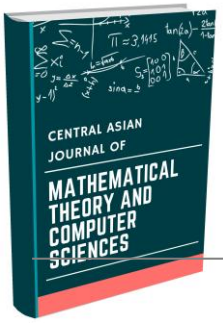

CENTRAL ASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES

https://cajmtcs.centralasianstudies.org

Volume: 03 Issue: 12 | Dec 2022 ISSN: 2660-5309

SYSTEMATIC ANALYSIS OF BLOCKCHAIN DATA STORAGE AND SHARING TECHNOLOGY

Anvar Kabulov, Inomjon Yarashov, Baxodir Daniyarov

National university of Uzbekistan named after Mirzo Ulugbek

Abstract

This article deals with a systematic analysis of blockchain technology and its application in the modern environment. The main focus is on the problems associated with distributed blockchain technology. Areas of application of technology are indicated in this article. Mathematical models and implementation algorithms of blockchain components are considered. A systematic analysis of the contradictions of blockchain technology is carried out with a brief analysis of the internal logic (coding and consensus). This work shows the prospects for the development of blockchain services based on the concept of "smart contract", which allows transactions between participants in an automatic mode, which allows the creation of decentralized, independent organizational units.

These units follow their own laws and operate almost independently, implementing decentralized programs. Decentralized applications are more flexible, transparent, and secure than modern software built using traditional models. As shown, using the features of "peer-to-peer" (P2P) networks with the equality of all participants, blockchain technologies allow direct transactions with any participant of this network. It creates a processing core of "decentralized independent organizations" that should be considered as a new type of organization similar to the digital company. Blockchain-based decisions create a secure and inherently decentralized framework for processing transactions. The main advantage of the blockchain compared to other models of databases is the algorithmic implementation of management using a single protocol. In conclusion, recommendations are given for the use of the technology of maintaining a single data register in the conditions of synchronous technologies of data processing and management.

ARTICLEINFO

Article history:
Received 23 Oct 2022
Revised form 24 Nov 2022
Accepted 26 Dec 2022

Keywords: *blockchain, problems, areas of application, consensus, synchronous data processing technologies.*

Introduction

At present, issues of system reliability are becoming more and more important; this creates new requirements for data processing and storage technologies. Analysis of blockchain technology (blockchain or block chain - a chain of transaction blocks) is a chain built from the created transaction blocks according to certain rules and is aimed at ensuring the mutual cooperation of a large number of users without using "trusted intermediaries" [1-6].

For the reliability of data storage, the blockchain has to pay with speed. For example, in the bitcoin system [7-11], the time required adding one block is about 10 minutes, which is due to the decentralization of the system; information about a new transaction must be distributed to about 80% of the network. In addition to speed, there is also a question of data storage: with each user storing more than 80 GB of memory and with more than 16 million users, the total storage capacity is more than 1.3 exabytes! From this we can conclude about the scale problems of blockchain technologies.

Blockchain originates from peer-to-peer networks, to which Bran Cohen later added distributed hash tables, thus implementing BitTorrent. Taking advantage of BitTorrent's achievements and solving the problem of decentralized consensus, Bitcoin created the first blockchain. For the first time, this term appeared as the name of a distributed database implemented in the bitcoin cryptocurrency. The next step should be considered Ethereum, which created a platform for developing decentralized applications by adding smart contracts to the blockchain system. It is also worth noting Hyperledger, which implemented a modular structure that simplifies integration with existing systems [12-17]. High-level protocols are based on the concept of a "smart contract" - an electronic algorithm that describes a set of conditions necessary for the execution of a transaction stored in network nodes.

Transaction refers to actions of system[18-22] participants related to interaction with data. When a transaction is made, it must be recorded on the blockchain, for which transactions are placed in blocks. But adding a new block to the blockchain requires permission from other network participants. The algorithm for obtaining this permission is called "consensus".

Blockchain technologies are promising for the implementation of corporate information systems, because today the back office is dominated by highly complex, confusing and opaque isolated internal business processes. It can be said that blockchain technologies are in demand in the modern world due to the many interactions of data sharing and storage [4-6]. The main problem is that each market, each organization has its own data register.

The following problems can be identified when using multiple registers:

- each party is forced to keep its own data register;
- inconsistency and data errors and, as a result, no less complex reconciliation operations;
- lack of standardization;

Blockchain technologies include:

- ✓ one common trusted register;
- ✓ central counterparty;
- ✓ elimination of distrust of counterparties.

Elimination of distrust occurs due to the impossibility of changing or deleting already added data and a distributed algorithm for adding new information. In addition, there is a reduction in costs, both time and money.

Due to the fact that the blockchain makes business processes transparent and protects information more reliably than any technology that has been used before, the blockchain finds a lot of applications for itself:

- digital corporate system;

- digital notary;
- trading platform without intermediaries;
- systems of interbank payments;
- electronic voting - e-voting.

Based on the foregoing, it can be assumed that the main attention in the future will be concentrated on:

- ✓ on pilot and other projects using blockchain - FireChat, PopcornTime, Lighthouse, Gems, CanadaCoin;
- ✓ research on decentralized consensus algorithms
- ✓ development of various application platforms: Bitcoin, Ethereum, Eris, Ripple, Dogecoin, Hyperledger, etc.;
- ✓ further unification and standardization of the blockchain;
- ✓ development of effective mechanisms for converting physical things into the digital world.

As part of this work, an attempt was made to systematize the basic provisions of the blockchain technology, which will make it possible to formulate specific practical recommendations for the implementation and maintenance of a unified data registry in the context of synchronous technologies for information support of product life cycle processes.

Systematic analysis of blockchain technology

Blockchain, like any "young" technology, is characterized by a number of tasks that need to be solved for full-scale implementation.

Consider the problem of decentralized data storage (Fig. 1). If a complete data register is stored in each network node, then it will be possible to restore the network up to the moment of destruction of the last network node, but the retribution for this is just as great - the network is constantly growing in the process of operation, which in the future will lead to uncontrolled volumes of data. Plus, to enter the network of a new participant, he will have to synchronize (download) a huge amount of data [11].

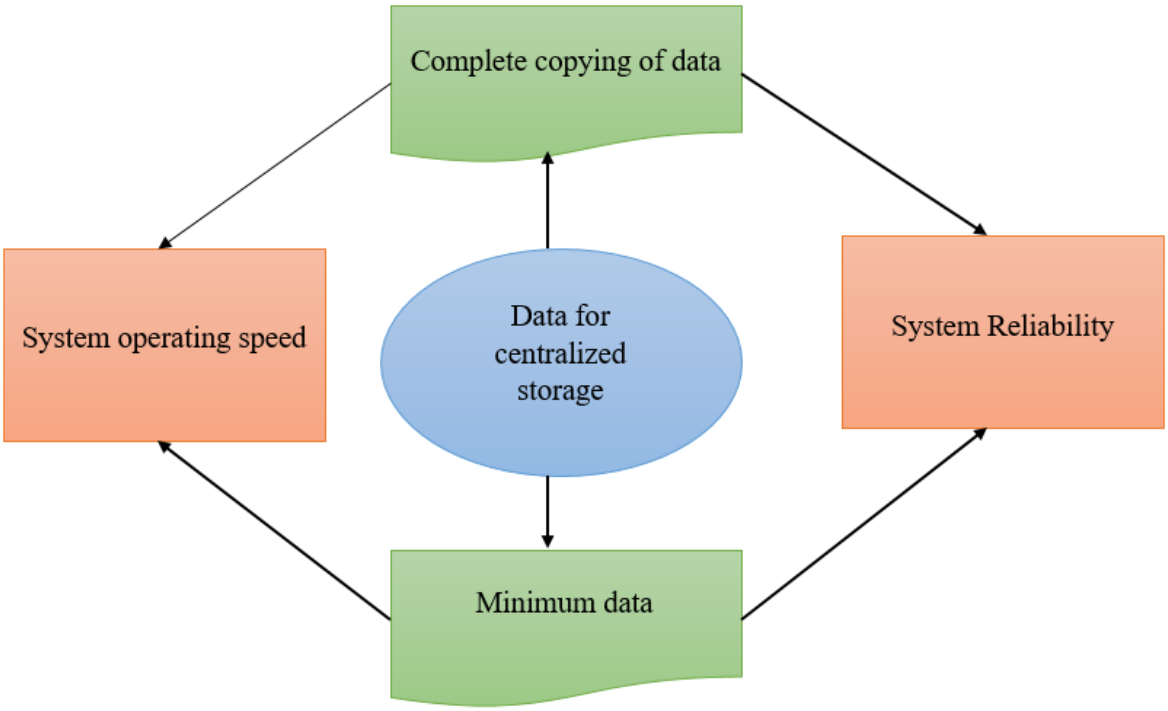

Fig 1. Map of contradictions for decentralized data storage

Alternatively, to solve this problem, it is possible to propose using a standard database in which real data is stored in encrypted form, and only their hash is entered into the blockchain and old blocks are archived. Although this is more of a delay than a solution to the problem. It may seem that to solve these problems it is possible to use methods from technologies such as Big Data [12]. It is also focused on working with large amounts of data storage and processing; various architectures have already been worked out - Map Reduce, Shared Memory, Shared Nothing, Shared Disk and others. The main obstacle to the integration of Big Data tools into the blockchain is the type of system: the blockchain is a decentralized, distributed system, which means that the calculations are distributed among several nodes and there are no nodes that control the work of other network nodes. But integration is also possible in the other direction: after all, technically, blockchain is a simple database with terrible scalability and lack of query languages, but decentralization, immutability, transparency and the possibility of universal data exchange more than compensate for its shortcomings. And BigchainDB and IPDB are currently being developed, which can become planetary-scale databases with decentralized management.

Another important task is to ensure trust in the system, i.e. the system must be both anonymous and transparent for its participants (Fig. 2).

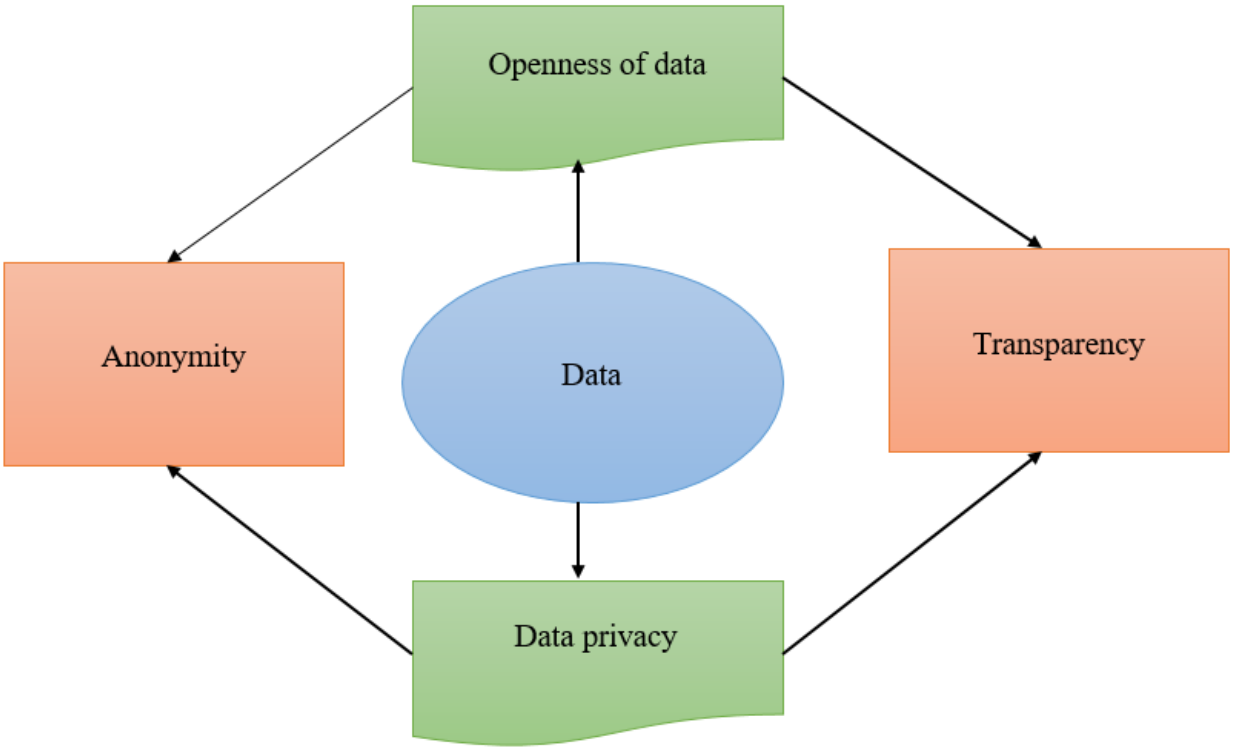

Fig 2. Contradiction map for system trust

Users want to see the movement of data on the network without other users knowing what they are doing. For this, it was decided to apply asymmetric encryption algorithms [9] - thus, each user has a pair of keys: private and public (Fig. 3).

Fig 3. Relationship of user data

The private key is used to sign blocks sent by the user. The user's address on the network is displayed using a public key.

Analysis and classification of application fields

The main areas of application of blockchain technology are shown in Figure 4.

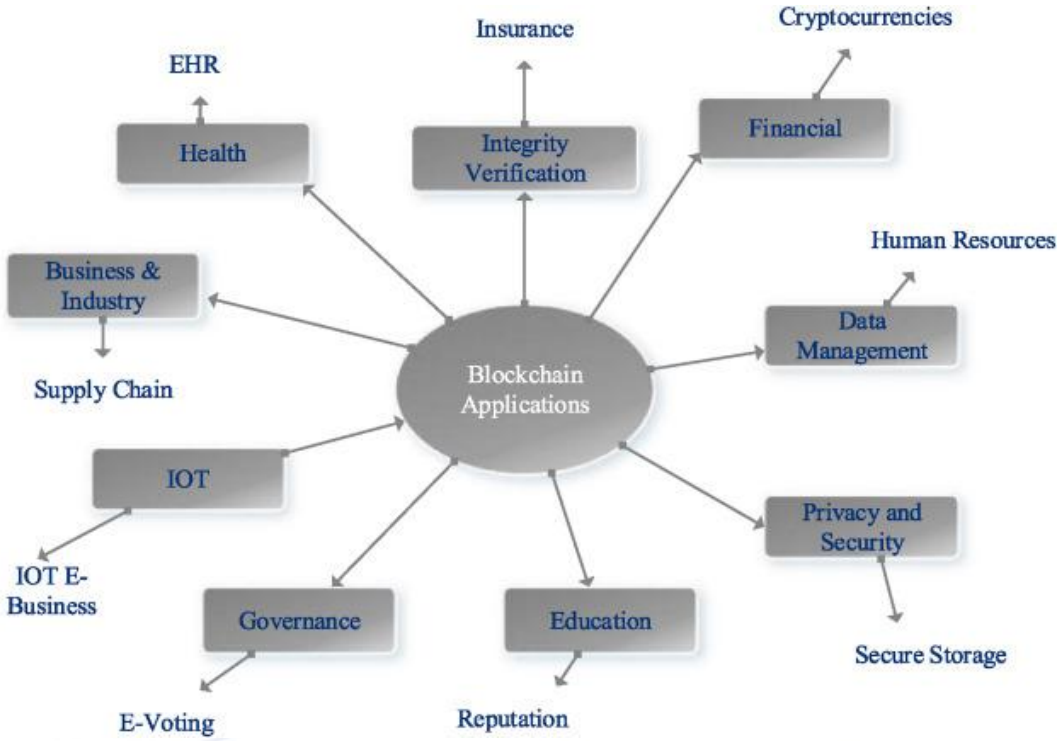

Fig 4. Classification of regional applications of blockchain technology

For example, credential management was implemented in notarial projects. In such applications, it allows the user to introduce himself in front of the controller through a photo or video. This file is added to the blockchain where it can no longer be modified or overwritten.

You can consider the implementation of blockchain-based markets using the example of OpenBazaar. OpenBazaar has no central server to answer everything. OpenBazaar is a peer-to-peer client that cannot be restricted by any government. OpenBazaar does not require legal permission to operate, reflecting the evolution of an unrestricted global marketplace. OpenBazaar allows sellers and buyers to interact to buy and sell goods without third parties and therefore without commission.

Among the interbank payment systems, one can note the system based on the Ripple protocol. The pilot program uses the RC Cloud cloud payment platform, which allows you to make local and international money transfers almost instantly and at a lower cost than traditional solutions. An example is the project of electronic voting from social networks - electronic voting. The main task is to protect the voice of the voter/shareholder. Blockchain as a voting platform provides all the requirements:

- ✓ error tolerance;
- ✓ each sound can be tracked according to its source;
- ✓ you cannot restrict access to the system;
- ✓ anonymity of the voter;
- ✓ the ability to check the results for each.

A logical model analysis of the "reliability" of blockchain technology

One of the main problems of the blockchain is the reliability of data, which determines the need for efficient encryption algorithms. It must guarantee sufficient cryptographic strength of information in the network, as well as provide the possibility of implementing a digital signature. Consider the RSA asymmetric encryption algorithm. First, two primes p and q are chosen. Next come the modules for the public and private keys (1) and the Euler function of the module (2):

$$n = p * q \ (1)$$

$$\varphi(n) = (p-1) * (q-1) \ (2)$$

After that, an integer e (open exponent) from 1 to $\varphi(n)$, coprime to $\varphi(n)$, is chosen. Usually, e is taken as prime numbers containing a small number of 1 bits in binary notation, but not too small for quick exponentiation.

Next is the number d corresponding to formula (3):

$$d * e \ mod \ \varphi(n) = 1 \ (3)$$

Thus, a private key {d, n} and a public key {e, n} are formed, which are used to encrypt (4) and decrypt (5) data.

$$c = m^e \ mod \ n \ (4)$$

$$m = c^d \ mod \ n \ (5)$$

where $m < n, c$ - encrypted data, m - unencrypted data, $mod \ \varphi(n)$ - range of values (the more, the better).

When you try to crack (pick up) the private key, you will have to go through 2^N combinations, where N is the length of the key. For example, with a key length of 256 bits and a password guessing rate of 1024 per second, it will take 1.23e + 67 years, which is a very, very long time, and the information will no longer be relevant by that time.

More advanced algorithms are also used, such as the Elliptic Curve Digital Signature Algorithm (ECDSA), which work in a similar way, but have their own subtleties.

Equally important is the question of special algorithms for concurrent access and collision resolution in the network.

Below are some of them:

- PBFT - a request to add a block is sent to all participants, and everyone calculates the hash of the next block, after which they send their decision to the rest of the participants, as a result, each participant receives an array of responses and accepts an answer with a total number of more than 50% as reliable, the disadvantage is that the transaction execution time increases depending on the size of the network;
- PoW - network nodes (miners) solve the problem of calculating the hash of the next block with a certain condition, and whoever calculates the hash faster, that block will be the next one. Cons - energy consumption due to the complexity of calculations and the presence of some centralization - miners;
- PoS - an alternative to PoW, does not require large computing power: network participants have an intra-system currency, and whoever is richer has priority for block formation, disadvantages - lack of randomness;
- Proof of some limited resource (Burn, Space, Bandwidth) - are varieties of PoW and PoS.

Concept of introduction of blockchain technologies in remote identification systems

It implements a closed network without cryptocurrency, supports the use of smart contracts and roles for participants, has a wide SDK, as well as a modular structure that allows you to replace each module of the system, thus allowing you to reuse the company's previous work. The generalized algorithm of the system

operation can be presented in the following sequence: 1. The user comes to one of the organizations that is part of the blockchain network consortium and goes through the authentication procedure. 2. Further, his data is entered into the database, and the user receives an electronic key from his record. 3. The user logs in to the network and generates a request for data processing, the controller requires identification data that the user has already left in the network. 4. The user enters his electronic key and marks the attributes of his record, which must be provided to the regulator. Thus, it is possible to carry out remote identification by means of an electronic key.

By implementing a closed network, where a group of developers, a project manager, a contractor, etc. will be located, blockchain technology ensures that a transaction is registered only at legally defined moments when performing work. Before this, the actions must be approved by the project manager and other developers, only after which the next transaction will be initialized. Thus, the interested parties receive a clear and evenly distributed incentive to register these facts along the chain: or you will not receive the resources that you ordered.

By implementing a closed network, where a group of developers, a project manager, a contractor, etc. will be located, blockchain technology ensures that a transaction is registered only at legally defined moments when performing work. Before this, the actions must be approved by the project manager and other developers, only after which the next transaction will be initialized. Thus, the interested parties receive a clear and evenly distributed incentive to register these facts along the chain: or you will not receive the resources that you ordered.

Conclusion

With a brief analysis of the internal logic (coding and consensus), a systematic analysis of the contradictions of blockchain technology is carried out. Decentralized applications are more flexible, transparent and secure than modern applications built according to traditional models. Using the features of "peer-to-peer" (P2P) networks with the equality of all participants, blockchain technologies allow direct transactions with any participant of this network. Blockchain-based decisions create a secure and unique decentralized framework for processing transactions. The main advantage of blockchain compared to other database models is the algorithmic implementation of management with a single protocol. The basic purpose is on the issue of distributed blockchain technology and areas of application of technology are indicated. In conclusion, in the conditions of synchronous technologies of data processing and management, recommendations are given on the use of the technology of maintaining a single register of data.

Reference

1. A. Kabulov, I. Kalandarov and I. Yarashov, "Problems Of Algorithmization Of Control Of Complex Systems Based On Functioning Tables In Dynamic Control Systems," 2021 International Conference on Information Science and Communications Technologies (ICISCT), 2021, pp. 1-4, doi: 10.1109/ICISCT52966.2021.9670017.
2. A. Kabulov and I. Yarashov, "Mathematical model of Information Processing in the Ecological Monitoring Information System," 2021 International Conference on Information Science and Communications Technologies (ICISCT), 2021, pp. 1-4, doi: 10.1109/ICISCT52966.2021.9670192.
3. A. Kabulov, I. Yarashov and A. Otakhonov, "Algorithmic Analysis of the System Based on the Functioning Table and Information Security," 2022 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), 2022, pp. 1-5, doi: 10.1109/IEMTRONICS55184.2022.9795746.
4. A. Kabulov, I. Saymanov, I. Yarashov and F. Muxammadiev, "Algorithmic method of security of the Internet of Things based on steganographic coding," 2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), 2021, pp. 1-5, doi: 10.1109/IEMTRONICS52119.2021.9422588.

5. I. Yarashov, "Algorithmic Formalization Of User Access To The Ecological Monitoring Information System," 2021 International Conference on Information Science and Communications Technologies (ICISCT), 2021, pp. 1-3, doi: 10.1109/ICISCT52966.2021.9670023.
6. A. Kabulov, I. Normatov, I. Kalandarov and I. Yarashov, "Development of An Algorithmic Model And Methods For Managing Production Systems Based On Algebra Over Functioning Tables," 2021 International Conference on Information Science and Communications Technologies (ICISCT), 2021, pp. 1-4, doi: 10.1109/ICISCT52966.2021.9670307.
7. A. Kabulov, I. Saymanov, I. Yarashov and A. Karimov, "Using Algorithmic Modeling to Control User Access Based on Functioning Table," 2022 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS),
8. Kabulov A. V., Yarashov I. K., Jo'Rayev M. T. Computer viruses and virus protection problems //Science and Education. – 2020. – Т. 1. – №. 9. – С. 179-184.
9. Kabulov A. et al. Algorithmic method of security of the Internet of Things based on steganographic coding. 2021 IEEE International IOT //Electronics and Mechatronics Conference, IEMTRONICS. – 2021.
10. Madrahimova D., Yarashov I. Limited in solving problems of computational mathematics the use of elements //Science and Education. – 2020. – Т. 1. – №. 6. – С. 7-14.
11. Kabulov A., Yarashov I., Vasiyeva D. SECURITY THREATS AND CHALLENGES IN IOT TECHNOLOGIES //Science and Education. – 2021. – Т. 2. – №. 1. – С. 170-178.
12. Kabulov A., Muhammadiyev F., Yarashov I. ANALYSIS OF INFORMATION SYSTEM THREATS //Science and Education. – 2020. – Т. 1. – №. 8. – С. 86-91.
13. Gaynazarov S. M. et al. ALGORITHM OF MOBILE APPLICATION FOR MEDICINE SEARCH //Science and Education. – 2020. – Т. 1. – №. 8. – С. 600-605.
14. Кабулов А. В. Шерзод Туйлибоевич Болтаев, and Гулдофарид Муроджоновна Хабибжонова.«АЛГОРИТМИЧЕСКИЕ АВТОМАТНЫЕ МОДЕЛИ И МЕТОДЫ СОЗДАНИЯ РАСПРЕДЕЛЕННЫХ МИКРОПРОЦЕССОРНЫХ СИСТЕМ УПРАВЛЕНИЯ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.» //WORLD SCIENCE: PROBLEMS AND INNOVATIONS. – 2019.
15. Yarashov I., Normatov I., Mamatov A. THE STRUCTURE OF THE ECOLOGICAL INFORMATION PROCESSING DATABASE AND ITS ORGANIZATION //International Conference on Multidimensional Research and Innovative Technological Analyses. – 2022. – С. 114-117.
16. Кабулов А. В. и др. АЛГОРИТМИЧЕСКИЕ АВТОМАТНЫЕ МОДЕЛИ И МЕТОДЫ СОЗДАНИЯ РАСПРЕДЕЛЕННЫХ МИКРОПРОЦЕССОРНЫХ СИСТЕМ УПРАВЛЕНИЯ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ //WORLD SCIENCE: PROBLEMS AND INNOVATIONS: сборник статей XXIX. – 2019. – С. 40.
17. Yarashov I., Normatov I., Mamatov A. ECOLOGICAL INFORMATION PROCESSING TECHNOLOGIES AND INFORMATION SECURITY //International Conference on Multidimensional Research and Innovative Technological Analyses. – 2022. – С. 73-76.
18. Kabulov A., Yarashov I., Mirzataev S. DEVELOPMENT OF THE IMPLEMENTATION OF IOT MONITORING SYSTEM BASED ON NODE-RED TECHNOLOGY //Karakalpak Scientific Journal. – 2022. – Т. 5. – №. 2. – С. 55-64.
19. Бабаджанов А. Ф. и др. АЛГОРИТМИЧЕСКИЙ АНАЛИЗ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ ТАБЛИЦ ФУНКЦИОНИРОВАНИЯ //International Journal of Contemporary Scientific and Technical Research. – 2022. – С. 216-219.

20. I. Yarashov, "Development of a reliable method for grouping users in user access control based on a Functioning table," 2022 International Conference on Information Science and Communications Technologies (ICISCT), 2022, pp. 1-5.
21. I. Normatov, I. Yarashov, A. Otakhonov and B. Ergashev, “Construction of reliable well distribution functions based on the principle of invariance for convenient user access control,” 2022 International Conference on Information Science and Communications Technologies (ICISCT), 2022, pp. 1-5.
22. S. Toshmatov, I. Yarashov, A. Otakhonov and A. Ismatillayev, “Designing an algorithmic formalization of threat actions based on a Functioning table,” 2022 International Conference on Information Science and Communications Technologies (ICISCT), 2022, pp. 1-5.