UDC 004.75–004.6

BLOCKCHAIN-BASED DATA INTEGRITY FOR DISTRIBUTED INFORMATION SYSTEMS

Chernenko K. S.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Perevyshko A.I. – Senior Lecturer at the Department of Foreign Languages

Annotation. This research explores the application of blockchain technology for ensuring data integrity in distributed information systems. At the beginning, the author gives a valuable information on blockchain principles and consensus mechanisms. Next, much attention is given to the advantages of decentralization, immutability, and cryptographic security in maintaining data integrity. At the end, it is spoken about challenges related to scalability, performance, and implementation complexity.

Keywords: blockchain, data integrity, distributed information systems, consensus mechanisms, cryptographic security, decentralization, immutability.

Introduction. Ensuring data integrity is a crucial aspect of modern distributed information systems, where data is often stored and processed across multiple nodes. Traditional approaches rely on centralized databases and access control mechanisms, which are susceptible to single points of failure, unauthorized modifications, and data breaches.

Blockchain technology provides an alternative solution by introducing a decentralized and tamper-resistant model for data storage and verification [1]. Utilizing cryptographic hashing, distributed consensus, and immutable ledgers, blockchain ensures that once recorded, data cannot be altered or deleted without detection. These properties make blockchain a promising tool for enhancing data integrity in distributed environments.

Main part. Blockchain is a distributed ledger technology that records transactions in a secure, transparent, and immutable manner. It consists of a continuously growing chain of blocks, where each block contains a set of transactions, a cryptographic hash of the previous block, and a timestamp.

Each new block is linked to the previous one through its hash, forming an unbroken chain of data (shown in Figure 1).

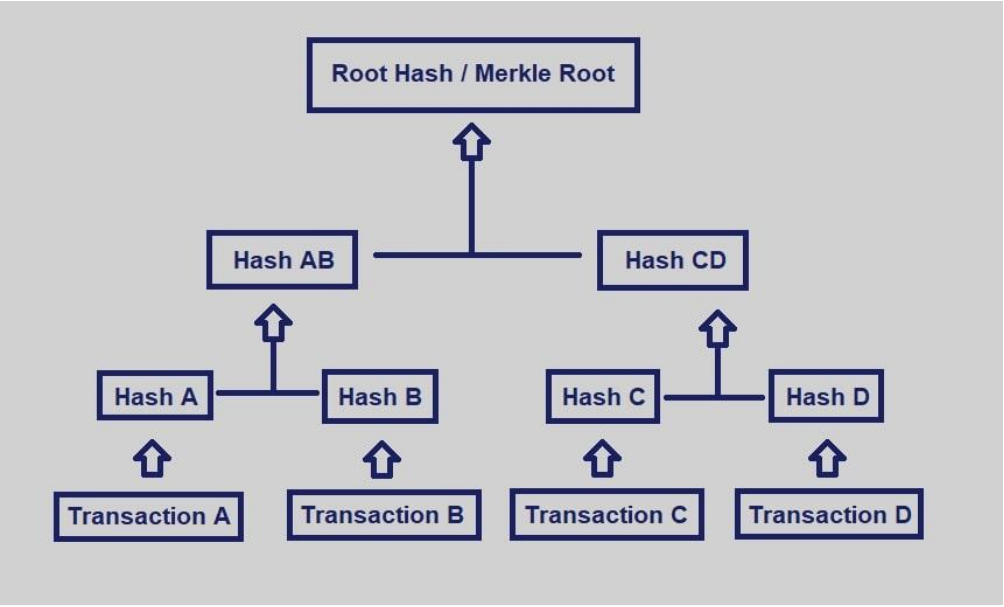

Figure 1 – The fundamental structure of a blockchain, showing how each block is linked to the previous

This structure ensures that any attempt to alter a block would require modifying all subsequent blocks, making tampering computationally infeasible.

Since blockchain operates in a decentralized environment, there is no central authority responsible for validating transactions or maintaining the ledger. Instead, this responsibility is distributed among network nodes, which are independent computers participating in the blockchain network. To ensure that all nodes maintain a consistent and trustworthy version of the ledger, blockchains rely on consensus mechanisms-protocols that allow nodes to agree on which transactions are valid and should be added to the blockchain.

Proof of Work (PoW) is a consensus mechanism that relies on computational effort to validate transactions and secure the blockchain. Participants, known as miners, compete to solve a complex mathematical puzzle. The first miner to solve it gets the right to add a new block to the blockchain.

One of the key security features of PoW is its resistance to the 51% attack. This attack occurs when a single entity gains control over more than 50% of the total mining power. With such power, the attacker could potentially alter transaction history, reverse completed transactions (double spending), or prevent new transactions from being confirmed. However, achieving such dominance is extremely expensive, requiring massive computational resources and electricity, making PoW blockchains highly secure but energy-intensive.

Proof of Stake (PoS) offers an alternative approach, replacing computational work with economic incentives. Instead of mining, the network relies on validators-participants who hold and «stake» a certain amount of tokens as collateral. The blockchain selects validators to confirm transactions and create new blocks, usually based on the amount of tokens they have locked up in the system. The more tokens a participant stakes, the higher their chances of being chosen as a validator.

This system significantly reduces energy consumption compared to PoW. However, it introduces the risk of centralization, as wealthier participants who can stake more tokens have greater influence over the network. To mitigate this, PoS blockchains often implement mechanisms like random selection or weighted voting to distribute validation rights more fairly.

Beyond PoW and PoS, several other mechanisms exist to balance security, decentralization, and efficiency:

Delegated Proof of Stake (DPoS): Instead of all token holders participating in validation, they vote for a small group of representatives who take on this responsibility [2]. This improves scalability but concentrates power in fewer hands.

Proof of Authority (PoA): Used mainly in private blockchains, where validation is performed by a fixed number of trusted entities rather than an open network of participants.

Each of these mechanisms is suited for different blockchain applications, depending on whether the priority is security, speed, or decentralization.

Ensuring data integrity in distributed systems relies on cryptographic hashing and digital signatures, which prevent unauthorized modifications and ensure authenticity.

A cryptographic hash function transforms input data into a unique, fixed-length hash. Even a small change in the input produces a completely different hash, making it easy to detect tampering. In blockchain, each block contains a hash of the previous block, creating a chain of blocks where any modification breaks the sequence, ensuring immutability.

A digital signature guarantees that transactions originate from legitimate sources and remain unchanged. When a user signs a transaction with their private key, others can verify it using the corresponding public key. This prevents unauthorized modifications and ensures that only the rightful owner can approve transactions.

These methods form the foundation of data integrity in blockchain, ensuring that stored information remains unaltered, authentic, and verifiable.

While blockchain offers strong security and data integrity guarantees, its widespread adoption is hindered by several critical challenges. The decentralized nature that makes blockchain resilient also introduces limitations in scalability, performance, and ease of integration into

existing systems. Addressing these obstacles is crucial for blockchain to transition from niche applications to mainstream use.

One of the most pressing issues is scalability. Unlike centralized systems that can process thousands of transactions per second (TPS), major blockchain networks like Bitcoin and Ethereum are constrained to much lower throughput due to their consensus mechanisms. Every transaction must be validated and recorded across multiple nodes, creating a bottleneck. To mitigate this, researchers and developers have introduced scaling solutions such as sharding (dividing the blockchain into smaller, parallel segments), off-chain transactions (handling certain operations outside the main blockchain), and Layer 2 protocols like the Lightning Network, which enable faster transactions while preserving security [3].

Another challenge is performance. Blockchain operations require significant computational resources, especially in networks using Proof of Work (PoW), where miners solve complex cryptographic puzzles to validate transactions. This results in high energy consumption and slow transaction processing times [4]. Alternative consensus mechanisms like Proof of Stake (PoS) aim to reduce these inefficiencies, but they introduce trade-offs, such as potential centralization due to wealth-based validation [5].

Finally, implementation complexity remains a major barrier to blockchain adoption. Integrating blockchain into existing distributed systems requires significant architectural changes, as well as new regulatory and operational frameworks. Additionally, the lack of standardization and expertise in blockchain development further complicates its deployment. Organizations must carefully evaluate their requirements and consider hybrid solutions that combine blockchain with traditional databases to balance security, efficiency, and practicality.

These challenges highlight the need for ongoing research and technological advancements to optimize blockchain's performance while maintaining its core advantages.

Conclusion. The use of blockchain for data integrity in distributed information systems offers a reliable approach to securing and verifying data without reliance on a central authority. Its decentralized structure, immutability, and cryptographic security mechanisms ensure that once recorded, information remains tamper-proof and transparent. These properties make blockchain an attractive solution for applications where data authenticity and trust are critical.

Despite these advantages, practical adoption is hindered by scalability limitations, performance constraints, and the complexity of integration into existing infrastructures. Ongoing research into improved consensus mechanisms, scaling techniques, and hybrid models is essential to overcoming these challenges. As these advancements progress, blockchain's role in distributed systems will continue to expand, enhancing both security and efficiency.

References

1. *Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System [Electronic resource]. Mode of access: https://bitcoin.org/bitcoin.pdf. Date of access: 15.03.2025.*

2. *Wood G. Ethereum: A Secure Decentralised Generalised Transaction Ledger [Electronic resource]. Mode of access: https://ethereum.github.io/yellowpaper/paper.pdf. Date of access: 16.03.2025.*

3. *Sharding: A Comprehensive Overview [Electronic resource]. Mode of access: https://vitalik.ca/general/2021/04/07/sharding.html. Date of access: 18.03.2025.*

4. *The Bitcoin Energy Consumption Index [Electronic resource]. Mode of access: https://digiconomist.net/bitcoin-energy-consumption. Date of access: 21.03.2025.*

5. *Blockchain Consensus Mechanisms Explained [Electronic resource]. Mode of access: https://www.ibm.com/topics/blockchain-consensus. Date of access: 23.03.2025.*