CYBERNETICS and COMPUTER TECHNOLOGIES

УДК 004.75 DOI:10.34229/2707-451X.25.2.7

D. DVORCHUK, I. SHPINAREVA

ANALYSIS OF BLOCKCHAIN-TECHNOLOGY

This paper presents a comprehensive analysis of blockchain technology, exploring its fundamental principles, classification, and evolving applications across various industries. The study highlights the key attributes of blockchain, including decentralization, transparency, and security, while also addressing its inherent limitations, such as scalability and transaction speed. A detailed comparison of consensus mechanisms – Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), and Byzantine Fault Tolerance (BFT) variations – illustrates their impact on blockchain performance. Additionally, the research examines Layer 1 (L1) and Layer 2 (L2) scaling solutions, such as sharding, optimistic rollups, and sidechains, to improve transaction throughput. The study concludes with insights into emerging trends, including hybrid consensus algorithms and AI-driven optimizations, which have the potential to enhance blockchain efficiency and security.

Keywords: *blockchain, decentralization, consensus mechanisms, optimistic rollups, sharding, transaction validation.*

Introduction. The emergence of blockchain technology has fundamentally transformed the understanding of distributed systems and trust mechanisms in digital environments. Initially developed as the foundational technology for cryptocurrencies such as Bitcoin and Ethereum, blockchain has evolved into a versatile platform applied across various sectors, including information technology, telecommunications, retail, financial services, manufacturing, and electronic voting. Its key attributes – security, transparency, and efficient data management – have contributed to its widespread adoption.

In 2022, an additional 40 of the Forbes Global 200 companies announced blockchain initiatives, with the majority (19 companies) operating in the financial sector, including BlackRock, Goldman Sachs, HSBC, and BNP Paribas.

Blockchain technology serves not only as a means of storing digital records but also as a secure mechanism for verifying the existence of documents and tracking related transactions. It facilitates the representation of various legal and administrative records, such as asset transfers, contractual agreements, and tax transactions. Consequently, blockchain is emerging as an innovative approach to managing and recording administrative and legal processes.

In parallel, the integration of blockchain with Industry 4.0 technologies – such as the Internet of Things (IoT), artificial intelligence (AI), radio-frequency identification (RFID), cyber-physical systems, and global positioning systems (GPS) – is creating a robust ecosystem for production planning, control and supply chain management (SCM) [1, 2]. This convergence is significantly expanding the potential applications of blockchain, enabling more efficient, transparent, and secure operations across both administrative and industrial domains.

This paper aims to analyze blockchain technology, identify its current challenges and limitations, and propose new directions for its future development.

Blockchain Classification

Modern blockchain systems are categorized into three types: public, private, and hybrid.

A public blockchain is fully decentralized, operating on the principle of a distributed ledger. All nodes in the network participate in transaction verification, ensuring transparency and security. It allows open data reading and writing, meaning that any participant can access and modify data within the blockchain. Additionally, public blockchains maintain immutability, as once a record is verified, it cannot be altered or deleted. However, a major drawback is the substantial computational power required to sustain a large-scale distributed ledger, leading to scalabil ty challenges. Public blockchains are commonly applied in sectors such as healthcare and education.

A private blockchain, in contrast, operates within a closed and restricted network, under the control of a central authority that can modify its usage policies at any time. Unlike public blockchains, private blockchains offer high-speed transactions and mitigate scalability issues. However, they are only suitable for specific applications, such as enterprise solutions. Notably, private blockchains are more vulnerable to security breaches, as transaction validation is managed by a network administrator rather than a decentralized consensus mechanism. Due to these concerns, some critics argue that private blockchains deviate from the fundamental principles of blockchain technology.

A hybrid blockchain integrates features of both public and private blockchains, creating a semi-open network shared among a limited group of organizations. This model is commonly used by commercial enterprises, financial institutions, and government agencies that require both transparency and controlled access to data.

Key strengths and weaknesses

Blockchain technology possesses several key advantages that have driven its widespread adoption, including:

- Decentralization
- Immutability: Transactions recorded on the blockchain are verified by network participants and permanently stored in blocks.
- Transparency: Since all transactions are verified and timestamped, users can easily trace and audit historical records.
- Anonymity

Despite these advantages, a primary challenge facing blockchain technology is to provide enough transaction processing speed for large-scale applications [3]. For instance, the Bitcoin network can process approximately seven transactions per second, while Ethereum can handle around 15 transactions per second [4]. Table 1 presents a comparison of transaction speeds and confirmation times across various blockchain networks [5]. The widespread adoption of blockchain technology across industries depends largely on the development of scalable solutions that enhance transaction throughput.

TABLE 1. Transaction processing speed of different cryptocurrencies

Cryptocurrency	Transactions per Second	Average Transaction Confirmation Time
Bitcoin	3–7	60 min
Ethereum	15–25	6 min
Ripple	1500	4 s
Bitcoin Cash	61	60 min
Stellar	1000	2–5 s
Litecoin	56	30 min
Monero	4	30 min
IOTA	1500	2 min
Dash	10–28	15 min

Layer 1 solutions: sharding and consensus mechanisms

To enhance blockchain throughput, two primary approaches are employed: modifications to the underlying blockchain architecture (Layer 1, or L1) and Layer 2 (L2) solutions, which function as auxiliary technologies built on top of L1 blockchains.

A Layer 1 blockchain is a foundational blockchain that independently processes and finalizes transactions within its own network, without reliance on external systems. However, Layer 1 blockchains are subject to the blockchain trilemma, which posits that a blockchain must balance three core attributes: decentralization, security, and scalability. Improving one of these characteristics often compromises the others. Examples of Layer 1 blockchains include Bitcoin, Ethereum, BNB Smart Chain, Tron, Cardano, Solana, Aptos, and NEAR.

Several solutions have been proposed to enhance transaction throughput at the Layer 1 level, including sharding and modifications to the consensus mechanism, both of which aim to improve the efficiency of transaction validation and agreement among network participants.

Sharding involves partitioning a blockchain into smaller, more manageable segments, or shards, which can process transactions and execute smart contracts in parallel. By distributing computational workload across multiple shards, blockchain networks can significantly improve throughput while reducing latency and resource consumption. Unlike traditional blockchain architectures, where all nodes must process every transaction, sharding allows subsets of nodes to validate only a portion of the total transactions, thereby increasing scalability. For instance, if a network with 1,000 nodes is divided into 10 shards of 100 nodes each, transaction processing speed can increase approximately tenfold.

An example of sharding implementation is the NEAR Protocol, a Layer 1 blockchain that employs Nightshade, a unique sharding technology designed to enhance scalability. NEAR operates using smart contracts and employs a Proof-of-Stake (PoS) consensus mechanism. Its network is capable of processing up to 160,000 transactions per second (TPS), significantly outperforming many other blockchain platforms, including Solana.

Another fundamental approach to improving blockchain performance is the adoption of alternative consensus mechanisms, which impact transaction speed, security, and energy efficiency.

Proof of Work (PoW) is a transaction validation algorithm that relies on computational problem-solving, requiring network participants (miners) to perform complex cryptographic calculations. Since Bitcoin's launch in 2009, the Proof-of-Work (PoW) consensus algorithm has been focal in securing blockchain networks [6]. The difficulty of these computations ensures network security but also results in significant energy consumption and slow transaction processing times. For example, the Bitcoin network, which utilizes PoW, can only process approximately seven transactions per second.

PoW-based networks also impose substantial environmental costs due to the high energy consumption associated with mining operations. The requirement for specialized, high-performance computing hardware further increases the economic burden of maintaining network security.

An alternative consensus mechanism, Proof of Stake (PoS), does not require extensive computational power and significantly reduces transaction times, making it a more efficient solution than Proof of Work (PoW). In PoS, rather than solving cryptographic puzzles to find the correct nonce, as in PoW, users must demonstrate ownership of a certain number of digital tokens to participate in block validation.

However, PoS introduces a potential centralization risk, as users holding a large number of tokens may dominate the network, undermining its decentralization. To address this issue, several modifications to the block validator selection process have been developed. For instance, Blackcoin implements a randomization mechanism to predict the next block generator (node) [7]. This mechanism employs a formula designed to find the smallest hash value in combination with the stake size, ensuring a fairer selection

process. Additionally, in [8], an alternative approach is proposed in which nodes holding a larger number of older tokens have a higher probability of generating new blocks.

Empirical studies support the efficiency of PoS. An experimental analysis conducted in [9] demonstrated that PoS-based consensus mechanisms can achieve transaction finalization up to 40% faster than PoW-based systems while consuming significantly less energy.

Delegated Proof of Stake (DPoS) is a modified consensus mechanism that addresses the limitations of both PoW and PoS. Developed in 2014 as part of the Graphene project, DPoS was first implemented in the BitShares blockchain and later adopted by the Steemit platform [10, 11].

The key feature of DPoS is the separation of voting and validating nodes. In this system, network participants (token holders) do not directly validate transactions. Instead, they elect a subset of delegates, who are responsible for block formation and transaction validation. This distinction introduces a fundamentally different operational structure compared to PoW and PoS.

To serve as a validator in a DPoS network, nodes must publicly disclose their identity and commit to maintaining full-node functionality, ensuring timely transaction verification and block generation. Unlike PoW and PoS systems, DPoS allows users to simultaneously participate in voting while continuing to conduct transactions. Moreover, a participant's voting power dynamically adjusts in response to changes in their token balance, ensuring a more flexible and adaptive governance model.

So far, the discussion has focused on consensus protocols used in open blockchain systems, which operate in public environments and prioritize decentralization. However, these protocols are not well-suited for corporate applications, as they generally exhibit low transaction throughput.

To address these limitations, a new class of Byzantine Fault Tolerance (BFT) consensus protocols has been introduced. These protocols enhance blockchain scalability and performance by limiting the number of participants involved in transaction validation.

Practical Byzantine Fault Tolerance (PBFT) is a consensus mechanism in which anonymity is not a critical factor. Instead, nodes within the network possess partial knowledge of each other and undergo authentication. This structural difference enables significant optimization of the consensus process, leading to much higher transaction throughput. In fact, PBFT-based systems can achieve speeds ten times faster than traditional PoW or PoS mechanisms, processing thousands of transactions per second – making them well-suited for corporate applications.

The PBFT protocol operates as follows:

- A validator node receives a transaction and must determine its validity.
- The validator performs internal verification procedures.
- It then queries other nodes within the network to confirm whether the transaction is valid.
- If at least 2/3 of the nodes reach consensus on the transaction’s validity, it is accepted and propagated to the blockchain network.

It is also important to note that PBFT does not rely on hashing procedures for block validation, which further reduces computational overhead and increases efficiency [12].

Delegated Byzantine Fault Tolerance (DBFT) is an extension of PBFT, designed to accommodate large-scale blockchain networks while maintaining high throughput. The algorithm was developed by the NEO blockchain team, led by Erik Zhang, and was first implemented in the NEO project in 2016 [13].

In DBFT, crypto-token holders elect specific nodes to serve different roles in the consensus process. These nodes are categorized into:

- Speaker nodes, which are responsible for conducting transactions and forming new blocks.
- Delegate nodes, which verify transactions proposed by speaker nodes and participate in the consensus process.

This hierarchical structure enhances network security and scalability, making DBFT a viable alternative for enterprise blockchain applications. However, one potential drawback of DBFT is the risk of centralization. If a majority of validating nodes are controlled by a single entity or a small group, the network's decentralization may be compromised [14].

The Federated Byzantine Agreement (FBA) is a consensus protocol that differs from Practical Byzantine Fault Tolerance (PBFT) and other Byzantine Fault Tolerance (BFT) variations in that it does not require prior authorization or a predefined set of participants. Instead, transactions are verified by a fixed number of participants selected from a list of active nodes in the network.

A key feature of FBA is the presence of gateways and market makers, which help maintain the integrity and liquidity of the network:

- Gateways function similarly to traditional banks, holding funds and issuing equivalent digital tokens.
- Market makers maintain accounts across multiple gateways and currencies, ensuring liquidity and facilitating seamless transactions [15].

The XRP Ledger Consensus Protocol is the consensus mechanism used in the XRP Ledger network, designed to achieve agreement between participating servers without requiring mining. Transactions in this protocol are validated by specialized nodes called validators. Once a majority of validators reach consensus, the transaction is confirmed and added to the ledger.

This consensus algorithm was developed by Ripple Labs Inc. and was first introduced in 2012 [16].

The XRP Ledger consists of:

- Tracking servers, which distribute transactions and respond to state queries.
- Validators, which process transactions and ensure consistency across the distributed ledger.

This structure enables efficient transaction processing while maintaining network decentralization.

In 2020, a novel probabilistic consensus algorithm known as Proof of Elapsed Work and Luck (PoEWAL) was introduced. This lightweight algorithm allows all nodes in a blockchain network to participate in the consensus process. PoEWAL is derived from the Proof of Work (PoW) consensus model but is optimized for efficiency and reduced computational overhead [17].

Shekhar Verma et al. [18] proposed the PoEWAL algorithm for non-cooperative blockchain environments, particularly for applications in Internet of Things (IoT) networks.

In 2022, Hongwu Qin et al. [19] introduced the Weighted Byzantine Fault Tolerance (WBFT) consensus algorithm, specifically designed for consortium blockchains. WBFT employs a dynamic weighting mechanism to optimize consensus node selection.

Experimental performance evaluations of WBFT, compared with PBFT and Reputation-Based Byzantine Fault Tolerance (RBFT), demonstrated that WBFT improves both system throughput and consensus delay, making it a promising alternative for high-performance blockchain applications.

Each consensus protocol discussed above has its own advantages and limitations. A comparative analysis of these consensus mechanisms, detailing their performance characteristics, scalability, and security features, is presented in Table 2 [20, 21].

Layer 2 solutions

To enhance blockchain throughput and scalability, various Layer 2 (L2) solutions have been developed. These solutions act as external integrations with the base layer (Layer 1, L1) and help address performance limitations while maintaining security.

The primary Layer 2 scaling solutions include:

1. State Channels

State channels enable off-chain transaction exchanges between participants, significantly reducing network congestion. Transactions occur outside the blockchain through third-party channels, and only the

final state is recorded on the main blockchain. This approach improves transaction speed and reduces transaction costs.

Examples:

- Lightning Network (Bitcoin) – Facilitates near-instant, low-cost Bitcoin transactions.
- Raiden Network (Ethereum) – Implements off-chain scaling solutions for Ethereum, allowing faster transactions with minimal fees.

TABLE 2. Comparative analysis of consensus protocols

Consensus protocol	Type of blockchain network	Productivity	Cost of energy	Decentralisation	Developed solutions
PoW	Public	Low	High	High	Bitcoin-NG, Byzcoin, Bitcoin
PoS	Public	High	Low	High	Tendermint, Ethereum
DPoS	Public	High	Low	Low	EOS , BitShares
BFT	Private	High	Low	Low	Hyperledger Fabric 1.0
PBFT	Private with permits	High	Low	Low	Hyperledger, Chain
DBFT	Private	Very high	Low	Low	NEO , TON
FBA	Private	High	Low	Low	Stellar
XRP	Private	High	Low	Low	Ripple
PoEWAL	Private	High	Low	Low	For IoT apps
WBFT	Private	High	Low	Low	

3. Sidechains

Sidechains are independent blockchains that operate alongside the main blockchain, with a two-way peg ensuring interoperability. These separate networks have their own consensus mechanisms, allowing increased scalability and transaction processing without overloading the main blockchain.

Examples:

- Polygon (Matic) – A widely used Ethereum-compatible sidechain.
- xDai – A stablecoin-based sidechain for fast and low-cost transactions.
- Ronin – A sidechain optimized for blockchain-based gaming applications.

A review of existing literature suggests that all the aforementioned Layer 2 scaling techniques are designed to improve blockchain transaction throughput and address scalability challenges. Each method has distinct advantages and trade-offs, making them suitable for different use cases within the blockchain ecosystem.

Ongoing research into blockchain scalability and performance enhancement has led to several novel approaches, including transaction model optimizations, dynamic sharding techniques, and modifications to consensus algorithms.

The study presented in [22] introduces a Dual Channel Parallel Broadcast (DCPB) transaction model, which incorporates three key innovations:

- Dual channel communication – One channel is dedicated to transaction processing, while the second executes Byzantine Fault Tolerant (BFT) consensus mechanisms.
- Parallel pipeline processing – Allows asynchronous execution, improving throughput.
- Optimized block broadcast strategies – Enhances efficiency and transaction propagation speed.

• Extensive experimental evaluations using BeihangChain, a prototype blockchain system, demonstrate that the proposed model can achieve a transaction processing speed of up to 16,000 transactions per second (TPS).

A novel PolyShard architecture is proposed in [23], designed to improve security, throughput, and storage scalability. Unlike traditional unencoded shard storage methods, PolyShard employs: encoded shards – created by linearly combining multiple unencoded shards of equivalent size; optimized throughput and latency – constrained only by the physical limitations of the network layer, ensuring efficient transaction processing. This approach enables high transaction throughput while maintaining security and reducing storage requirements.

A dynamic shard allocation process is proposed in [24], which dynamically assigns transactions to shards based on the sender's data. Key features include: adaptive shard allocation – adjusts the shard assignment based on network conditions; snakechain optimization algorithm (SOA) – Determines the optimal number of shards required to minimize latency while maximizing efficiency. Experimental results indicate significant reductions in latency, demonstrating that the optimized system achieves lower average transaction times across various transaction volumes.

Modifying consensus algorithms is another critical area of blockchain research, aiming to enhance scalability and transaction processing efficiency.

The study in [5] proposes a method to accelerate the Proof of Work (PoW) process through:

• Parallel mining – A distributed mining approach that allows multiple miners to contribute to block validation simultaneously.

• Equal participation – Ensures fairness among miners, balancing computational power and increasing network scalability.

Results indicate that as the network complexity and number of miners increase, parallel PoW significantly improves blockchain scalability compared to traditional PoW mechanisms.

In [25], researchers introduce a hybrid consensus mechanism combining: Proof of Stake (PoS) can be used for verifiable pseudo-random node selection and Practical Byzantine Fault Tolerance (PBFT) can be applied for efficient transaction validation. The proposed two-stage strategy optimizes throughput, delay, and scalability by reducing the number of consensus nodes to a constant value while ensuring network security and efficiency.

A novel particle swarm optimization-based Proof of Work (PSO-PoW) model is proposed in [26], incorporating:

• Automatic miner selection – Uses particle swarm optimization (PSO) algorithms to dynamically select the most optimal block manager.

• Scalability improvements – Reduces waiting times by ensuring that unresponsive miners are automatically replaced.

• Optimized reward system – Implements an intelligent work allocation mechanism to improve mining efficiency.

This approach effectively addresses blockchain scalability challenges while maintaining decentralization and security.

Conclusion

This study presents a generalized overview of the current state of blockchain technology development, including a comparative analysis of blockchain networks and consensus protocols.

Layer 1 (L1) solutions enhance the fundamental parameters of blockchain systems; however, without radical architectural changes, they cannot achieve global scalability. Layer 2 (L2) solutions address challenges related to transaction speed and fees but require high reliability to function effectively. The integration of L1 and L2 solutions is key to the development of high-performance blockchain systems.

Despite advancements, existing consensus algorithms still suffer from performance bottlenecks, including:

1. Low throughput and high latency
2. Unstable performance under varying network conditions
3. Resilience issues and vulnerability to targeted attacks

The combination of optimized consensus mechanisms and machine learning techniques introduces new possibilities for blockchain evolution. These innovations can accelerate transaction processing, reduce energy consumption, and enhance network security. In the future, the development of hybrid consensus algorithms and AI-driven predictive models may lead to widespread blockchain adoption across diverse industries.

Author's contributions: D. Dvorchuk – research, conceptualization, methodology, formal analysis, writing – original draft. I. Shpinareva – generalization, resources, editing.

References

1. Bai C.A., Sarkis J., Xue W. Improving operational efficiency and effectiveness through blockchain technology. *Prod Plan Control*. 2024. **35**. P. 857–865. https://doi.org/10.1080/09537287.2024.2329182
2. Chowdhury R.H. Automating supply chain management with blockchain technology. *World J Adv Res Rev*. 2024. **22** (3). P. 1568–1574. https://doi.org/10.30574/wjarr.2024.22.3.1895
3. Bennet D., Maria L., Sanjaya Y.P.A., Zahra A.R.A. Blockchain technology: revolutionizing transactions in the digital age. *ADI J Recent Innov*. 2024. **5** (2). https://doi.org/10.34306/ajri.v5i2.1065
4. Morillon T. Bitcoin's value proposition: shorting expansionary monetary policies. *Stud Econ Finance*. 2022. **39** (1). P. 20–44. https://doi.org/10.1108/SEF-03-2021-0107
5. Hazari S.S., Mahmoud Q.H. Improving transaction speed and scalability of blockchain systems via parallel proof of work. *Future Internet*. 2020. **12** (8). 125. https://doi.org/10.3390/fi12080125
6. Ahn J., Yi E., Kim M. Blockchain consensus mechanisms: a bibliometric analysis (2014–2024) using VOSviewer and R Bibliometrix. *Information*. 2024. **15** (10). 644. https://doi.org/10.3390/info15100644
7. Vasin P. Blackcoin's proof-of-stake protocol v2. Whitepaper.io; 2018. https://blackcoin.org/blackcoin-pos-protocol-v2-whitepaper.pdf (accessed: 07.03.2025)
8. King S., Nadal S. Peercoin: peer-to-peer cryptocurrency with proof-of-stake. Self-published paper; 2012. https://peercoin.net/assets/paper/peercoin-paper.pdf (accessed: 07.03.2025)
9. Kushwaha S.S., Joshi S., Singh D., Kaur M., Lee H.N. Systematic review of security vulnerabilities in Ethereum blockchain smart contracts. *IEEE Access*. 2022. **10**. P. 6605–6621. https://doi.org/10.1109/ACCESS.2021.3140091
10. Yang F., Zhou W., Wu Q., Long R., Xiong N., Zhou M. Delegated proof of stake with downgrade: a secure and efficient blockchain consensus algorithm with downgrade mechanism. *IEEE Access*. 2019. **7**. P. 118541–118555. https://doi.org/10.1109/ACCESS.2019.2935149
11. Ozisik P., Andresen G., Bissias G., Houmansadr A., Levine B. Graphene: a new protocol for block propagation using set reconciliation. In: Data Privacy Management, Cryptocurrencies and Blockchain Technology. 2017. P. 420–428. https://doi.org/10.1007/978-3-319-67816-0_24
12. Sukhwani H., Martínez M., Chang X., Trivedi S., Rindos A. Performance modeling of PBFT consensus process for permissioned blockchain networks (Hyperledger Fabric). *Proc IEEE 36th Symp Reliab Distrib Syst (SRDS)*. 2017. P. 253–255. https://doi.org/10.1109/SRDS.2017.36
13. Gao S., Yu T., Zhu J., Cai W. T-PBFT: an EigenTrust-based practical Byzantine fault tolerance consensus algorithm. *China Commun*. 2019. **16** (12). P. 111–123. https://doi.org/10.23919/JCC.2019.12.008
14. Wang Q., Yu J., Peng Z., Bui C., Chen S., Ding Y. Security analysis on DBFT protocol of NEO. In: *Proc Int Conf Financial Cryptography Data Security*. 2020. P. 20–31. https://doi.org/10.1007/978-3-030-51280-4_2
15. Mazieres D. The stellar consensus protocol: a federated model for internet-level consensus [Internet]. Stellar Development Foundation, 2015. https://johnpconley.com/wp-content/uploads/2021/01/stellar-consensus-protocol.pdf (accessed: 07.03.2025)
16. Chase B., MacBrough E. Analysis of the XRP ledger consensus protocol. Cornell University, 2018. https://arxiv.org/abs/1802.07242 (accessed: 07.03.2025)

17. Upadhyay V., Vaish A., Kokila J. The need for lightweight consensus algorithms in IoT environment: a review. *Proc 16th Int Conf Contemp Comput (IC3-2024)*. Noida, India. 2024. https://doi.org/10.1145/3675888.3676072
18. Raghav N., Andola N., Venkatesan S., Verma S. PoEWAL: a lightweight consensus mechanism for blockchain in IoT. *Pervasive Mobile Comput*. 2020. **69**. 101291. https://doi.org/10.1016/j.pmcj.2020.101291
19. Qin H., Cheng Y., Ma X., Li F. Weighted Byzantine fault tolerance consensus algorithm for enhancing consortium blockchain efficiency and security. *J King Saud Univ Comput Inf Sci*. 2022. **34** (5). https://doi.org/10.1016/j.jksuci.2022.08.017
20. Gol D.A., Gondaliya N. Blockchain: a comparative analysis of hybrid consensus algorithm and performance evaluation. *Comput Electr Eng*. 2023. https://doi.org/10.1016/j.compeleceng.2023.108934
21. Sayeed S., Marco-Gisbert H. Assessing blockchain consensus and security mechanisms against the 51% attack. *Appl Sci*. 2019. **9**. https://doi.org/10.3390/app9091788
22. Feng L., Zhang H., Tsai W.T., Sun S. System architecture for high-performance permissioned blockchains. *Front Comput Sci*. 2019. **13** (3). P. 1–15. https://doi.org/10.1007/s11704-018-6345-4
23. Li S., Yu M., Yang C.S., Avestimehr S. PolyShard: coded sharding achieves linearly scaling efficiency and security simultaneously. *IEEE Trans Inf Forensics Secur*. 2020. **16**. P. 249–261. https://doi.org/10.1109/TIFS.2020.3009610
24. Shimal S., Ameen S.Y., Ahmed J.A. Enhancing blockchain scalability with snake optimization algorithm: a novel approach. *Front Blockchain*. 2024. https://doi.org/10.3389/fbloc.2024.1361659
25. Wu Y., Song P., Wang F. Hybrid consensus algorithm optimization: a mathematical method based on POS and PBFT and its application in blockchain. *Math Probl Eng*. 2020. **11**. P. 1–13. https://doi.org/10.1155/2020/7270624
26. Saqib N.A., AL-Tall S.T. Scaling up security and efficiency in financial transactions and blockchain systems. *J Sens Actuator Netw*. 2023. **12** (2). 31. https://doi.org/10.3390/jsan12020031

Received 07.03.2025

Dvorchuk Danylo Serhiyovych,
postgraduate student, department of Mathematical Support of Computer Systems,
Odessa I.I. Mechnikov National University,
https://orcid.org/0009-0006-4487-0499
dvorchyk.d@gmail.com

Shpinareva Iryna Mykhailivna,
Candidate of Physical and Mathematical Sciences,
Associate Professor of the Department of Mathematical Support of Computer Systems,
Odessa I.I. Mechnikov National University.
https://orcid.org/0000-0001-9208-4923

UDC 004.75

Danylo Dvorchuk [*], Iryna Shpinareva

Analysis of Blockchain-Technology

Odessa I. I. Mechnikov National University
[*] *Correspondence: dvorchyk.d@gmail.com*

Introduction. Blockchain technology has emerged as a transformative innovation in distributed computing, providing a secure, transparent, and decentralized mechanism for data management. Initially introduced as the backbone of cryptocurrencies, blockchain has expanded into various sectors, including finance, healthcare, supply chain management, and governance. However, despite its numerous advantages, blockchain faces significant challenges, including scalability, transaction speed, and energy consumption. This article presents a comprehensive analysis of blockchain technology, focusing on its classification, consensus mechanisms, scalability solutions, and future trends. The study explores the comparative advantages and limitations of different blockchain architectures and evaluates emerging optimization techniques such as hybrid consensus algorithms and artificial intelligence-based enhancements.

Purpose of the Work. The objective of this study is to conduct an in-depth analysis of blockchain technology, investigating its core principles, operational mechanisms, and performance optimization strategies. The research aims to provide a systematic comparison of consensus algorithms, including Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), and Byzantine Fault Tolerance (BFT) variations, assessing their impact on transaction speed, energy efficiency, and security. Additionally, the study examines Layer 1 (L1) and Layer 2 (L2) scaling solutions such as sharding, rollups, and sidechains to address blockchain's scalability challenges. The research also highlights emerging trends in blockchain development, particularly hybrid models and AI-driven optimization techniques, which can enhance blockchain efficiency and security.

Results. The analysis reveals that different blockchain architectures exhibit varying trade-offs between decentralization, security, and scalability. Public blockchains, such as Bitcoin and Ethereum, prioritize decentralization and security but suffer from limited scalability. Private blockchains, in contrast, offer higher transaction throughput but compromise decentralization. Hybrid blockchains aim to balance these aspects by integrating the strengths of both models. A detailed comparison of consensus mechanisms indicates that PoW, while highly secure, is energy-intensive and slow, whereas PoS and its variations provide faster and more energy-efficient alternatives. The study also finds that Byzantine Fault Tolerance-based mechanisms, such as PBFT and DBFT, offer high-speed consensus suitable for enterprise applications. Furthermore, Layer 1 improvements, including sharding, enhance on-chain transaction processing, while Layer 2 solutions, such as optimistic rollups and zero-knowledge rollups, significantly increase throughput by offloading computations to secondary layers. The research highlights recent advancements, such as AI-assisted transaction validation and adaptive consensus algorithms, as promising directions for blockchain scalability and security.

Conclusions. The study underscores the importance of optimizing blockchain scalability and consensus mechanisms to enable broader adoption across industries. While Layer 1 and Layer 2 solutions provide significant improvements in throughput and efficiency, their integration remains a key challenge. The findings suggest that hybrid consensus models and AI-based optimizations could further enhance blockchain performance, reducing energy consumption while maintaining security and decentralization. Future research should focus on developing dynamic sharding techniques, parallel consensus mechanisms, and predictive analytics for transaction management to advance blockchain's applicability in large-scale real-world scenarios. The continued evolution of blockchain technology will play a critical role in shaping secure, efficient, and decentralized digital ecosystems.

Keywords: blockchain, decentralization, consensus mechanisms, optimistic rollups, sharding, transaction validation.

УДК 004.75

Д.С. Дворчук [*], І.М. Шпінарева

Аналіз блокчейн-технології

Одеський національний університет імені І.І. Мечникова
[*] Листування: dvorchyk.d@gmail.com

Вступ. Технологія блокчейн стала революційним досягненням у сфері розподілених обчислень, надаючи безпечний, прозорий і децентралізований механізм управління даними. Спочатку представлена як основа для криптовалют, технологія блокчейн згодом також знайшла своє застосування у ряді інших галузей, включаючи фінанси, охорону здоров'я, управління ланцюгами постачання та державне управління. Однак, незважаючи на численні переваги, технологія блокчейн стикається з серйозними викликами, такими як масштабованість, швидкість обробки транзакцій і споживання енергії. У цій статті представлено комплексний аналіз блокчейн-технології, зосереджений на її класифікації, механізмах консенсусу, рішеннях щодо масштабованості та майбутніх тенденціях. Дослідження розглядає порівняльні переваги та обмеження різних блокчейн-архітектур, а також оцінює перспективні методи оптимізації, зокрема гібридні алгоритми консенсусу та вдосконалення на основі штучного інтелекту.

Мета роботи. Проведення глибокого аналізу блокчейн-технології, дослідження її основних принципів, операційних механізмів та стратегій оптимізації продуктивності. Дослідження спрямоване на надання систематичного порівняння алгоритмів консенсусу, включаючи Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS) та варіації Byzantine Fault Tolerance (BFT), оцінюючи їх вплив на швидкість транзакцій, енергоефективність та безпеку. Крім того, у дослідженні розглядаються рішення для масштабування першого (L1) та другого (L2) рівнів, такі як шардинг, ролапи та сайдчейни, для вирішення проблем масштабованості блокчейну. Також висвітлюються перспективні тенденції розвитку блокчейну, зокрема гібридні моделі та оптимізаційні методи на основі штучного інтелекту, які можуть підвищити ефективність і безпеку блокчейну.

Результати. Аналіз показує, що різні блокчейн-архітектури мають відмінні компроміси між децентралізацією, безпекою та масштабованістю. Публічні блокчейни, такі як Bitcoin і Ethereum, надають пріоритет децентралізації та безпеці, але мають обмежену масштабованість. Приватні блокчейни, навпаки, забезпечують вищу пропускну здатність обробки транзакцій, але поступаються у децентралізації. Гібридні блокчейни прагнуть збалансувати ці аспекти, інтегруючи переваги обох моделей. Детальне порівняння механізмів консенсусу показує, що PoW, хоча і дуже безпечний, є енергоємним та повільним, тоді як PoS та його варіації забезпечують швидші та більш енергоефективні альтернативи. Дослідження також виявило, що механізми, засновані на Byzantine Fault Tolerance, такі як PBFT і DBFT, забезпечують високу швидкість консенсусу, що робить їх придатними для корпоративних застосувань. Крім того, таке Layer 1 рішення як шардинг, суттєво підвищує ефективність обробки транзакцій у ланцюзі, а рішення Layer 2, такі як оптимістичні ролапи та Zero-Knowledge ролапи, значно збільшують пропускну здатність, знижуючи навантаження на основний блокчейн. Дослідження також підкреслює останні досягнення, такі як валідація транзакцій за допомогою штучного інтелекту та адаптивні алгоритми консенсусу, як перспективні напрями розвитку масштабованості та безпеки блокчейну.

Висновки. Дослідження підкреслює важливість оптимізації масштабованості блокчейну та механізмів консенсусу для розширення його застосування в різних галузях. Хоча рішення Layer 1 та Layer 2 забезпечують значні покращення у пропускній здатності та ефективності, їх інтеграція залишається ключовою проблемою. Отримані результати свідчать про те, що гібридні моделі консенсусу та оптимізації на основі штучного інтелекту можуть ще більше підвищити продуктивність блокчейну, зменшуючи споживання енергії та дотримуючись принципів безпеки та децентралізації. Майбутні дослідження повинні зосередитися на розробці динамічних технік шардингу, паралельних механізмів консенсусу та прогнозної аналітики для управління транзакціями, щоб покращити застосовність блокчейну у великих реальних сценаріях. Подальший розвиток блокчейн-технології відіграватиме вирішальну роль у формуванні безпечних, ефективних та децентралізованих цифрових екосистем.

Ключові слова: блокчейн, децентралізація, механізми консенсусу, оптимістичні роллапи, шардинг, валідація транзакцій.