Volume 3, Issue 5 May 2025 **ISSN (E):** 2938-3757

SYSTEMATIC IMPLEMENTATION OF BLOCKCHAIN TRANSACTION AND ANALYSIS OF MODERN DATA PROCESSING TECHNOLOGY

Mirabbos Akbarov 1,
Inomjon Yarashov 1, 2
1 Diplomat University
2The University of World Economy and Diplomacy
e-mail: m_akbarov@mail.ru

Abstract
This article presents a systematic analysis of blockchain technology and explores its application in contemporary digital environments. The primary focus is on the challenges associated with distributed blockchain architectures, while also identifying key application domains. The study examines mathematical models and implementation algorithms for core blockchain components, and provides a structured analysis of inherent contradictions within the technology, including a brief review of its internal mechanisms such as data encoding and consensus algorithms. The paper highlights the developmental potential of blockchain-based services, particularly through the concept of smart contracts, which enable autonomous transactions among network participants. These smart contracts facilitate the creation of decentralized, independent organizational units that function according to internally defined rules and operate with minimal external intervention. Such decentralized applications (dApps) offer significant advantages over traditional software systems, particularly in terms of flexibility, transparency, and security. Leveraging the principles of peer-to-peer (P2P) networks, wherein all participants are treated as equals, blockchain technologies enable direct transactions between users without intermediaries. This capability supports the formation of a core processing framework for decentralized autonomous organizations (DAOs)—a novel form of digital enterprise. Decisions built on blockchain technology provide a secure and inherently decentralized infrastructure for transaction processing and data management. A distinct advantage of blockchain, compared to traditional database models, is its algorithmic governance, implemented through a unified protocol. In conclusion, the article offers recommendations for the adoption of blockchain as a means of maintaining a unified data registry, particularly in environments requiring synchronized data processing and management systems.

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

Web of Technology: Multidimensional Research Journal
webofjournals.com/index.php/4

Web of Technology: Multidimensional Research Journal
webofjournals.com/index.php/4

Introduction

In recent times, issues of system reliability have become increasingly significant, creating new demands for data processing and storage technologies. Blockchain technology, which involves a chain of transaction blocks created according to specific rules, plays a pivotal role in ensuring mutual cooperation among a large number of users without the need for trusted intermediaries [1-6].

However, the reliability of data storage in blockchain systems comes at the expense of processing speed. For instance, in the Bitcoin system [7-11], the time required to add a single block is approximately 10 minutes, largely due to the decentralized nature of the system. This delay occurs because information about new transactions must be distributed to approximately 80% of the network. In addition to speed, the issue of data storage arises: with each user storing over 80 GB of data and more than 16 million users, the total storage capacity exceeds 1.3 exabytes. These factors highlight the scalability challenges associated with blockchain technologies.

Blockchain technology originated from peer-to-peer networks, with Bran Cohen adding distributed hash tables to implement BitTorrent. By leveraging the achievements of BitTorrent and solving the problem of decentralized consensus, Bitcoin introduced the concept of the blockchain. The term "blockchain" was first used to describe a distributed database implemented in the Bitcoin cryptocurrency. The next significant advancement came with Ethereum, which expanded blockchain capabilities by introducing smart contracts and providing a platform for developing decentralized applications. Additionally, Hyperledger introduced a modular structure that facilitates integration with existing systems [12-17].

At a high level, blockchain protocols are built around the concept of the "smart contract", which is an electronic algorithm that defines the conditions for executing transactions, and is stored across the blockchain's network nodes. A transaction refers to any interaction by participants with the system’s data. Once a transaction occurs, it must be recorded on the blockchain by placing it within a block. However, adding a new block to the blockchain requires consensus from other network participants, a process known as "consensus".

Blockchain technologies hold significant promise for the development of corporate information systems. Current back-office systems are often highly complex, opaque, and reliant on isolated internal business processes. The demand for blockchain in modern systems is driven by the need for efficient data sharing and storage [4-6]. A primary issue arises because each market or organization maintains its own data register, leading to inefficiencies.

The challenges associated with the use of multiple registers include:

- Each party must maintain its own data register.
- Data inconsistency and errors, leading to complex reconciliation operations.
- Lack of standardization.

Blockchain technologies offer several solutions:

- A common trusted register shared by all participants.
- A central counterparty to facilitate transactions.

Elimination of distrust between counterparties by ensuring data immutability and the use of a distributed algorithm to add new information.

By ensuring data immutability and implementing distributed consensus, blockchain reduces both time and financial costs. Moreover, blockchain's ability to make business processes more transparent and secure has resulted in its increasing adoption in various applications, including:

- Digital corporate systems.
- Digital notary services.
- Intermediary-free trading platforms.
- Interbank payment systems.
- Electronic voting (e-voting).

Looking ahead, the focus will likely be on:

- Pilot projects utilizing blockchain technology, such as FireChat, PopcornTime, Lighthouse, Gems, and CanadaCoin.
- Research on decentralized consensus algorithms.
- Development of diverse application platforms like Bitcoin, Ethereum, Eris, Ripple, Dogecoin, and Hyperledger.
- Further unification and standardization of blockchain technologies.
- Development of mechanisms for digitizing physical assets and integrating them into blockchain systems.

This work aims to systematize the core principles of blockchain technology, providing a foundation for specific, practical recommendations on implementing and maintaining a unified data registry within the context of synchronous technologies that support product life cycle processes.

Systematic analysis of blockchain technology

Blockchain, like any emerging technology, faces several challenges that must be addressed before it can be fully implemented at scale. One key issue is the problem of decentralized data storage (see Fig. 1). If a complete data register is stored at each network node, this configuration allows the network to be restored up to the point of destruction of the last node. However, this solution comes with significant trade-offs.

The primary drawback is the continuous growth of the network over time, which inevitably leads to the accumulation of uncontrollable volumes of data. This expansion poses serious concerns regarding storage management and data scalability. Moreover, any new participant joining the network must undergo a synchronization process, which involves downloading a massive amount of data to fully integrate into the blockchain system [11]. These factors contribute to the complexity of managing decentralized storage in blockchain networks, necessitating the development of strategies to mitigate data overload and improve the efficiency of synchronization for new participants.

Web of Technology: Multidimensional Research Journal
webofjournals.com/index.php/4

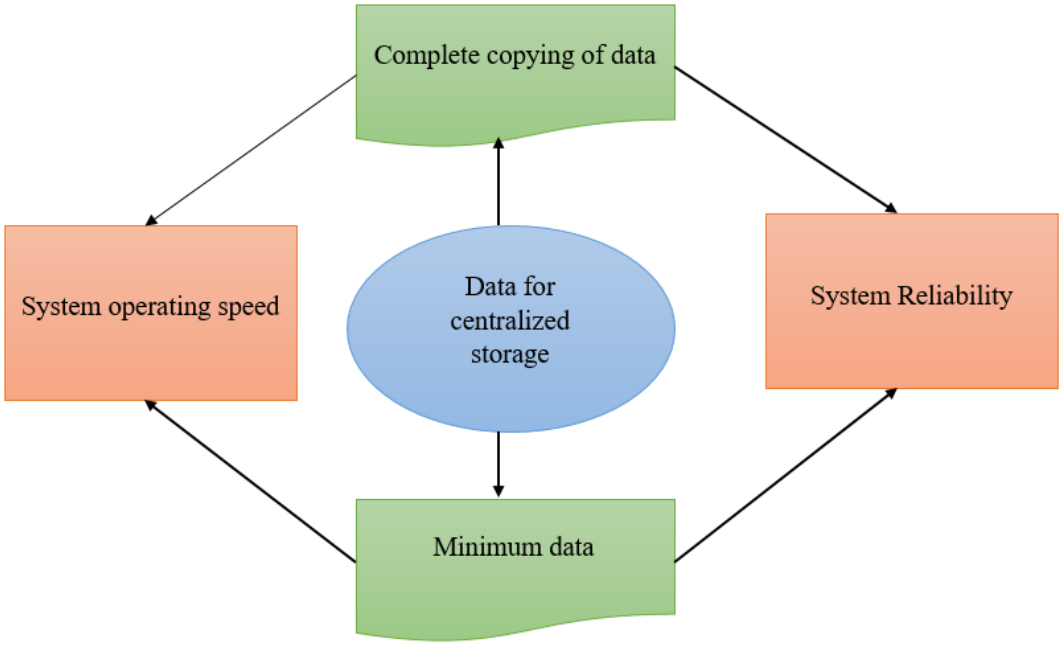

Fig 1. Map of contradictions for decentralized data storage

To address the challenge of decentralized data storage, one alternative approach is to utilize a standard database where real data is stored in encrypted form, with only their hashes being recorded in the blockchain, while older blocks are archived. However, this solution serves more as a temporary delay rather than a definitive resolution to the problem. Another potential solution could involve leveraging techniques from Big Data technologies [12], which are already tailored to handle large-scale data storage and processing. Various architectures such as MapReduce, Shared Memory, Shared Nothing, Shared Disk, and others have been developed to address these issues.

The main obstacle to integrating Big Data tools into the blockchain lies in the inherent system architecture: blockchain operates as a decentralized, distributed system, meaning the calculations are distributed across multiple nodes with no central authority overseeing the operations of the network nodes. However, integration could be feasible in the reverse direction, as blockchain, at its core, is a simple database with inherent challenges in scalability and a lack of query languages. Nevertheless, its advantages—decentralization, immutability, transparency, and universal data exchange—provide substantial benefits that outweigh its limitations. In this context, technologies such as BigchainDB and IPDB are being developed, which could potentially evolve into planetary-scale databases with decentralized management.

Another critical task is establishing trust within the system. For the system to be effective, it must balance both anonymity and transparency for its participants (see Fig. 2).

Web of Technology: Multidimensional Research Journal
webofjournals.com/index.php/4

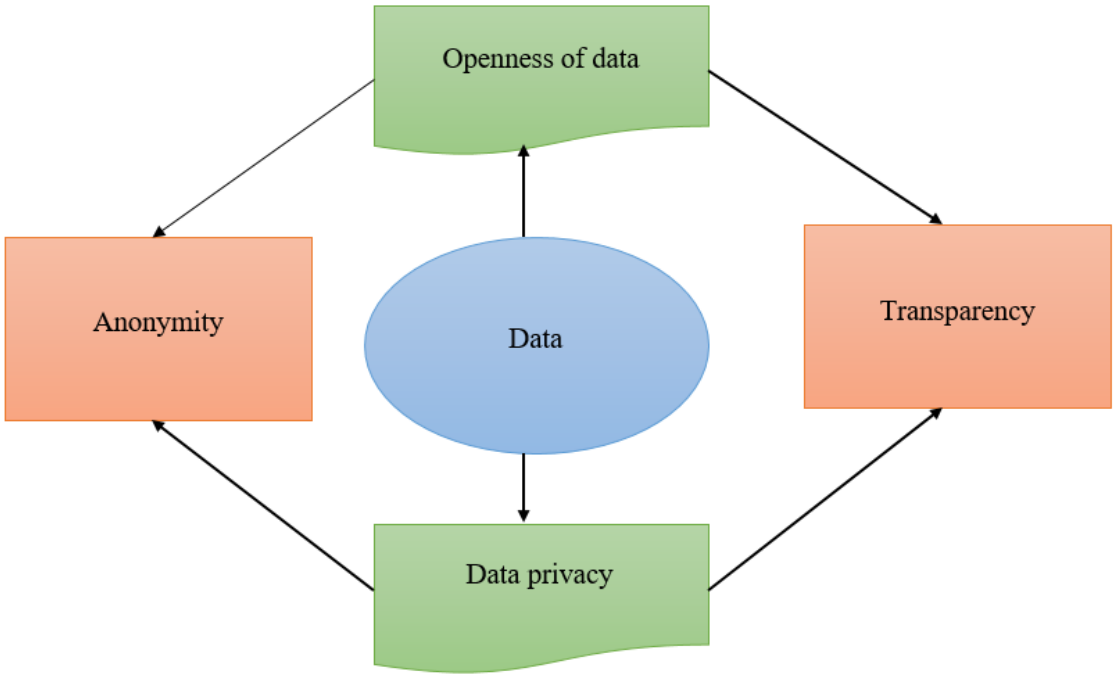

Fig 2. Contradiction map for system trust

To ensure that users can observe the movement of data on the network while maintaining privacy regarding their actions, it was decided to implement asymmetric encryption algorithms [9]. In this approach, each user is provided with a key pair: a private key and a public key (see Fig. 3). This method allows for secure data transmission while safeguarding the identity and activities of the users involved.

Fig 3. Relationship of user data

The private key is utilized to sign blocks sent by the user, ensuring the authenticity and integrity of the transaction. On the other hand, the user's address within the network is represented by the public key, which allows other participants to verify the authenticity of the user's actions without exposing sensitive information.

Analysis and classification of application fields

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

Web of Technology: Multidimensional Research Journal
webofjournals.com/index.php/4

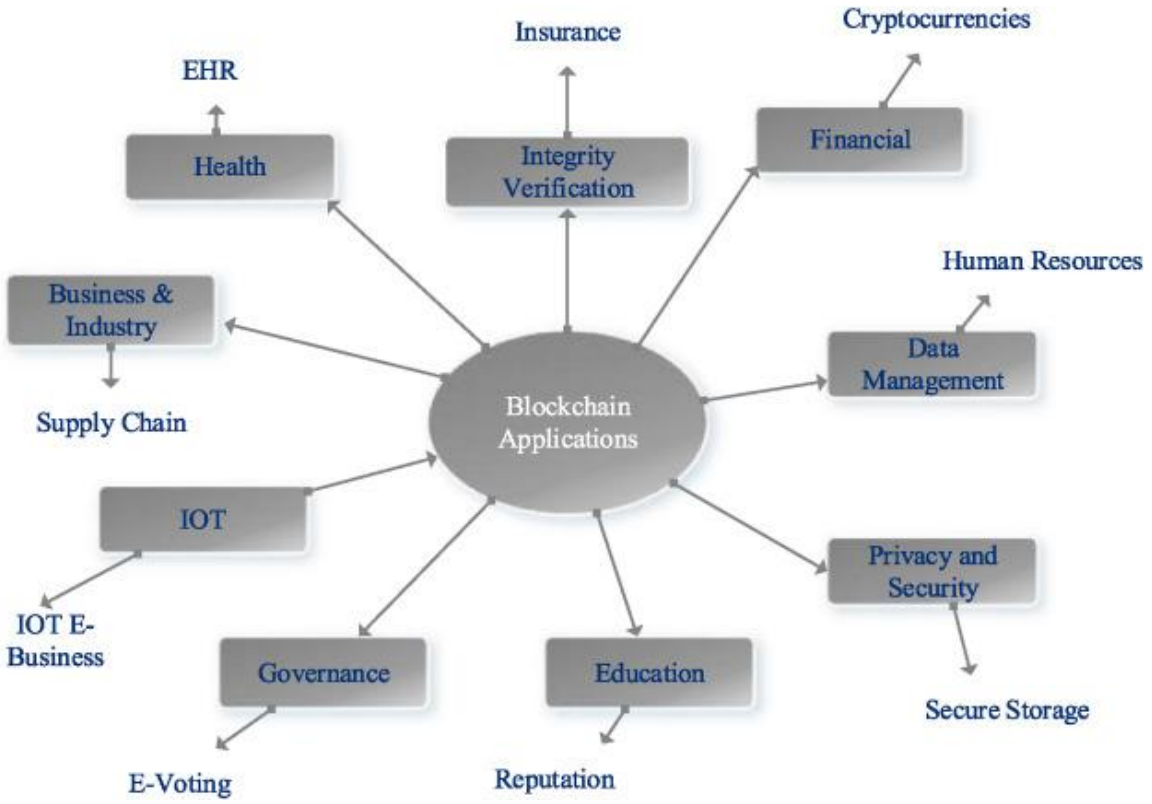

Fig 4.Classification of regional applications of blockchain technology

An example of credential management implementation can be observed in notarial projects, where users authenticate themselves through photos or videos presented to the system controller. These multimedia files are subsequently added to the blockchain, ensuring they cannot be altered or overwritten, thus providing a tamper-proof record of the user's identity.

The application of blockchain technology in marketplaces can be demonstrated by OpenBazaar, a decentralized peer-to-peer platform. Unlike traditional systems, OpenBazaar operates without a central server, meaning it is not susceptible to government restrictions. This model reflects the evolution of an unrestricted global marketplace where buyers and sellers can directly interact, facilitating transactions without the need for intermediaries or commission fees.

In the realm of interbank payment systems, the Ripple protocol has gained attention. The pilot program utilizing the RC Cloud cloud payment platform allows for local and international money transfers to occur almost instantly and at a reduced cost compared to traditional financial solutions.

Moreover, electronic voting has emerged as a blockchain-based solution within social networks. This system ensures the integrity of the voting process by offering several key advantages:

- Error tolerance, ensuring minimal risk of incorrect results.
- The ability to track each vote to its source, enhancing accountability.
- Unrestricted access to the system, ensuring broad participation.
- Voter anonymity, which guarantees privacy.
- The capability to verify results by all participants.

Web of Technology: Multidimensional Research Journal
webofjournals.com/index.php/4

Web of Technology: Multidimensional Research Journal
webofjournals.com/index.php/4

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

One of the primary challenges facing blockchain technology is ensuring the reliability of data, which underscores the necessity for efficient encryption algorithms. These algorithms must not only guarantee sufficient cryptographic strength for securing information within the network but also enable the implementation of digital signatures to authenticate transactions and communications. A widely used encryption method in blockchain systems is the RSA asymmetric encryption algorithm. The algorithm operates by first selecting two large prime numbers, p and q. These primes are used to generate the public and private keys through the following steps:

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

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

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):

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

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

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

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

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

When attempting to crack or retrieve the private key, it is necessary to test 2^N combinations, where N is the length of the key. For instance, with a 256-bit key and a guess rate of 1024 attempts per second, it would take approximately 1.23×10^{67} years to break the key. This is an extraordinarily long time, making it practically impossible to retrieve the key before the information becomes obsolete.

Additionally, there are advanced algorithms such as the Elliptic Curve Digital Signature Algorithm (ECDSA), which operate on similar principles but with their own particularities, enhancing security and efficiency. ECDSA provides shorter key lengths while maintaining a high level of security, which is particularly valuable in situations with limited storage or bandwidth.

Another critical issue in blockchain technology is ensuring concurrent access and resolving collisions in the network. Below are some noteworthy algorithms:

PBFT (Practical Byzantine Fault Tolerance): In this algorithm, a request to add a block is sent to all participants. Each participant computes the hash of the next block and sends their decision to the others. After gathering all responses, the answer with more than 50% approval is considered reliable. A key drawback of PBFT is the increased transaction execution time as the network size grows.

PoW (Proof of Work): In this consensus mechanism, network nodes (often called miners) solve complex problems to compute the hash of the next block. The first miner to solve the problem adds the block to the blockchain. The main disadvantages of PoW are its high energy

consumption and the potential for centralization, as miners with stronger computational resources have an advantage.

PoS (Proof of Stake): PoS is an alternative to PoW that does not require significant computational power. Instead, participants use an internal system currency (like tokens or coins), and those with more currency have a higher chance of creating the next block. The main limitation of PoS is the lack of randomness, which may lead to wealthy participants having too much influence over the system.

Limited Resource Proofs (e.g., Burn, Space, Bandwidth): These are variations of PoW and PoS. Participants must prove that they have a certain amount of a limited resource (disk space, network bandwidth, or tokens burned) to participate in the block creation process. These methods aim to reduce the need for heavy computational power while still maintaining fairness and security.

Concept of introduction of blockchain technologies in remote identification systems

This system operates within a closed network that does not involve cryptocurrency. It supports the use of smart contracts and role-based access for participants, along with a comprehensive SDK and a modular structure. This modularity allows for the replacement of individual system modules, making it possible to reuse the company's prior work. The general operational algorithm of the system can be outlined as follows:

1. The user visits an organization that is part of the blockchain network consortium and undergoes an authentication process.
2. After successful authentication, the user's data is entered into the database, and the user is assigned an electronic key linked to their record.
3. The user logs into the network and generates a request for data processing. The controller then requires the identification data that the user previously provided to the network.
4. The user enters their electronic key and selects the attributes of their record that should be shared with the regulator. This enables remote identification using the electronic key.

In this closed network, which consists of developers, project managers, contractors, and other relevant parties, blockchain technology ensures that a transaction is recorded only at legally defined moments during the execution of work. Prior to these moments, actions must receive approval from the project manager and other developers. Once approval is granted, the next transaction is initiated. This structure provides clear and evenly distributed incentives for the parties involved to register these events along the blockchain. Essentially, participants are incentivized to register these actions correctly, as failure to do so would result in the non-receipt of the resources they requested.

Conclusion

By analyzing the internal mechanisms, including coding and consensus models, a systematic evaluation of blockchain technology's contradictions is conducted. Decentralized applications (DApps) offer greater flexibility, transparency, and security compared to traditional applications built on conventional architectures. Leveraging the advantages of peer-to-peer (P2P) networks, where all participants are treated equally, blockchain technologies facilitate direct transactions between network members. Blockchain-based solutions establish a secure, immutable, and

Web of Technology: Multidimensional Research Journal
webofjournals.com/index.php/4

decentralized framework for handling transactions. One of the key benefits of blockchain, as opposed to other database systems, is its ability to implement algorithmic management under a unified protocol. The primary focus here is on the distributed nature of blockchain technology and the various fields where it can be applied. In conclusion, within the context of synchronous data processing and management technologies, recommendations are provided on the adoption of blockchain for maintaining a single, transparent register of data.

References

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.

Web of Technology: Multidimensional Research Journal
webofjournals.com/index.php/4