Universal Library of Engineering Technology Research Article

ISSN: 3064-996X | Volume 2, Issue 1

Open Access | PP: 43-48

DOI: https://doi.org/10.70315/uloap.ulete.2025.0201008

# Approaches to Security in Distributed Applications

**Artem Iurchenko**

Senior Software Engineer at Dexian, Atlanta, USA.

## Abstract

*The article examines security approaches in distributed applications (dApps) based on blockchain technologies and related decentralized systems. The primary focus is on existing consensus algorithms (PoW, PoS, DPoS, pBFT, PoA, and Casper) and their limitations, as well as vulnerabilities associated with double-spending and other forms of cyber threats. To enhance resilience and adaptability, a hybridization approach to consensus mechanisms (DPoSW, PoSW, PoCASBFT, DBPoS, etc.) is proposed, integrating the best features of multiple protocols. Additionally, the role of machine learning (ML) methods in dynamic anomaly detection and threat prediction is explored, enabling timely responses to cyberattacks and network parameter optimization. The practical section of the article describes the methodology for deploying an experimental network on the ProximaX platform, which combines decentralized storage, a smart contract layer, and a blockchain ledger. The results of simulating various attacks, including the 51% attack, and analyzing metrics such as network throughput, block confirmation time, and anomaly detection accuracy are presented. Experiments demonstrate that the hybridization of consensus algorithms, combined with ML modules, improves overall security and system scalability, albeit at the cost of additional computational resources. The conclusion highlights future research directions, including the expanded application of reinforcement learning methods, the development of more energy-efficient ML models, and the implementation of advanced privacy-preserving techniques. Approaches to security in distributed applications are of interest to researchers and practitioners specializing in interdisciplinary analyses of information security, distributed computing systems, and cryptographic protocols.*

**Keywords:** *Hybrid Consensus Algorithms, Machine Learning, Blockchain, 51% Attacks, Distributed Applications, Network Security, Anomaly Detection.*

## INTRODUCTION

In recent years, the use of distributed applications (dApps) has significantly increased, covering areas such as smart energy grids, healthcare systems, the financial sector, and supply chain management. Alongside this growth, the risk of cyberattacks has also risen.

Oyinloye D. P. et al. [1] provide a comprehensive analysis of alternative consensus protocols, emphasizing the trade-off between transaction processing speed and security levels. Lashkari B. and Musilek P. [11], along with Wang W. et al. [17] and Xiao Y. et al. [19; 23], identify key scalability and reliability challenges in distributed systems. Based on these studies, it can be concluded that existing approaches often struggle with adapting to increasing loads and evolving cyber threats, highlighting a research gap in developing unified models that integrate high security with performance efficiency.

Wang B., Li Z., and Li H. [2] propose a hybrid algorithm combining a modified proof-of-probability mechanism with delegated proof of stake (DPoS). Wu Y., Song P., and Wang F. [6] introduce mathematical optimization that integrates elements of Proof of Stake (PoS) and the practical byzantine fault tolerance (pBFT) algorithm. The contribution of Buterin V., Reijsbergen D., Leonardos S., and Piliuras G. [7] focuses on analyzing incentive mechanisms in the hybrid Casper protocol, emphasizing the importance of economic incentives for security. Additional modifications of DPoS presented by Bachani V. and Bhattacharjya A. [5], along with Chen S. et al. [8], and the use of enhanced consensus mechanisms in collective network opinion governance proposed by Chen Y. and Liu F. [20], reflect a growing trend toward balancing scalability, transaction speed, and security. The low communication complexity in the dual-layer pBFT model proposed by Feng C. et al. [12] and the adaptation of the algorithm for scalable traceability suggested by Liu S. et al. [14] contribute to the research novelty in improving the efficiency of consensus mechanisms.

Hu Y. et al. [9] develop a practical «heartbeat»-based security scheme to counter cloning attacks in Power of Attorney (PoA)

**Citation:** Artem Iurchenko, "Approaches to Security in Distributed Applications", Universal Library of Engineering Technology, 2025; 2(1): 43-48. DOI: https://doi.org/10.70315/uloap.ulete.2025.0201008.

-based systems, demonstrating the application of specialized security methods in networks with a limited trust model. Saad M. et al. [15] propose mempool optimization as a defense against Distributed Denial of Service (DDoS) attacks in Proof of Work (PoW) systems, addressing the resilience of network infrastructure. The work of Liu D. et al. [13] on the development of an anonymous reputation system for IoT solutions using a PoS blockchain highlights the integration of privacy and trust aspects in distributed applications. The application of machine learning techniques for trust assurance in edge networks, demonstrated by Xiao L. et al. [24], and the concept of a hybrid crowdsourcing platform utilizing zero-knowledge proof mechanisms (zkCrowd) described by Zhu S. et al. [25], indicate that combining adaptive algorithms with advanced cryptographic methods can significantly enhance security and trust in distributed systems. The review by Shafay M. et al. [3] on the application of blockchain technology in deep neural networks underscores the need for further research into the integration of artificial intelligence methods for dynamic system protection.

Sapra N., Shaikh I., and Dash A. [16] conduct a systematic analysis of the environmental impact of PoW applications, revealing significant ecological constraints of traditional algorithms. Andoni M. et al. [21], in a review of blockchain applications in the energy sector, discuss both the challenges and opportunities for securing distributed energy systems, while Meland P. H. et al. [22] use systematic cybersecurity data mapping to highlight the necessity of developing universal security assessment indicators.

The studies of Khobragade P. and Turuk A. K. [4], along with the research of Wood G. et al. [18], provide large-scale reviews comparing and systematizing various consensus mechanisms. The authors examine both traditional methods based on proof of work and more modern approaches, including proof of stake and hybrid solutions aimed at improving fault tolerance and scalability in distributed systems.

The work of Kiayias A. et al. [10] presents a deep formal approach to security, introducing the Ouroboros protocol, which possesses provable cryptographic properties within the proof-of-stake model.

Despite significant advancements in the development and optimization of consensus algorithms for securing distributed applications, the literature reveals contradictions in achieving a balance between scalability, transaction speed, and security levels. Additionally, the integration of artificial intelligence methods into adaptive security systems and the environmental impact of PoW blockchains remain insufficiently explored, necessitating further empirical research and the development of more comprehensive models.

The objective of this study is to consolidate a hybrid approach to security in distributed systems, combining the advantages of multiple consensus algorithms and machine learning techniques.

The scientific novelty of this research lies in the proposed methodology for hybridizing consensus algorithms with machine learning integration for dynamic predictive threat analysis. This enables adaptive network parameter management, reducing cyberattack risks and enhancing the security of distributed applications.

The research hypothesis suggests that the use of machine learning for predictive threat and anomaly analysis, combined with hybrid consensus algorithms, can significantly improve the security of distributed applications, minimizing the likelihood of 51% attacks and transaction manipulation.

This study employs a comprehensive methodology:

1. Theoretical analysis of scientific literature and existing consensus mechanisms (Proof of Work, Proof of Stake, pBFT, PoA, etc.).
2. Description of a hybrid architecture incorporating machine learning (ML) modules for anomaly detection and a blockchain platform (ProximaX or similar) to test the combination of multiple consensus protocols.
3. Comparative analysis of key performance metrics (throughput, latency, decentralization degree, attack detection accuracy) against existing solutions.

## RESEARCH RESULTS

In distributed systems, particularly blockchain platforms, consensus plays a key role in maintaining a consistent state of the ledger across multiple nodes [1, 4]. Figure 1 below illustrates the core components underlying consensus mechanisms.

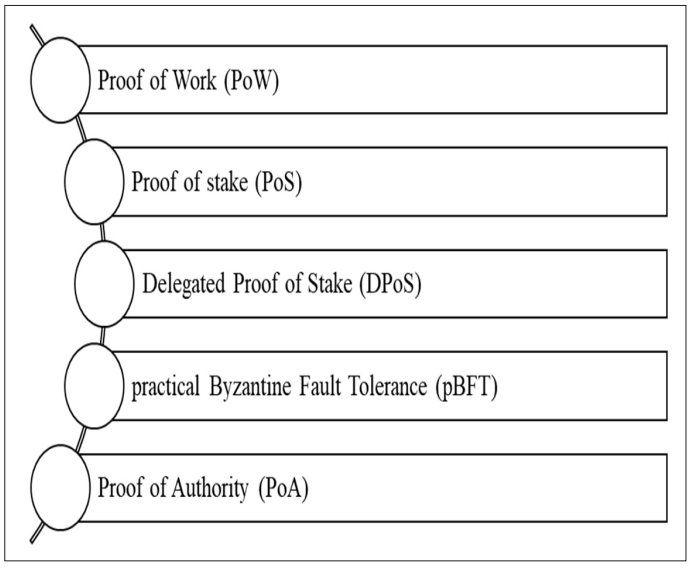


**Fig.1.** Components of consensus mechanisms

Proof of Work (PoW) is one of the earliest consensus algorithms, implemented in the Bitcoin network. Miner nodes solve complex cryptographic puzzles (hashing), competing for the right to add a new block. This approach ensures strong resistance to transaction history modifications, as an attacker would need to control substantial computational power to rewrite the blockchain [3].

Instead of computational power, PoS validators are selected based on their «stake» in the network [10]. This reduces energy consumption and accelerates transaction confirmation [11].

In DPoS, users delegate validation rights to elected «delegates,» which speeds up the consensus process by allowing blocks to be created and confirmed within a limited group of validators [5]. This results in higher transactions per second (TPS) and lower latency [6].

pBFT is a consensus algorithm used in distributed systems to reach agreement among nodes even in the presence of faulty or malicious nodes [2]. Such nodes may attempt to disrupt or compromise the system by spreading false or distorted information, conducting denial-of-service attacks, or distributing malicious code. This behavior degrades service quality and threatens data integrity. It is modeled using probabilistic and stochastic methods to predict potential attack vectors and assess system risks. The model incorporates trust evaluation between nodes and temporal anomaly analysis, combining elements of information theory, cryptography, and game theory.

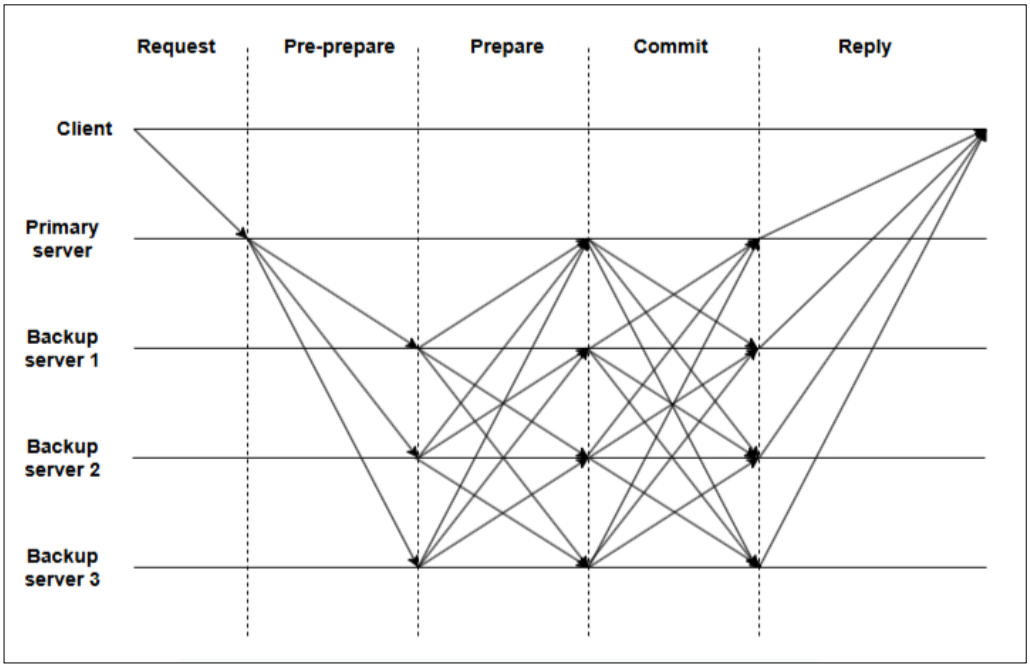


**Fig.2.** The operating principle of pBFT [22]

As shown in Figure 2, the primary node changes in each consensus round, with all nodes voting to select a new primary node.

Proof of Authority (PoA) relies on a small group of pre-approved validators with verified «reputation.» This ensures high performance, low transaction costs, and simplified administration, making it suitable for private or consortium blockchains [17, 18].

Across all described consensus mechanisms, a significant threat comes from attacks in which an adversary gains control over more than half of the resources determining consensus (hashing power, stake, etc.) [2, 10].

The execution of a 51% attack becomes easier in centralized conditions (large mining pools, a limited number of validators). Hybrid algorithms (such as PoSW, DPoSW, PoCASBFT) are mentioned in several studies as a way to further complicate such attack scenarios, requiring an attacker to simultaneously control multiple resource types [2, 5].

Table 1 presents a comparative analysis of major consensus algorithms, highlighting their strengths and vulnerabilities.

**Table 1.** Comparative analysis of common consensus algorithms [2, 5, 8, 10].

| Algorithm | Strengths | Main Vulnerabilities |
|---|---|---|
| PoW | - High level of decentralization - Resistance to history modifications | - High energy consumption - Risk of mining pool centralization - Susceptibility to 51% attacks |
| PoS | - Lower energy consumption - Faster block confirmation | - “Nothing at Stake” issue - Centralization of large stakes - Vulnerability to price volatility attacks |
| DPoS | - High speed and throughput - Simplified participation | - Centralization through delegates - Risk of collusion and vote buying - Low voter participation |
| pBFT | - Fast finality - High resistance to Byzantine failures | - Poor scalability - 1/3 faulty node limitation - Complex communication overhead |

| | | |
|---|---|---|
| PoA | - High performance - Low transaction costs - Suitable for consortiums | - Centralized trust in validators - Lack of incentives - Vulnerability if validators are compromised |
| Casper | - Fast finalization - Stake-slashing mechanisms | - Complexity in parameter selection - Risk of false penalties - Tendency toward centralization |

Thus, no single "ideal" algorithm exists for all scenarios. In practical applications, a combination (hybridization) of multiple mechanisms is relevant, leveraging their strengths while balancing weaknesses. Special emphasis is placed on integrating machine learning (ML) techniques for proactive threat detection and intelligent consensus parameter management, which will be discussed in detail in the following sections of the article.

## Hybrid Consensus Algorithms and Machine Learning Integration

The previous section examined classical consensus mechanisms (PoW, PoS, DPoS, pBFT, PoA, Casper) and their vulnerabilities. However, modern trends indicate that to enhance reliability and scalability, hybridization of algorithms (combining elements of multiple protocols) is often required, along with the integration of machine learning (ML) methods that enable timely anomaly detection, cyberattack prevention, and dynamic network parameter adaptation to changing conditions [2, 5].

Hybridization of consensus refers to the combination of the strengths of multiple protocols (e.g., PoW + PoS, DPoS + pBFT) to compensate for their individual weaknesses [7, 9]. For instance, merging Proof of Work (PoW) and Proof of Stake (PoS) results in a scheme conventionally called Proof of Stake and Work (PoSW), while combining Delegated Proof of Stake (DPoS) and PoW leads to Delegated Proof of Stake Work (DPoSW) [5]. Similarly, integrating Casper and pBFT is often referred to in the literature as PoCASBFT, while a mechanism combining DPoS and practical Byzantine fault tolerance (pBFT) may be denoted as DBPoS [2, 12].

The key idea is to create an adaptive «consensus layer» that considers not only the internal state of the ledger but also external signals such as network load, the probability of collusion, node behavior, and other factors.

To demonstrate the potential of hybrid algorithms with ML integration, four examples are presented in Table 2. These illustrate different ways to integrate PoW, PoS, pBFT, DPoS, and ML modules.

**Table 2.** Examples of hybrid consensus algorithms with integrated ML modules [2, 5, 8, 9, 13].

| Hybrid Model | Components | Key Integration Ideas | Advantages |
|---|---|---|---|
| DPoSW | DPoS + PoW + ML | - PoW generates new blocks - DPoS validates - ML module predicts network load and detects suspicious patterns | - High throughput - Reduced risk of 51% attacks - Adaptive mining complexity |
| PoSW | PoS + PoW + ML | - PoW enhances security - PoS speeds up confirmations - ML regulates resource allocation, analyzing validator status and network behavior | - Lower energy consumption compared to pure PoW - Harder to take over the network - Proactive anomaly detection |
| PoCASBFT | Casper (PoS) + pBFT + ML | - pBFT ensures fast finality - Casper introduces economic penalties (slashing) - ML detects validation errors and analyzes transaction time series | - High resilience to Byzantine failures - Balance between economic incentives and fast consensus |
| DBPoS | DPoS + pBFT + ML | - DPoS delegates aggregate blocks - pBFT confirms agreement - ML detects vote bias, identifies collusion trends, and signals fraud | - Faster block verification - Ability to detect and block "captured" delegates - Scalability |

As shown in Table 2, in all cases, integrating ML enables the following:

- Automatic analysis of network metrics (number of transactions, block intervals, block rejection rates, etc.).
- Accumulation of historical data for training, allowing timely recognition of new fraudulent behavior beyond deterministic rule-based detection [14, 19].
- Reduced likelihood of 51% attacks, as an adversary would find it more difficult to manipulate behavior statistics learned from large datasets [15, 21].

Hybrid consensus algorithms represent a promising direction in blockchain technology, combining the advantages of multiple methods (PoW, PoS, DPoS, pBFT, etc.) within a single network.

At the same time, ML integration increases computational requirements and demands a comprehensive approach to privacy and model robustness against adversarial attacks. These challenges are the focus of ongoing research. In the future, the most practically successful implementations will likely involve «self-learning» hybrid protocols capable of anticipating and adapting to threats without operator intervention [25].

Table 3 outlines the main stages of the methodology for applying hybrid consensus algorithms and integrating machine learning.

**Table 3.** The main stages of the methodology for applying hybrid consensus algorithms and integrating machine learning, along with expected results [16, 19, 20, 21].

| Stage / Step | Actions | Result |
|---|---|---|
| Step 1. Attack scenario analysis and identification | 1) Analyze business requirements and potential threats (51% attack, double spending, delegate collusion) 2) Define security criteria | - Comprehensive list of threats and attack vectors - Initial requirements for performance and scalability |
| Step 2. Selection and design of hybrid consensus | 1) Determine which algorithms to combine (PoW+PoS, DPoS+pBFT, etc.) 2) Develop logic for switching/merging 3) Account for platform-specific features (e.g., ProximaX) | - Architectural scheme of the hybrid protocol - Data models and block structures |
| Step 3. Development of ML modules | 1) Collect and clean transaction and network telemetry data 2) Generate training datasets (anomaly detection, classification) 3) Hyperparameter tuning | - Trained models for anomaly detection and attack prediction - Metrics (accuracy, recall, F1 score) |
| Step 4. ML and consensus integration | 1) Embed ML modules into the decision-making process 2) Define result-sharing protocols (global, P2P, off-chain or on-chain) 3) Ensure privacy preservation | - Fully functional "intelligent" consensus layer - Clear interfaces for calling ML algorithms |
| Step 5. Testing and simulations | 1) Simulate attack scenarios (51% attack, double spending, DDoS) 2) Collect performance metrics (TPS, latency, throughput) 3) Analyze false positives in ML detections | - System stability report - Specific performance/security improvement metrics |
| Step 6. Analysis and optimization | 1) Compare with alternative solutions 2) Optimize hybrid protocol parameters 3) Final ML module calibration | -Finalized metrics (latency, overhead, attack detection accuracy) - Recommendations for real-world deployment |

At each stage, the methodology defines the necessary actions, target metrics, and required blockchain platform configurations.

Future research directions include:

- Automated parameter tuning using reinforcement learning (RL), allowing the system to «learn» to optimize the trade-off between throughput and security.
- Implementation of lightweight (edge) ML models to reduce computational overhead and enable broader adoption in public blockchains.
- Advanced privacy-preserving techniques, including homomorphic encryption for distributed learning, which is especially crucial in environments handling highly sensitive data.

## CONCLUSION

The analysis of existing consensus algorithms (PoW, PoS, DPoS, pBFT, PoA, Casper) demonstrated that while each has strengths, they also exhibit limitations affecting scalability, energy efficiency, and resistance to various cyberattacks. To address these challenges, hybrid schemes combining mechanisms from multiple protocols (e.g., PoSW, DPoSW, PoCASBFT, DBPoS) are a viable solution. These approaches enhance resistance to 51% attacks and minimize the risk of double spending by requiring an attacker to simultaneously control multiple resources (computational power, stake distribution, delegation, etc.).

Additionally, the study highlights the growing role of machine learning. ML techniques integrated into the consensus decision-making process enable early anomaly detection, automation of fraudulent transaction identification, and intelligent network parameter tuning (block creation time, mining/validation difficulty, stake size).

The implementation of these approaches on the ProximaX platform demonstrated the potential of hybrid consensus models in specific scenarios, such as consortium networks, smart grids, and industrial IoT. However, challenges remain in establishing a secure and decentralized environment for ML model training (federated learning), utilizing homomorphic encryption, and developing heuristics to counter adversarial attacks.

Future research should focus on deeper integration of reinforcement learning mechanisms for automatic adaptation to emerging threats and optimization of network throughput while maintaining high security. Expanding the experimental dataset and developing energy-efficient models with low computational overhead are also critical for real-world applications, where transaction confirmation speed and resilience to dynamic loads are paramount.

## REFERENCES


1 Oyinloye D. P. et al. Blockchain consensus: An overview of alternative protocols //Symmetry. – 2021. – Vol. 13 (8). – pp. 1363.

2 Wang B., Li Z., Li H. Hybrid consensus algorithm based on modified proof-of-probability and DPoS //Future Internet. – 2020. – Vol. 12 (8). – pp. 122.

3 Shafay M. et al. Blockchain for deep learning: review and open challenges //Cluster Computing. – 2023. – Vol. 26 (1). – pp. 197-221.

4 Khobragade P., Turuk A. K. Blockchain consensus algorithms: A survey //International Congress on Blockchain and Applications. – Cham : Springer International Publishing. - 2022. – pp. 198-210.

5 Bachani V., Bhattacharjya A. Preferential delegated proof of stake (PDPoS)—modified DPoS with two layers towards scalability and higher TPS //Symmetry. – 2022. – Vol. 15 (1). – pp. 4.

6 Wu Y., Song P., Wang F. Hybrid consensus algorithm optimization: A mathematical method based on POS and pBFT and its application in blockchain //Mathematical Problems in Engineering. – 2020. – Vol. 2020(1). – pp. 7270624.

7 Buterin V., Reijsbergen D., Leonardos S., & Piliuras G. // Incentives in the hybrid Casper protocol. In Proceedings of the IEEE International Conference on Blockchain and Cryptocurrency. - 2019. - pp. 236–244.

8 Chen S. et al. Improvement of the DPoS consensus mechanism in blockchain based on PLTS //2021 7th IEEE Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing,(HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS). – IEEE. - 2021. – pp. 32-37.

9 Hu Y. et al. A practical heartbeat-based defense scheme against cloning Attacks in PoA blockchain //Computer Standards & Interfaces. – 2023. – Vol. 83. – pp. 1-9.

10 Kiayias A. et al. Ouroboros: A provably secure proof-of-stake blockchain protocol //Annual international cryptology conference. – Cham : Springer International Publishing. - 2017. – pp. 357-388.

11 Lashkari B., Musilek P. A comprehensive review of blockchain consensus mechanisms //IEEE access. – 2021. – Vol. 9. – pp. 43620-43652.

12 Feng C. et al. A Low Communication Complexity Double-layer pBFT Consensus //Wireless Blockchain: Principles, Technologies and Applications. – 2021. – pp. 73-92.

13 Liu D. et al. Anonymous reputation system for IIoT-enabled retail marketing atop PoS blockchain //IEEE Transactions on Industrial Informatics. – 2019. – Vol. 15 (6). – pp. 3527-3537.

14 Liu S. et al. P-pBFT: An improved blockchain algorithm to support large-scale pharmaceutical traceability // Computers in biology and medicine. – 2023. – Vol. 154. – pp. 5-17.

15 Saad M. et al. Mempool optimization for defending against DDoS attacks in PoW-based blockchain systems //2019 IEEE international conference on blockchain and cryptocurrency (ICBC). – IEEE, 2019. – pp. 285-292.

16 Sapra N., Shaikh I., Dash A. Impact of proof of work (PoW)-based blockchain applications on the environment: A systematic review and research agenda //Journal of Risk and Financial Management. – 2023. – Vol. 16 (4). – pp. 218.

17 Wang W. et al. A survey on consensus mechanisms and mining strategy management in blockchain networks // Ieee Access. – 2019. – Vol. 7. – pp. 22328-22370.

18 Wood G. et al. Ethereum: A secure decentralised generalised transaction ledger //Ethereum project yellow paper. – 2014. – Vol. 151. – pp. 1-32.

19 Xiao Y. et al. A survey of distributed consensus protocols for blockchain networks //IEEE Communications Surveys & Tutorials. – 2020. – Vol. 22 (2). – pp. 1432-1465.

20 Chen Y., Liu F. Improvement of DPoS consensus mechanism in collaborative governance of network public opinion //2021 4th International Conference on Advanced Electronic Materials, Computers and Software Engineering (AEMCSE). – IEEE, 2021. – pp. 483-488.

21 Andoni M. et al. Blockchain technology in the energy sector: A systematic review of challenges and opportunities //Renewable and sustainable energy reviews. – 2019. – Vol. 100. – pp. 143-174.

22 Meland P. H. et al. A systematic mapping study on cyber security indicator data //Electronics. – 2021. – Vol. 10 (9). – pp. 1092.

23 Xiao Y. et al. A survey of distributed consensus protocols for blockchain networks //IEEE Communications Surveys & Tutorials. – 2020. – Vol. 22 (2). – pp. 1432-1465.

24 Xiao L. et al. A reinforcement learning and blockchain-based trust mechanism for edge networks //IEEE Transactions on Communications. – 2020. – Vol. 68 (9). – pp. 5460-5470.

25 Zhu S. et al. zkCrowd: a hybrid blockchain-based crowdsourcing platform //IEEE Transactions on Industrial Informatics. – 2019. – Vol. 16 (6). – pp. 4196-4205.