UDC 004.75

# RELIABILITY ANALYSIS OF NETWORKS BASED ON BLOCKCHAIN TECHNOLOGY

**Abdullaev K.**
*master's degree, Baku State University (Baku, Azerbaijan)*

# АНАЛИЗ НАДЕЖНОСТИ СЕТЕЙ НА ОСНОВЕ БЛОКЧЕЙН-ТЕХНОЛОГИЙ

**Абдуллаев Х.И.**
*магистр, Бакинский государственный университет (Баку, Азербайджан)*

**Abstract**

Blockchain technology, known for its decentralized nature and cryptographic security, is widely adopted in industries such as finance, supply chain, and healthcare. However, ensuring the reliability of blockchain networks remains a significant challenge as their integration into mission-critical applications grows. This paper analyzes the reliability of blockchain networks by examining key elements such as consensus mechanisms, scalability, and security. Through a comparison of popular blockchain systems such as Bitcoin, Ethereum, and Ripple, the paper investigates their performance and resilience under varying conditions. The study also highlights the potential of layer 2 solutions to enhance scalability and transaction throughput. Overall, this research provides insights into the factors influencing blockchain reliability, offering a foundation for future improvements in blockchain-based applications.

**Keywords:** blockchain, consensus mechanisms, scalability, security, reliability, layer 2 solutions.

**Аннотация**

Блокчейн-технология, известная своей децентрализованной природой и криптографической безопасностью, широко используется в таких отраслях, как финансы, цепочки поставок и здравоохранение. Однако обеспечение надежности блокчейн-сетей остается важной проблемой с учетом их внедрения в критически важные приложения. В статье проводится анализ надежности блокчейн-сетей с учетом ключевых факторов, таких как механизмы консенсуса, масштабируемость и безопасность. Через сравнение популярных блокчейн-систем, таких как Bitcoin, Ethereum и Ripple, исследуются их производительность и устойчивость при различных условиях. В работе также рассматривается потенциал решений второго уровня для повышения масштабируемости и пропускной способности транзакций. В целом, исследование предоставляет ценные данные о факторах, влияющих на надежность блокчейнов, и служит основой для дальнейших улучшений в приложениях на базе блокчейн-технологий.

**Ключевые слова:** блокчейн, механизмы консенсуса, масштабируемость, безопасность, надежность, решения второго уровня.

## Introduction

Blockchain technology, which operates through a decentralized and distributed ledger system, has seen widespread adoption across numerous sectors, including finance, supply chain management, healthcare, and data security. The underlying principles of blockchain – such as transparency, immutability, and decentralization – make it an attractive alternative to traditional centralized systems. However, despite its advantages, the reliability of blockchain networks remains a critical concern. As blockchain technology becomes more integrated into mission-critical applications, understanding and ensuring the reliability of these networks is essential to their continued growth and adoption.

The purpose of this study is to analyze the reliability of blockchain networks by evaluating their resilience to failures, scalability challenges, and potential vulnerabilities. Blockchain systems, due to their decentralized nature, are often touted as being more secure and resistant to single points of failure. However, the complexity of blockchain protocols, consensus mechanisms, and network architecture introduces new challenges that may compromise system performance and reliability. This paper seeks to explore these aspects in depth, considering both theoretical foundations and practical case studies of blockchain implementations. This paper is structured to provide a comprehensive understanding of the reliability of blockchain networks. The first section covers the theoretical foundations of blockchain technology, including key components such as consensus mechanisms, smart contracts, and distributed ledger systems. The second section explores various factors influencing blockchain reliability, such as network topology, transaction processing speed, and resistance to attacks. Practical examples from real-world blockchain deployments are included to illustrate the application of these theoretical concepts in real-world scenarios.

## Main part

Blockchain technology offers a revolutionary approach to managing and securing transactions, driven by its decentralized nature and the cryptographic guarantees it provides [1]. The core of blockchain's reliability lies in its ability to maintain consistency and security across a distributed network. However, the performance and reliability of blockchain systems can vary significantly based on several factors, including the choice of consensus mechanisms, network scalability, and security protocols. In this section, the analysis of blockchain reliability will be structured around these key elements, with a focus on understanding their interplay and impact on system performance.

The consensus mechanism is a crucial element in determining how a blockchain network achieves agreement on the validity of transactions. Various consensus mechanisms, such as Proof of Work (PoW), Proof of Stake (PoS), and Byzantine Fault Tolerance (BFT), offer different trade-offs between security, scalability, and energy consumption. These mechanisms ensure the integrity of the blockchain by preventing double-spending and fraud while maintaining the decentralized nature of the system.

Table 1 provides a comparison of five popular consensus mechanisms, highlighting key characteristics such as transaction speed (transactions per second or TPS), energy consumption, security level, and scalability. For instance, PoW, used by Bitcoin, offers high security but suffers from low scalability and high energy consumption. On the other hand, Proof of Stake, implemented in Ethereum 2.0, offers improved scalability and lower energy consumption, but its security level is considered moderate compared to PoW. These trade-offs play a vital role in determining the overall reliability of a blockchain network, as the consensus mechanism impacts both the performance and the fault tolerance of the system [2].

Table 1

Consensus mechanisms comparison

| **Consensus mechanism** | **Transaction speed (TPS)** | **Energy consumption** | **Security level** | **Scalability** |
|---|---|---|---|---|
| PoW | 7 | High | High | Low |
| PoS | 100 | Low | Moderate | High |
| Delegated proof of stake (DPoS) | 1000 | Low | Moderate | High |
| Proof of authority (PoA) | 5000 | Low | High | Very high |

| | | | | |
|---|---|---|---|---|
| BFT | 3000 | Moderate | High | Moderate |

The scalability of blockchain systems, as influenced by the consensus mechanism, directly affects their reliability. Blockchain networks that struggle with scalability may experience delayed transaction processing times, particularly during periods of high demand. For instance, Bitcoin's transaction speed is limited to just 7 TPS, which can lead to congestion, especially during market surges. In contrast, newer consensus models, such as those used by Polkadot and Ethereum 2.0, are designed to enhance transaction throughput, potentially improving overall network reliability.

Scalability is another critical factor impacting the reliability of blockchain networks. As the size of the network grows, the number of transactions that must be processed also increases [3]. This can lead to network congestion, slower transaction speeds, and higher transaction costs, undermining the efficiency and reliability of the blockchain.

Table 2 compares several major blockchain networks based on their transaction speed (TPS) and primary use cases. For example, Ripple, designed for cross-border payments, supports a much higher transaction throughput (1500 TPS) compared to Bitcoin, whose slow transaction processing can hinder its use in real-time financial applications. The scalability of these networks is a result of various optimizations, such as the implementation of more efficient consensus mechanisms (like Ripple's protocol) and innovative technologies like sharding (used by Ethereum 2.0) that allow parallel transaction processing across multiple chains.

Table 2

Blockchain networks comparison

| **Blockchain network** | **Year of launch** | **Consensus mechanism** | **Transactions per second** | **Primary use case** |
|---|---|---|---|---|
| Bitcoin | 2009 | PoW | 7 | Digital currency |
| Ethereum | 2015 | PoS (Ethereum 2.0) | 30 | Smart contracts |
| Ripple | 2012 | Ripple protocol | 1500 | Cross-border payments |
| Polkadot | 2020 | Nominated proof of stake (NPoS) | 1000 | Multi-chain interoperability |
| Cardano | 2017 | Ouroboros PoS | 250 | Smart contracts & DApps |

This table outlines the key features of various blockchain networks, showing how they have evolved over time and their specific areas of application. It provides insight into the performance and reliability of these networks based on their scalability and transaction handling capabilities.

One promising solution to blockchain scalability is the use of layer 2 solutions, such as the Lightning Network for Bitcoin and Rollups for Ethereum [4]. These solutions aim to offload some of the transaction processing from the main blockchain, reducing congestion and improving overall system performance. As blockchain networks scale, it is essential to balance scalability with decentralization to ensure the reliability of the system.

**Security and attack resistance in blockchain networks**

The security of a blockchain network is fundamental to its reliability. Blockchain systems, while generally considered secure due to their cryptographic foundations, are not immune to various types of attacks. For example, the 51% attack occurs when a malicious actor gains control over the majority of a network's mining or staking power, potentially allowing them to alter the blockchain's transaction history.

Despite these vulnerabilities, several strategies are employed to mitigate risks and enhance the security of blockchain networks. One key approach is the implementation of robust smart contract audits and formal verification, which can prevent vulnerabilities from being exploited by attackers. Additionally, the decentralized nature of blockchain networks makes them inherently resistant to certain types of attacks, as there is no central point of failure [5]. However, achieving the right balance between security and system performance remains a key challenge, as overly stringent security measures can reduce transaction speed and overall system reliability.

In Ethereum, for example, the shift PoS through Ethereum 2.0 is expected to enhance both scalability and security, reducing the risk of 51% attacks compared to PoW. Similarly, Polkadot's multi-chain interoperability offers added security by allowing different blockchains to communicate securely while maintaining their individual consensus protocols.

**Governance and its impact on blockchain reliability**

Blockchain governance is another crucial factor that impacts the reliability of blockchain networks. Governance refers to the mechanisms by which decisions regarding protocol upgrades, consensus rules, and network management are made. In decentralized networks, governance is typically distributed among stakeholders, such as miners, developers, and token holders. However, governance models in blockchain networks can sometimes lead to fragmentation or instability. Disagreements over protocol changes or updates can lead to hard forks, where a blockchain splits into two separate chains. Such forks can cause temporary disruptions in the network's operation, affecting its reliability [6]. Ethereum's hard fork in 2016, following the DAO hack, is a notable example of governance challenges affecting the blockchain's continuity. Ensuring that blockchain governance remains efficient and transparent is essential to maintaining long-term network stability and reliability.

**Practical examples of blockchain reliability in use cases**

The real-world applications of blockchain technology provide valuable insights into its reliability. Case studies from industries such as finance, supply chain, and healthcare offer a glimpse into how blockchain networks perform under real-world conditions [7]. For example, Ripple's blockchain network has demonstrated its reliability in cross-border payments, offering a fast and secure way to transfer funds internationally. Ripple's high transaction throughput (1500 TPS) and low transaction fees make it a viable option for financial institutions looking to improve efficiency in global payment systems. However, the network's reliance on a centralized consortium of validators raises questions about the true decentralization of the system and its long-term reliability [8].

In the supply chain industry, blockchain technology is being used to track the movement of goods and ensure transparency. IBM's Food Trust Network, which uses blockchain to trace the origins of food products, is a prime example of blockchain's potential to improve transparency and reliability in supply chain management. However, challenges related to data accuracy, system integration, and scalability must be addressed to ensure that such systems remain reliable as they grow [9].

**Blockchain reliability testing through code example**

To further evaluate the reliability of a blockchain network, testing the transaction speed and confirmation times can provide valuable insights. Below is an example of a Python script that measures the transaction confirmation time on the Ethereum network using the web3.py library:

```
from web3 import Web3
import time

# Connect to an Ethereum node (Infura or local node)
w3 = Web3(Web3.HTTPProvider('https://mainnet.infura.io/v3/YOUR_INFURA_PROJECT_ID'))

# Define the sender and recipient address, and the amount to send (in Wei)
sender_address = '0xYourSenderAddress'
recipient_address = '0xRecipientAddress'
amount = w3.toWei(0.1, 'ether')

# Get the latest nonce (transaction count) for the sender address
nonce = w3.eth.getTransactionCount(sender_address)

# Create the transaction
transaction = {
    'to': recipient_address,
    'value': amount,
    'gas': 2000000,
    'gasPrice': w3.toWei('20', 'gwei'),
    'nonce': nonce,
    'chainId': 1
}

# Sign the transaction with the sender's private key (replace with your own)
private_key = 'your_private_key'
signed_transaction = w3.eth.account.signTransaction(transaction, private_key)

# Send the transaction
start_time = time.time()
transaction_hash = w3.eth.sendRawTransaction(signed_transaction.rawTransaction)

# Wait for transaction confirmation
receipt = w3.eth.waitForTransactionReceipt(transaction_hash)
end_time = time.time()

# Measure the time taken for transaction confirmation
confirmation_time = end_time - start_time
print(f"Transaction confirmed in {confirmation_time} seconds.")
```

This testing approach allows for a detailed assessment of blockchain network reliability in terms of transaction speed and confirmation times. By measuring how long it takes for a transaction to be confirmed, it becomes possible to evaluate the responsiveness of the network [10]. This is particularly important for applications requiring high-frequency transactions, such as financial services, where delays in transaction finality can lead to significant disruptions. Furthermore, understanding the variability in confirmation times across different blockchain networks can help identify areas for improvement, such as optimizing consensus mechanisms or reducing network congestion.

Additionally, this method provides valuable insights into the scalability of blockchain networks. As blockchain adoption increases, networks will face greater transaction volumes, and it is essential to understand how well they handle this increased load. By testing transaction confirmation times under varying network conditions, it is possible to simulate real-world scenarios and assess the network's capacity to maintain high levels of performance and reliability [11]. This kind of stress testing can guide decisions about which blockchain platforms are best suited for specific use cases, ensuring that the selected system can handle the demands of real-world applications.

## Conclusion

The reliability of blockchain networks is a critical factor for their successful implementation across various industries. This paper has explored the key elements that influence the reliability of blockchain systems, including consensus mechanisms, scalability, and security. A particular focus was placed on analyzing different blockchain networks, such as Bitcoin, Ethereum, Ripple, and Polkadot, assessing their ability to maintain reliability under high demand and potential security threats. Consensus mechanisms play a vital role in ensuring the integrity of blockchain networks. However, the choice of a specific mechanism depends on several factors, such as transaction speed requirements, energy consumption, and security levels. Systems utilizing PoW and PoS have demonstrated different trade-offs between performance and attack resistance, which significantly impacts their reliability in real-world applications.

Finally, the adoption of layer 2 technologies, such as the Lightning Network for Bitcoin and Rollups for Ethereum, emerges as a promising solution to improve scalability. These advancements are essential for ensuring blockchain networks remain reliable as they scale to handle increasing transaction volumes, providing a foundation for future blockchain-based applications across various sectors.

**References**

1. Lo S.K., Xu X., Staples M., Yao L. Reliability analysis for blockchain oracles // Computers & Electrical Engineering. 2020. Vol. 83. P. 106582.
2. Liu Y., Zheng K., Craig P., Li Y., Luo Y., Huang X. Evaluating the reliability of blockchain based internet of things applications // In 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN). 2018. P. 230-231.
3. Chang Y.X., Wang Q., Li Q.L., Ma Y., Zhang C. Performance and Reliability Analysis for PBFT-Based Blockchain Systems with Repairable Voting Nodes // IEEE Transactions on Network and Service Management. 2024. Vol. 12. P. 100506.
4. Akhatov A.R., Nazarov F.M., Rashidov A. Mechanisms of information reliability in bigdata and blockchain technologies // 2021 International Conference on Information Science and Communications Technologies (ICISCT). IEEE, 2021. P. 1-4.
5. Wang Z., Zhang S., Zhao Y., Chen C., Dong X. Risk prediction and credibility detection of network public opinion using blockchain technology // Technological Forecasting and Social Change. 2023. Vol. 187. P. 122177.
6. Dudak A., Israfilov A. Application of blockchain in IT infrastructure management: new opportunities for security assurance // German International Journal of Modern Science. 2024. No. 92. P. 103-107.
7. Putro A.N.S., Mokodenseho S., Hunawa N.A., Mokoginta M., Marjoni E.R.M. Enhancing security and reliability of information systems through blockchain technology: a case study on impacts and potential // West Science Information System and Technology. 2023. Vol. 1(01). P. 35-43.
8. Modares A., Emroozi V.B., Gholinezhad H., Modares A. An integrated cognitive reliability and error analysis method (CREAM) and optimization for enhancing human reliability in blockchain // Decision Analytics Journal. 2024. Vol. 12. P. 100506.
9. Goyat R., Kumar G., Alazab M., Saha R., Thomas R., Rai M.K. A secure localization scheme based on trust assessment for WSNs using blockchain technology // Future Generation Computer Systems. 2021. Vol. 125. P. 221-231.
10. Yang T., Cui Z., Alshehri A.H., Wang M., Gao K., Yu K. Distributed maritime transport communication system with reliability and safety based on blockchain and edge computing // IEEE Transactions on Intelligent Transportation Systems. 2022. Vol. 24(2). P. 2296-2306.
11. Ibrahim H.A., Shouman M.A., El-Fishawy N.A., Ahmed A. Improving the reliability of nanosatellite swarms by adopting blockchain technology // Complex & Intelligent Systems. 2024. Vol. 10(5). P. 7163-7182.