UDC 004

ANALYSIS OF BLOCKCHAIN TECHNOLOGY

Kashaganova G.B., Sekushin N.S.

Almaty Technological University, Almaty, Kazakhstan

Abstract. This article provides a brief overview of blockchain technology. Blockchain is a decentralized distributed database that ensures secure and transparent transactions. It allows transactions to occur without the need for third parties. The article gives an example of blockchain technology, explains its basic principles, types, and examples of its use in IT products.

Keywords: blockchain, system, transactions, network, cryptocurrency, bitcoin.

Materials and Methods. Blockchain is a complex and rapidly growing technology, gaining popularity due to its versatility. It stands at the intersection of several scientific disciplines and areas of activity, such as distributed computing, macroeconomics, and even game theory methods, which are widely used in the mathematics behind cryptocurrencies. This encourages various actions from participants in the system.

Blockchain is considered the core technological innovation behind Bitcoin. Users can rely on a public ledger system stored on many different decentralized nodes around the world, instead of depending on trust in a transaction counterparty (another person) or a third-party intermediary (such as a bank). This system can be used for processing any currency, financial contract, or asset, whether fixed or inactive [3, p. 12].

In October 2008, an anonymous author or group of authors under the name "Satoshi Nakamoto" published an article about Bitcoin. It was the first electronic monetary system that did not require third-party trust. However, the term "blockchain" was not mentioned in the text. The idea of this technology was introduced later. The first blockchain, created in 2010, was a convenient transactional payment system that allowed the transfer of money from one point to another, offering a wide range of financial services: lending, borrowing, depositing, investing, etc. [2, p. 10].

One key aspect of blockchain technology is its ability to support video calls or audio consultations, where patients can directly interact with doctors about their health, simplifying the process of seeking medical advice and making it more accessible and faster.

Bitcoin is based on cryptographic schemes that allow participants in the network to verify transactions in an untrusted environment and store them in a cryptographically protected and immutable ledger.

Today, blockchain is widely used in the financial sector. It is actively applied in stock trading, Know Your Customer (KYC) systems in banks, and cross-border payments. Any type of property or asset can be registered on the blockchain, making it possible to transfer assets, verify ownership, or maintain a transaction log. Blockchain also plays a critical role in creating peer-to-peer systems, enabling Internet of Things (IoT) devices to interact with each other, while different communication models and protocols do not interfere [4, p. 38].

Currently, public blockchain models are the most common. They involve a highly decentralized, fully connected network based on a public chain. These models rely on the principle of absolute trust, where there is no need to trust the counterparty at all [2, p. 14].

Private blockchain models have their own rules, with specific participants managing the nodes and accessing the network services. These rules may include financial and legal requirements. In such networks, participants are identifiable, and access is restricted and regulated according to network rules [2, p. 15].

Hybrid blockchain models combine the features of both open and closed networks. They offer data confidentiality, ease of deployment, and seamless integration with third-party IT solutions [2, p. 16].

Blockchain consortia involve multiple equal parties acting as validators. Consortium organizations share responsibility for the blockchain's operation and determining access rights to the data [2, p. 17].

Technology Capabilities

Decentralization in blockchain refers to the process of shifting control and decision-making from a central authority (such as an individual, organization, or group) to a distributed network of participants. In a decentralized blockchain, transparency ensures that all participants can trust each other. This reduces the influence any one participant can have over others, which helps maintain the functionality of the network.

Immutability means that once data is entered into the blockchain, it cannot be changed. No participant can alter a transaction after it has been added to the ledger. If an error is found in a record, a new transaction must be created to correct it. Both the original transaction and the correction will appear in the blockchain.

The blockchain system follows a set of **consensus rules**, which define how participants agree on the validity of transactions. New transactions can only be added to the blockchain once a majority of the network participants approve them [5, p. 1].

Principles of Operation

Step 1: Recording a transaction. A transaction is a single entry in the blockchain database. It includes information about the time, location, and participants of the transaction. First, the transaction data is hashed (converted into a fixed-length code) and then signed using an electronic signature algorithm [1, p. 123].

Step 2: Reaching consensus. The majority of participants in the blockchain network must confirm that the transaction is valid. Common consensus algorithms used in blockchain are Proof of Work (PoW) and Proof of Stake (PoS) [2, p. 27].

Step 3: Blockchain. The **mempool** is a storage area on the nodes (computers in the network) where transactions are temporarily placed before being grouped into blocks. The larger the value of the cryptocurrency and the higher the number of transactions, the bigger the mempool grows [1, p. 127].

Once transactions are selected and verified, they are combined into a **block**. To do this, a **Merkle tree** is used, where each leaf of the tree is the hash of a

transaction. These hashes are paired up, and new hash codes are generated for each pair. If the number of transactions is odd, the last transaction is duplicated. In the end, only one hash code remains — the **root** of the Merkle tree — and this is added to the block. This tree structure allows clients to verify if their transaction was included in the block [1, p. 128].

Step4: Open public access to the registry. The system makes the latest copy of the blockchain available to all participants in the network [2, p. 27].

Conclusion. This simplified explanation of blockchain highlights its core features: decentralization, immutability, and consensus-driven transaction validation. These principles ensure that blockchain can operate securely and transparently without the need for intermediaries. Let me know if you'd like any further simplification or clarification!

References:

1. Ishchukova, E.A., Panasenko, S.P., Romanenko, K.S., Salmanov, V.D. (2022). Cryptographic foundations of technologies. Moscow: DMK Press, 302 pages.

2. Pestrenko, A.S. (2022). Quantum threat to the security of control technology: a teaching aid. St. Petersburg: Athena Publishing House, 105 pages.

3. Swan, M. (2017). Blockchain: The scheme of the new economy (translated from English). Moscow: Olimp-Business, 240 pages.

4. Singhal, B., Dameja, G., Panda, P.S. (2020). Blockchain: A guide for novice developers (translated from English). St. Petersburg: BHV-Petersburg, 288 pages.

5. Amazon Web Services (AWS). What is Blockchain. Retrieved from https://aws.amazon.com/ru/what-is/blockchain/