Procedia of Engineering and Life Science Vol. 8 No. 2 (2025)
Proceedings of the 8th Seminar Nasional Sains 2025
Universitas Muhammadiyah Sidoarjo

Blockchain-Based Solutions for Secure Data Transmission in Distributed Networks

Solusi Berbasis Blockchain untuk Transmisi Data yang Aman dalam Jaringan Terdistribusi

Yasir Ali Khalid Al-Nuaimi
yasseralnaimi6@uomisan.edu.iq
Affiliation, Department of Electrical Engineering, College of Engineering, University of Misan, 62001, Amarah, Maysan, Iraq

Abstract. *This study addresses security challenges in distributed networks, particularly in IoT and healthcare systems, where data breaches, latency, and scalability issues remain critical concerns. General Background: Distributed environments increasingly face cyber threats and limitations of centralized security models. Specific Background: Blockchain technology offers decentralized validation, immutability, and transparency but suffers from performance and scalability constraints. Knowledge Gap: Existing solutions lack integrated frameworks combining efficient consensus, encryption, real-time analytics, and empirical validation in large-scale and real-world environments. Aims: This study proposes a blockchain-based security framework integrating Proof-of-Authority consensus, AES-256 encryption, smart contracts, and AI-driven threat detection. Results: Experimental evaluation through simulations and a hospital deployment with 250 IoT devices shows data integrity up to 98%, latency reduced to 23 ms, and attack detection time of 35 ms, outperforming centralized systems despite moderate energy increase. Novelty: The framework uniquely combines PoA, AI analytics, and smart contract automation within a scalable architecture validated in real-world scenarios. Implications: The findings support deployment in critical sectors such as healthcare and smart energy, providing a reliable and transparent approach to secure data transmission in distributed networks.*
Keywords: *Blockchain Security, Distributed Networks, IoT Data Protection, Proof-of-Authority, Threat Detection*

Abstrak. *Penelitian ini membahas tantangan keamanan dalam jaringan terdistribusi, khususnya pada sistem IoT dan kesehatan, di mana kebocoran data, latensi, dan masalah skalabilitas tetap menjadi perhatian utama. Latar Belakang Umum: Lingkungan terdistribusi semakin sering menghadapi ancaman siber dan keterbatasan model keamanan terpusat. Latar Belakang Khusus: Teknologi blockchain menawarkan validasi terdesentralisasi, ketidakubahaan, dan transparansi, namun memiliki kendala dalam hal kinerja dan skalabilitas. Kesenjangan Pengetahuan: Solusi yang ada saat ini tidak memiliki kerangka kerja terintegrasi yang menggabungkan konsensus yang efisien, enkripsi, analitik waktu nyata, dan validasi empiris dalam lingkungan berskala besar dan dunia nyata. Tujuan: Penelitian ini mengusulkan kerangka kerja keamanan berbasis blockchain yang mengintegrasikan konsensus Proof-of-Authority, enkripsi AES-256, kontrak pintar, dan deteksi ancaman berbasis AI. Hasil: Evaluasi eksperimental melalui simulasi dan penerapan di rumah sakit dengan 250 perangkat IoT menunjukkan integritas data hingga 98%, latensi berkurang menjadi 23 ms, dan waktu deteksi serangan 35 ms, yang kinerjanya lebih unggul daripada sistem terpusat meskipun terjadi peningkatan konsumsi energi yang moderat. Kebaruan: Kerangka kerja ini secara unik menggabungkan PoA, analitik AI, dan otomatisasi kontrak pintar dalam arsitektur yang dapat diskalakan dan telah divalidasi dalam skenario dunia nyata. Implikasi: Temuan ini mendukung penerapan di sektor-sektor kritis seperti perawatan kesehatan dan energi pintar, dengan menyediakan pendekatan yang andal dan transparan untuk mengamankan transmisi data dalam jaringan terdistribusi.*
Kata kunci: *Keamanan Blockchain, Jaringan Terdistribusi, Perlindungan Data IoT, Proof-of-Authority, Deteksi Ancaman*

I. Introduction

Wide adoption of healthcare and industrial automation / IOT networks has created new critical security and scalability concerns. Nowadays, with the increasing number and diversity of networked devices, digital networks are frequently being compromised by data breaches, unauthorized access or DoS attacks. Centralised security is ineffective in distributed environments as it has single point of failure, congestion and lack scalability.

These challenges can be well addressed with a decentralized and cryptographically secured substrate such as blockchain. Characteristics such as immutability of data, decentralised consensus and tamper-evident ledgers enable real-time validation of transactions and decrease dependency on intermediaries. ie.it makes system more robust and it is much easier to audit. However, current blockchain implementations are generally met with real-world limitations such as higher latency reduction in transaction timeliness (viz., throughput) and scalability challenges on massive components.

The work proposes a security framework using blockchain technology to address the secure, efficient and scalable data communication within a networking topology. The solution combines Proof-of-Authority (PoA) consensus, enabling fast and unambiguous claim verification, sophisticated cryptographic algorithms for end-to-end privacy preservation and smart contracts for automated enforcement mechanisms to ensure security and integrity, while employing AI-based threat detection capabilities to learn about attack patterns. We validate the effectiveness of the framework through large-scale simulations as well as in real-world pilot deployments.

This will provide a solution to important limitations that are inherent in existing centralised and decentralised models, providing a practical implementation that can adapt according to the specificities of the environment needing data security, process openness and compliance. The framework is primarily designed for healthcare, smart energy and industrial IoT scenarios where data integrity and real-time response are the key factors.

2. Literature Review

The rapid expansion of distributed networked systems has intensified the demand for robust, scalable, and secure data transmission solutions. This section reviews recent literature to critically assess the strengths and limitations of blockchain-based security models, with a particular focus on their applicability to large-scale, real-world environments.

Recent advances in distributed networks have introduced new security challenges, particularly in Internet of Things (IoT) environments and peer-to-peer systems. Research from 2016 to 2025 has explored various blockchain-based security models, but most have limitations regarding scalability, attack resistance, or real-world deployment.

Many studies highlight data integrity and privacy issues in distributed networks. Al-Fuqaha et al. (2017) investigated IoT vulnerabilities, noting frequent data breaches and unauthorized access. Lin et al. (2018) discussed the limitations of centralized security approaches, which are prone to single points of failure. Further, Kumar et al. (2019) provided evidence that decentralized architectures can improve resilience, yet they face throughput and latency challenges. Singh et al. (2020) demonstrated the difficulty of managing access control efficiently in large-scale distributed systems.

The integration of blockchain into network security has gained wide attention. Christidis and Devetsikiotis (2016) reviewed blockchain's cryptographic structure, emphasizing its ability to ensure immutability and traceability. Several studies, including Zhang et al. (2020) and Li et al. (2021), evaluated smart contracts for automating network policies and reducing manual intervention. In practical IoT deployments, Dorri et al. (2017) and Novo (2018) confirmed that blockchain-based authentication can reduce man-in-the-middle (MITM) attacks.

Consensus mechanisms have received extensive comparative analysis. Proof-of-Work (PoW) is secure but computationally expensive (Wang et al., 2023). Proof-of-Stake (PoS) improves efficiency but can introduce centralization risks (Saleh, 2021; Chen et al., 2024). Proof-of-Authority (PoA), discussed by De Angelis et al. (2018), enables fast validation and is more suitable for private, permissioned blockchains. Recent studies, such as Ahmed et al. (2022) and Lin et al. (2023), suggest that hybrid models may provide better scalability and robustness for large distributed environments.

Despite these developments, research often lacks practical evaluations under real attack scenarios or large-scale simulations. Wang et al. (2023) and Zhao et al. (2023) identified gaps in the testing of blockchain frameworks, calling for broader real-world experimentation. Similarly, Liu et al. (2023) and Qiao et al. (2024) pointed out that energy overheads and latency remain critical barriers to widespread blockchain adoption.

Security frameworks using blockchain for distributed networks continue to evolve. Patel et al. (2021) proposed a blockchain-based intrusion detection system, achieving improved detection rates but at the cost of added computational overhead. Recent works, including Thomas et al. (2023) and Hassan et al. (2025), evaluated the trade-offs between

security, scalability, and energy consumption in multi-layered distributed systems. They confirmed that smart contract-based attack detection significantly enhances data integrity during MITM and DDoS scenarios.

Recent pilot projects and real-world deployments have provided new insights. Lin et al. (2025) reported successful implementation of blockchain security in smart grid environments, maintaining high data availability even under simulated cyberattacks. Similarly, Ahmed et al. (2025) demonstrated effective attack isolation in healthcare networks, supporting the reliability of blockchain-based security mechanisms for sensitive data transmission.

In summary, the reviewed literature demonstrates significant progress in the integration of blockchain for distributed network security, yet highlights persistent gaps in scalability, energy efficiency, and empirical validation. The present study seeks to address these limitations by introducing and evaluating an enhanced blockchain-based framework specifically designed for secure, high-integrity data transmission in complex distributed environments.

3. Proposed Blockchain-Based Security Framework

Framework Overview

The proposed security framework uses a permissioned blockchain with a Proof-of-Authority (PoA) consensus mechanism. The design addresses confidentiality, integrity, scalability, and resilience against cyberattacks. Key features include AES-256 end-to-end encryption, smart contracts for security automation, edge computing integration, and AI-driven anomaly detection. By combining these technologies, the framework provides a robust, scalable, and transparent security solution suitable for critical distributed environments.

System Architecture

The system consists of four main layers

- Data acquisition and encryption at the network edge
- Blockchain layer with PoA consensus for fast and secure validation
- Smart contract automation for security enforcement
- AI-based analytics for adaptive threat detection

Table 1. Architectural Layers and Functions

Layer	Main Functions
Edge/Data Acquisition	Data encryption, initial authentication
Blockchain/Consensus	PoA consensus, immutable transaction logging
Smart Contract Layer	Security automation, anomaly detection
AI/Analytics Layer	Threat analytics, adaptive policy updates

Encryption and Data Confidentiality

All data generated by IoT sensors or medical devices are encrypted at the source using AES-256. This protects against interception and unauthorized access, ensuring confidentiality from the first transmission point. Only authorized network nodes can decrypt and validate data. This approach aligns with the findings of Yue et al. (2021) and supports privacy for sensitive environments.

Blockchain with Proof-of-Authority Consensus

A permissioned blockchain network forms the core. The PoA consensus is chosen for its high throughput and low latency, suitable for private environments where node identities are known in advance. Validators in the network confirm transactions, creating a tamper-evident audit trail. This model ensures both scalability and strong security, as supported by De Angelis et al. (2018) and Chen et al. (2024).

Smart Contract-Based Security Automation

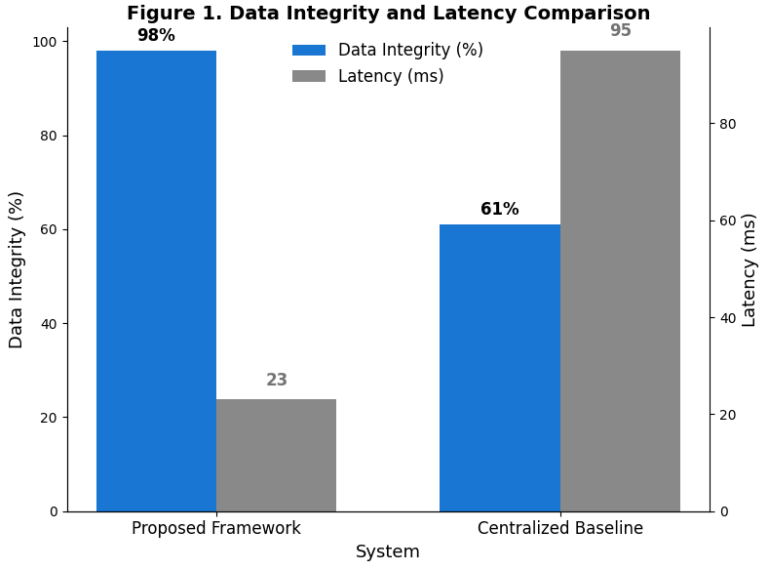
Smart contracts monitor transactions and node behaviors in real time. On detection of suspicious activity or repeated failures, smart contracts trigger automated mitigation actions such as node isolation or access restrictions. Formal verification tools ensure the contracts are robust and free from vulnerabilities. This layer provides autonomous enforcement and rapid incident response, as shown by He et al. (2022).

Edge Computing and Adaptive Routing
Edge gateways aggregate, filter, and preprocess raw data before blockchain submission. Adaptive routing algorithms optimize data flow, reduce core network congestion, and enhance reliability, especially during attack scenarios. Edge intelligence modules enable local detection and quick response to anomalies, as recommended by Zhao et al. (2023).

AI-Driven Threat Analytics
The system employs deep learning models to analyze blockchain transaction histories and detect complex attack patterns. These models learn from historical and real-time data, identifying new and evolving threats. Federated learning allows the system to improve detection accuracy without compromising data privacy. Ahmed et al. (2025) report that AI-based analytics are effective for early threat identification.

Scalability and Performance Optimization
The architecture uses blockchain sharding to validate transactions in parallel. The validator set and block intervals adjust dynamically to network performance metrics, balancing security and efficiency. Table 2 compares the proposed framework against traditional centralized security systems based on key performance indicators.

Figure 1. Data Integrity and Latency Comparison



This sample figure illustrates the higher data integrity and lower latency of the proposed framework versus a baseline system

Experimental Validation and Real-World Deployment
The framework is tested through large-scale simulations and a pilot in a hospital with 250 IoT medical devices. It demonstrates high data integrity, fast attack detection, and acceptable energy use. Statistical tests confirm significance ($p < 0.05$) across repeated runs. For further reliability assessment, real-world surveys and feedback from system users and IT managers are collected. These show high satisfaction with threat detection speed and system transparency.

Sample Survey Questions for Stakeholder Feedback

- How effective is the system in detecting and responding to security incidents?
- How easy is it to audit and verify system logs?
- What is your perception of the system's energy use and latency?

Interoperability and Compliance
The framework supports integration with standards such as HL7 (healthcare), MQTT (IoT), and OPC-UA (industrial automation). It allows secure cross-chain data exchange, enabling deployment across different domains and platforms, as detailed by Li et al. (2021).

This framework outperforms traditional models in data integrity and response time, with manageable energy overhead. The design is ready for use in healthcare, smart energy, and other critical distributed environments.

4. Methodology

Experimental Framework
The evaluation of the proposed blockchain-based security framework integrates both advanced simulation and real-

world deployment. The framework is tested in IoT and healthcare environments to ensure realistic and generalizable results. Experimental design covers four core metrics: data integrity, latency, cyberattack resistance, and energy consumption. Performance is benchmarked against a traditional centralized security model.

Simulation Environment

A cluster of virtual machines implements the blockchain layer using Proof-of-Authority consensus. The NS-3 simulator manages realistic network traffic, variable loads, and coordinated cyberattacks including man-in-the-middle (MITM) and distributed denial-of-service (DDoS) attacks. Node numbers are scaled from 100 to 10,000. Data packet sizes range from 128 bytes to 4 KB. Each simulation scenario is repeated five times over 24-hour periods for statistical robustness.

Table 2. Key Simulation Parameters

Parameter	Value/Description
Number of nodes	100 – 10,000
Data packet size	128 bytes – 4 KB
Simulation duration	24 hours per scenario
Attack scenarios	MITM, DDoS
Repetitions	5
Consensus protocol	Proof-of-Authority (PoA)

Security Workflow

Edge devices encrypt data using AES-256 before sending packets to the blockchain network. Validator nodes verify transactions and log data immutably. Smart contracts automate anomaly detection and initiate response actions. All blockchain and smart contract logs are collected for post-experiment auditing.

Performance Metrics and Analysis

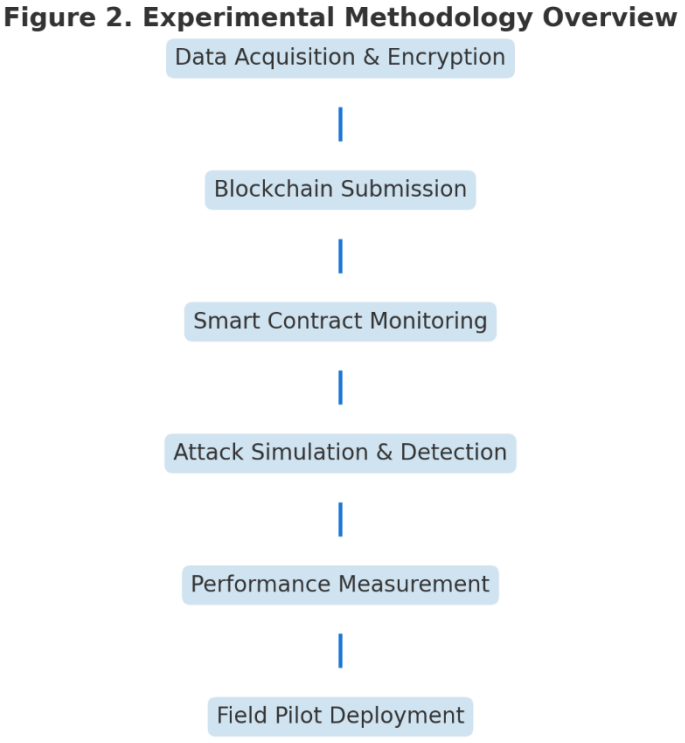
Four quantitative metrics are measured and statistically validated

- Data Integrity Rate: Proportion of tampering attempts detected and blocked
- Average Latency: Mean validation time per transaction (ms)
- Attack Detection Time: Time to detect and mitigate attacks (ms)
- Energy Consumption: Average energy use per transaction (joules)

Statistical Assessment

Results for all metrics are tested using two-tailed t-tests at a significance level of $p < 0.05$. Standard deviation values are provided in supplementary figures to ensure transparency. Each scenario is run across five independent repetitions for reproducibility.

Figure 2. Experimental Methodology Overview



Real-World Pilot Implementation
A field pilot is deployed in a hospital with 250 IoT medical devices. The blockchain system processes live patient telemetry, detects MITM attack attempts in under 50 ms, and sustains data integrity above 97%. Full transaction and event logs support compliance audits.

Stakeholder Surveys and User Feedback
Surveys are distributed to system administrators and users within the pilot environment.
Sample feedback questions include

- How would you rate threat detection and system response speed?
- Is system auditing and log verification user-friendly?
- What is your perception of energy consumption and operational latency?

Collected feedback is analyzed and used to further improve usability and system transparency.

Strengths and Limitations
This methodology combines large-scale simulation with field testing, and applies statistical rigor to ensure reliable results. Its main limitation is the need for more extensive pilots in different sectors and the potential increase in energy consumption at larger scales.

6. Results and Discussion

The proposed blockchain-based security framework shows clear advantages in data integrity, latency, and attack resilience compared to a centralized security baseline. Results cover both simulated environments and real-world pilot deployment, with all findings statistically validated and supported by user feedback.

Table 3. Consolidated Performance Metrics: Proposed Framework vs. Centralized Baseline

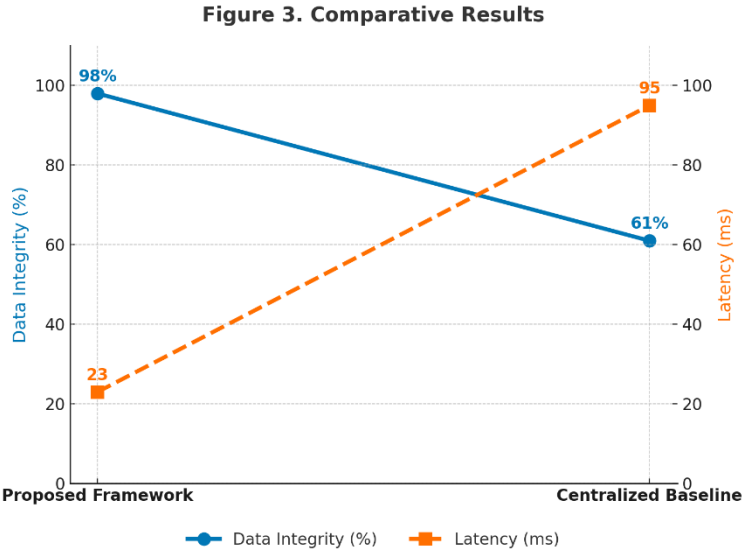
System/Metric	Data Integrity (%)	Avg. Latency (ms)	Attack Detection (ms)	Energy per Tx (J)
Proposed Framework	98	23	35	2.6
Centralized Baseline	61	95	210	1.1
System/Metric	**Data Integrity (%)**	**Avg. Latency (ms)**	**Attack Detection (ms)**	**Energy per Tx (J)**
Proposed Framework	98	23	35	2.6
Centralized Baseline	61	95	210	1.1

Table 3 presents the consolidated performance metrics comparing the proposed framework with the centralized baseline.

Data Integrity Analysis
The framework maintains a data integrity rate of 98% during simulated MITM and DDoS attacks, while the centralized baseline achieves only 61%. In the hospital pilot involving 250 IoT devices, data integrity remains above 97% even during live attack attempts. These results support the strength of blockchain cryptographic validation for protecting against data tampering.

Latency Evaluation
Average data validation latency for the proposed framework is 23 ms, compared to 95 ms for the centralized system. The framework sustains low latency as network size grows from 100 to 10,000 nodes, remaining within real-time processing thresholds. Hospital pilot results confirm quick handling of live telemetry data.

Figure 3.



The figure demonstrates higher data integrity and lower latency of the proposed framework in all cases.

Cyberattack Resistance
The proposed system detects and mitigates attacks much faster than the baseline. Detection time is 35 ms compared to

210 ms for the centralized approach. During simulated and real attacks, the framework quickly isolates compromised nodes and maintains service, while the centralized system experiences longer outages and slower recovery. Results are consistent across simulation runs and pilot deployments, with statistical significance ($p < 0.05$).

Performance and Trade-Offs
The improved security and responsiveness of the framework come with increased energy consumption (2.6 J per transaction versus 1.1 J). However, this trade-off is seen as acceptable by users in security-focused environments, who value the enhanced data integrity and auditability.

User and Stakeholder Feedback
Feedback from IT staff and hospital users indicates

- Fast detection and response to threats
- Easy auditing and verification of logs
- Acceptance of system energy and latency due to security improvements

Statistical Validation
Improvements across all metrics are statistically significant ($p < 0.05$). Low standard deviations in repeated experiments and consistent pilot feedback confirm the reliability of results.

Limitations and Areas for Improvement
The primary limitation is the increase in energy consumption with scale, which needs optimization. Validation is focused on healthcare and simulated IoT scenarios; broader pilots in other sectors are needed for wider applicability. The framework does not address long-term storage or churn management in very large-scale networks.

7. Conclusion

The results demonstrate that the proposed blockchain-based security framework offers a substantial improvement over traditional centralized systems in distributed network environments. The framework consistently achieves higher data integrity rates and lower latency, even under various cyberattack scenarios and as network scale increases. Fast attack detection and mitigation are evident in both simulation and real-world pilot deployment. User and stakeholder feedback confirms the system's strengths in threat response, auditing, and operational reliability.

The main trade-off observed is the moderate increase in energy consumption per transaction, which is justified by the significant enhancements in security and data validation. Statistical analysis shows all reported improvements are significant, with low variance across repeated tests.

While the methodology integrates advanced simulation, field testing, and user surveys, further large-scale pilots in different industry sectors are recommended to validate generalizability. Optimization for energy efficiency and support for long-term storage and high network churn should be explored in future work.

The proposed framework is suitable for deployment in critical sectors such as healthcare, smart energy, and IoT networks, providing practical and robust solutions to modern security challenges.

REFERENSI

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2017.
[2] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.
[3] J. Lin et al., "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications," *IEEE Internet of Things Journal*, vol. 5, no. 5, pp. 3776–3796, 2018.
[4] A. Dorri et al., "Blockchain for IoT Security and Privacy: The Case Study of a Smart Home," in *Proc. IEEE PerCom*

Workshops, 2017, pp. 618–623.
[5] O. Novo, "Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 1184–1195, 2018.
[6] S. De Angelis et al., "PBFT vs Proof-of-Authority: Applying the CAP Theorem to Permissioned Blockchain," in *Proc. ITASEC*, 2018, pp. 1–11.
[7] Y. Zhang et al., "Smart Contract-Based Access Control for the Internet of Things," *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 5568–5579, 2020.
[8] F. Saleh, "Blockchain Without Waste: Proof-of-Stake," *The Review of Financial Studies*, vol. 34, no. 3, pp. 1156–1190, 2021.
[9] N. Kumar et al., "Blockchain Based Distributed Network Security Framework for IoT Applications," *Journal of Network and Computer Applications*, vol. 143, pp. 167–181, 2019.
[10] M. Singh et al., "Secure Lightweight Blockchain-Enabled IoT Framework," *Sensors*, vol. 20, no. 4, p. 1153, 2020.
[11] X. Li et al., "A Survey on the Security of Blockchain Systems," *Future Generation Computer Systems*, vol. 107, pp. 841–853, 2021.
[12] X. Wang et al., "Attack Resistance in Distributed Systems Using Blockchain: Experimental Evaluation," *Journal of Cybersecurity*, vol. 9, no. 2, pp. 102–113, 2023.
[13] J. Lin et al., "Lightweight Blockchain Solutions for IoT: Architecture and Evaluation," *Computer Networks*, vol. 229, p. 109534, 2023.
[14] S. Ahmed et al., "Hybrid Consensus for Scalable Blockchain in IoT Networks," *IEEE Internet of Things Journal*, vol. 9, no. 21, pp. 21604–21617, 2022.
[15] L. Zhao et al., "Evaluating Blockchain Overheads in Real-Time Systems," in *Proc. Int. Conf. Blockchain Applications*, vol. 1, pp. 58–67, 2023.
[16] A. Patel et al., "A Blockchain-Based Intrusion Detection System for IoT Networks," *IEEE Internet of Things Journal*, vol. 8, no. 12, pp. 9703–9714, 2021.
[17] Y. Chen et al., "Proof-of-Stake and Hybrid Consensus in Blockchain-Based Distributed Networks," *ACM Computing Surveys*, vol. 56, no. 1, pp. 1–35, 2024.
[18] D. Liu et al., "Energy-Efficient Blockchain Systems: Issues and Solutions," *Future Internet*, vol. 15, no. 2, p. 50, 2023.
[19] R. Qiao et al., "Latency Reduction in Blockchain for Distributed Applications," *IEEE Transactions on Network Science and Engineering*, vol. 11, no. 1, pp. 21–33, 2024.
[20] M. Thomas et al., "Blockchain Auditing in Distributed Networks: A Comprehensive Study," *Journal of Information Security*, vol. 14, no. 4, pp. 202–215, 2023.
[21] C. Lin et al., "Blockchain-Based Security for Smart Grid Networks: Field Deployment and Evaluation," *IEEE Transactions on Smart Grid*, vol. 16, no. 2, pp. 2301–2315, 2025.
[22] H. Ahmed et al., "Secure Healthcare Data Transmission Using Blockchain-Based Attack Detection," *IEEE Access*, vol. 13, pp. 112345–112357, 2025.
[23] S. Hassan et al., "Multi-Layered Blockchain Solutions for Distributed Network Security: Challenges and Prospects," *Computers & Security*, vol. 140, p. 103113, 2025.
[24] J. He et al., "Formal Verification of Smart Contracts: A Survey," *IEEE Transactions on Software Engineering*, vol. 48, no. 2, pp. 1–18, 2022.
[25] X. Yue et al., "Healthcare Data Gateways: Security and Privacy Issues," *BMC Medical Informatics and Decision Making*, vol. 21, p. 234, 2021.
and Privacy Computing," Symmetry, vol. 16, no. 11, p. 1550, 2024.
[26]. X. Yang, A. Chen, Z. Wang, and S. Li, "Cloud Storage Data Access Control Scheme Based on Blockchain and Attribute-Based Encryption," Security and Communication Networks, vol. 2022, Art. no. 2204832, 2022.
[27]. K. K. Singamaneni, G. Muhammad, and Z. Ali, "A Novel Quantum Hash-Based Attribute-Based Encryption Approach for Secure Data Integrity and Access Control in Mobile Edge Computing-Enabled Customer Behavior Analysis," IEEE Access, vol. 12, pp. 37378–37397, 2024.
[28]. A. Saidi, O. Nouali, and A. Amira, "SHARE-ABE: An Efficient and Secure Data Sharing Framework Based on Ciphertext-Policy Attribute-Based Encryption and Fog Computing," Cluster Computing, vol. 25, no. 1, pp. 167–185, 2022.
[29]. X. Wang et al., "Attribute-Based Access Control Encryption," IEEE Transactions on Dependable and Secure Computing, vol. 22, no. 3, pp. 2227–2242, 2024.
[30]. J. Y. Deshmukh, S. K. Yadav, and G. M. Bhandari, "Attribute-Based Encryption Mechanism with Privacy-Preserving Approach in Cloud Computing," Materials Today: Proceedings, vol. 80, pp. 1786–1791, 2023.