory and Applications*. Springer International Publishing, Cham, 2022, pp. 115–137. doi: https://doi.org/10.1007/978-3-030-94910-5_7
6. V. Romanenko, Y. Miliavskyi, and H. Kantsedal, "Stabilization of Impulse Processes of the Cognitive Map of Cryptocurrency Usage with Multirate Sampling and Coordination Between Some Nodes Parameters," in M. Zgurovsky, N. Pankratova (eds) *System Analysis and Artificial Intelligence. Studies in Computational Intelligence*, vol. 1107. Springer, Cham, 2023, pp. 83–100. doi: https://doi.org/10.1007/978-3-031-37450-0_5
7. V. Romanenko, Y. Miliavskyi, and H. Kantsedal, "Automated Control Problems for Dynamic Processes Applied to Cryptocurrency in Finansial Markets," in Y. Kondratenko, V. Kuntsevich, A.Chikrii, Y. Gubarev (eds.) *Recent Developments in Automatic Control Systems*. River Publishers, 2022, pp. 417–442. doi: 10.13140/RG.2.2.24246.42561/1
8. G. Ebrahimpour, M. Sayad Haghighi, "Is Bitcoin Future as Secure as We Think? Analysis of Bitcoin Vulnerability to Bribery Attacks Launched through Large Transactions," *ACM Trans. Priv. Secur.*, vol. 27, issue 2, Article 14, May 2024, 22 p. doi: https://doi.org/10.1145/3641546

Received 10.05.2024

INFORMATION ON THE ARTICLE

Viktor D. Romanenko, ORCID: 0000-0002-6222-3336, Educational and Research Institute for Applied System Analysis of the National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Ukraine, e-mail: romanenko.viktorroman@gmail.com

Heorhii O. Kantsedal, ORCID: 0000-0003-2740-2176, Educational and Research Institute for Applied System Analysis of the National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Ukraine, e-mail: g.kantsedal@protonmail.com

СИСТЕМАТИЧНІ ДОСЛІДЖЕННЯ ІНСТРУМЕНТІВ ВИКОРИСТАННЯ КРИПТОВАЛЮТИ НА ФІНАНСОВИХ РИНКАХ / В.Д. Романенко, Г.О. Канцедал

Анотація. Проаналізовано процеси майнінгу за використання криптовалюти на фінансових біржах. Розглянуто когнітивну карту (КК) використання криптовалюти як складної системи. Розкрито всі функції процесів майнінгу у ході взаємодії зі спекулятивними інструментами в умовах невизначеності та ризиків. Для дослідження динамічних властивостей вільного руху вершин КК під дією випадкових збурень виконано цифрове моделювання імпульсних процесів у КК.

Ключові слова: криптовалюта, когнітивна карта, майнінг, імпульсні процеси.