International Journal of
Human Computations & Intelligence
Vol. 04, Issue. 05, 2025

RESEARCH ARTICLE OPEN ACCESS

Optimized Integration of Blockchain and IoT: A Review of Lightweight Approach for Scalable and Secure Ecosystems

Abhishek Bhardwaj . Shivansh . Munish Kumar . Pradeep Chouksey . Mayank Chopra . Parveen Sadotra

Department of Computer Science and Informatics,
Central University of Himachal Pradesh, Kangra, India

DOI: **10.5281/zenodo.15745463**
Received: 18 May 2025 / Revised: 24 June 2025 / Accepted: 26 June 2025
©Milestone Research Publications, Part of CLOCKSS archiving

Abstract – Blockchain technology has been making waves in recent years, and people are starting to think about how it could help to make Internet of Things (IoT) systems more secure and reliable. In this paper, we dive into how these two worlds could collide, looking at what the IoT is made up of (sensors, networks, devices, etc.) and how it could hook up with Blockchain. In theory IoT systems can address common challenges such as breaches of data, hacks, unauthorized access, and system failures by using Blockchain's decentralized, tamper proof features. In addition, the paper looks at how smart contracts can automate operations in IoT systems to ensure secure, efficient communication between devices. We also elaborate on how Lightweight Blockchain frameworks and Energy efficient protocols can make Blockchain suitable for resource constrained IoT devices, opening the frontier in healthcare, supply chain and smart cities. However, despite the potential, we discuss the issues with such integration scalability, energy consumption and privacy concerns and leave directions for research on future seamless IoT-Blockchain integration.

Index Terms – IoT, IIoT, BPIIoT, Blockchain, Lightweight blockchain.

I. Introduction

Internet technology is also described as the method that links machines, equipment and other objects to the internet through use of wireless technologies. IoT is a web of physical things stuffed with technology enhancing their ability to sense, connect and respond to conditions within and outside of them. The Internet of Things is a near real time information system for internet-linked devices using product embedded code and Radio Frequency Identification. Technological advancement, which is the IoT is revolutionizing how

MILESTONE
RESEARCH.IN
OPEN ACCESS

ISSN (Online): 2583-5696
Int. Jr. of Hum Comp. & Int.

people and things connect with the environment. ranging across home automation to healthcare, means IoT is complex network of devices, sensors, and networks capable of gathering, analyzing, and sharing data in real-time. IoT is one of the emerging field in technology. IoT have these components as follow,

- Sensors: Physical devices that take environmental information (temperature, humidity, motion) and collect it. These are the eyes and ears of the IoT system.
- Networks: IoT objects can communicate with each other and with the cloud via these are communication systems. Wireless or wired, networks include Wi-Fi, Bluetooth, or cellular networks.
- Devices: The IoT system consists of these actual devices. Smartphones, laptops, smart appliances, or any devices that can connect to the Internet are examples of them.
- Platforms: Software systems operating on these devices and networks enabling communication and exchange of data among and between the devices and networks and the cloud.

A. Problem in IoT:

- Data Gathering: When devices collect sensitive information, there are risks to how it is stored and without proper safeguards information is vulnerable to unauthorized access.
- Data Transmission: If encryption or secure communication protocols aren’t being used, then data sent between IoT devices can be intercepted.
- Tag Embedded: IoT systems can be targeted so that the compromised or cloned tags such as RFID, allow unauthorized access or identity theft.
- Data Storing: IoT data volumes grow, but unless you have protections like encryption and access controls in place there can be breaches.
- Consensus Algorithms and Trust: Weak consensus mechanism in distributed systems can break trust and data integrity.
- Authentication and Access Control: But still poorly implemented authentication allows the attackers to gain unauthorized control over IoT devices.
- Infrastructure: Cyberattacks into IoT networks can be through insecure hardware or software.

1.1. Role of Blockchain:

In simple terms blockchain is the encryption algorithm based and the shared data based technology. With its algorithm of stamping mechanism, it uses the hash chain based encryption algorithm, as well as the certification consistency algorithm to continue to maintain the computational consistency between node data and block data. The data is encrypted on programmable smart contracts in virtual machines. Communication technology is based on blockchain according to a cryptographic security termed consensus mechanism. The three key application of blockchain are Identity Management, Supply Chain Management and IoT. Blockchain makes IoT secure. While blockchain offers IoT security both opportunities and challenges, the decentralized and consensus based nature of blockchain can provide for better security, however, concomitant security challenges meet in the space. Consensus mechanisms give security to IoT through blockchain: A set of rules work with node in order to get its consensus on the data, creating a decentralized network. It verifies data, claims, replaces human verifiers and trust between the nodes. With the help of Proof of Stake (PoS), Proof of burn, Proof of Work (PoW), Proof of Resilience, etc. lockchain ensures reliability of IoT: With distributive network structure among nodes, the blockchain designs based on the structure ensure that even one or more node has been attacked to the data on network but the system is still reliable and safe and can be figured out by the consensus mechanism to disallow such a node and does not affect to whole system.

Blockchain significantly reduce equipment costs of IoT system: Full peer to peer computing in blockchain (P2P) reduces costs from maintaining centralize database and reduces costs of hundreds of billions of transactions using IoT. It is able to utilize computing storage capacity and ideal devices spread all over IoT. Under blockchain model, blockchain can extend the lifecycle of product services: That means they assume responsibility for the management of the equipment in themselves becoming a self-maintenance community. Smart contracts increase the functionality of IoT: By enabling automated secure financial operations together with blockchain-based access rules and inviolable data. The technology enables receivers to authenticate devices as well as prevents DDoS attacks and allows devices to securely communicate with each other. Smart contracts through their decentralized functionality and trust less operating environments optimize the security and efficiency as well as the interoperability performance of the Internet of Things.

A. Problem Statement :

While the use of Blockchain for IoT systems has the potential, there exists a large gap to practice on deployment. Because of these vulnerabilities, i.e. unauthorized access, data breaches, and lack of trust, IoT systems are suffering from weak consensus mechanisms. Furthermore, the scalability and energy consumption of the traditional Blockchain frameworks make them inappropriate for resource constrained IoT devices. Nevertheless, there is no interoperability between Blockchain networks and IoT ecosystems, thus there is no seamless integration and application. In dealing with the above challenges this research develops scalable, energy efficient, and interoperable solutions for IoT environments**.**

II. Literature Review

The literature review aims to study blockchain tech, its unique features, and research problems, as well as how it integrates with IoT. There are some studies that focus on IoT security using blockchain to identify issues and opportunities. Other reviews explore the IoT and blockchain relationship, lightweight blockchain, and how it can be improved. Some studies aim to find gaps in existing research, and suggest ways to address those gaps, like looking at blockchain-based identity management and how it can improve IoT.

A. Architectural Challenges in Blockchain-IoT Integration

- *Resource Constraints of IoT Devices*: The principal obstacle arises from restricted computing power and storage space and network speed capabilities of IoT devices. Limited computational power of IoT devices does not support running complex cryptographic operations and maintaining distributed ledger protocols which traditionally operate with blockchain systems[1], [2], [3].

- *Scalability Issues:* Blockchain platforms face an operational challenge because a large interconnected IoT device network produces massive amounts of data and transactions. Large-scale IoT implementations challenge traditional blockchain systems because they struggle to handle the required high processing speed for validations[2], [4], [5].
- *Security of IoT Devices*: The security enhancements of blockchain face challenges because individual IoT devices have built-in vulnerabilities. A compromised hardware or software in an IoT device poses the risk of sabotaging blockchain data integrity. Protection of a wide variety of IoT devices with different security parameters remains a major security challenge[6], [7], [8].
- *Privacy Concerns:* The security improvements offered by blockchain encryption do not resolve existing challenges related to privacy management within IoT environments. The ability to decide which blockchain data remains public or private along with secure access control systems across numerous devices and users must be balanced against privacy regulation requirements[6], [7], [9].
- *Network Heterogeneity and Latency:* Different IoT devices transmit data within multiple network systems that vary in performance quality. Some real-time IoT applications might experience prohibitive delays because of the communication expenses from blockchain protocols. Establishing smooth communication links between blockchain networks along with IoT devices across all types of networks poses a difficult architectural problem[2], [4], [5]
- *Consensus Mechanisms:* Blockchain consensus mechanisms like Proof-of-Work (PoW) are **compute intensive and energy-consuming**, making them unsuitable IoT devices. The development of specific consensus mechanisms needs to focus on both lightweight operation and energy efficiency for IoT environments[3], [5], [10].
- *Data Management and Integration:* The large quantities of IoT device data require proper data management solutions before shifting it to the blockchain system. Various architectural hurdles arise from the challenge of validating and standardizing data that comes from IoT sources and ensures its integrity and authenticity and relevance[7], [8], [9].
- *Interoperability:* Many different devices and protocols together with multiple platforms populate the IoT environment alongside numerous blockchain platforms. Multiple architectural obstacles exist due to the need to establish complete interoperability between heterogeneous wireless systems. Multiple blockchain platforms utilize distinctive data formats and protocol requirements that limit the capability of IoT devices to handle multiple blockchain network connections[9], [11], [12][13].

Table. 1: Lightweight Blockchain Frameworks

Approach	Characteristics	Use Cases
LightChain	Resource-efficient blockchain for IIoT with Synergistic Multiple Proof (SMP), LightBlock (LB), and Unrelated Block Offloading Filter (UBOF)	Industrial IoT (IIoT)
Lightweight Blockchain-Based IoT Identity Management	Consortium blockchain-based identity system for IoT, distributing authority among organizations and utilizing separate immutable ledgers	IoT Identity Management
Lightweight Hash-Based Blockchain Architecture	Selects lightweight hash functions (QUARK, PHOTON, SPONGENT) dynamically to optimize mining and performance	Industrial IoT (IIoT)

LSB - Lightweight Scalable Blockchain	Optimized blockchain storage platform with Lightweight Consensus (LC) algorithm for improved throughput and traffic management	General IoT Applications
FogBus	Integrates lightweight blockchain with fog and edge computing, ensuring secure data transfer with Master-Worker mode nodes	Edge and Fog Computing IoT Systems
Tikiri	Scalable blockchain using Apache Kafka, Aplos smart contract platform, microservices, and functional programming	Resource-Constrained IoT Devices
BPIIoT	Blockchain-based platform for IIoT addressing security and trust with on-chain transactions and off-chain storage	IIoT Ecosystem and Smart Manufacturing

The paper “ Embedding Blockchain Technology into IoT for Security: A Survey” explores the many security challenges that plague the Internet of Things. The analysis divides blockchain-based IoT security into two main aspects consisting of structural security which includes sensors networks and applications and functional security responsible for updates authentication as well as anti-DDoS measures. The speed of blockchain-based IoT systems get limited because of restrictions in network bandwidth together with computational processing capabilities. Blockchain technology faces challenges with scalability. The energy systems implemented by blockchain technology have the potential to deplete the battery power of IoT devices rapidly. Future investigators work to build efficient blockchain networks as well as extend scalability capabilities and improve the connection between Internet of Things and blockchain frameworks[1].

BPIIoT (Blockchain for Programmable Industrial Internet of Things) represents a lightweight blockchain-based platform according to the paper that addresses Industrial IoT security challenges as well as trust issues and island connectivity problems. BPIIoT operates through an on-chain network which combines functionality with an off-chain network. The on-chain network handles digital signatures in addition to programmable permissions which combined with access control functions. The off-chain network assists blockchain operations by overseeing network data storage functions and performing intricate data processing procedures that blockchain cannot handle. Through smart contracts connected consumer and manufacturing entities obtain real-time access to manufacturing services. Multiple barriers exist in the system involving excessive energy usage and privacy issues alongside security matters but also problems with interface integration and delayed network speed and high implementation costs and complex script programming and challenges with trust maintenance and regulatory requirements and organizational governance. On-chain and off-chain researchers study smart contracts as they develop data security mechanisms which incorporate Secure Multi-Party Computation (SMPC) and secret sharing[12].

The paper "Next Generation IoT and Blockchain Integration" gives an extensive explanation of the advantages that come from unifying IoT with Blockchain technology. Through Blockchain technology users gain decentralized systems together with unchanging records and full visibility thus improving security as well as addressing IoT security and privacy challenges. This paper demonstrates how Blockchain technology introduces scalable protection against the security vulnerabilities that result from centralized IoT architecture design. The paper examines previous research about IoT integration by exploring security methods based on Blockchain while studying its capacity to protect IoT data exchange.

IoT security faces challenges from scalability problems and operational complexities together with substantial power usage and privacy vulnerabilities and mixed system interoperability and unwieldy standards. Upcoming work in this field combines blockchain systems with edge computing to minimize latency and creates new consensus procedures for IoT while establishing smart contracts to automate industrial operations including healthcare and manufacturing[4].

The research document "A Study on Leveraging Blockchain Technology for IoT Security Enhancement" investigates how Blockchain technology solves security and privacy problems in IoT systems. Unprotected IoT devices face continuous threats from attackers due to their deployment in exposed locations. The paper demonstrates how blockchain's decentralized system with its unalterable features functions as a protected and transparent information exchanging framework. The research describes implementation examples and evaluates the existing obstacles in joining Blockchain and IoT systems. Obstacles in Blockchain-IoT integration stem from performance limitations along with energy consumption problems as well as compatibility issues that stem from the absence of standardized practices. Researchers explore the development of combined blockchain-edge-cloud solutions to address security demands and scalability requirements while optimizing efficiency. Secure lightweight consensus protocols which suit IoT requirements and new privacy methods need development to establish IoT data protection alongside Blockchain benefits[9].

This paper “A Multiple Blockchains Architecture On Inter-Blockchain Communication” delivers an innovative architectural solution that combines blockchain technology to overcome scalability limits in individual blockchain networks. The proposed blockchain system allows secure communication among blockchain networks through its 'router blockchain component.' The proposed system includes dedicated protocols which make sure cross-chain deals preserve their atomic status and consistency throughout the transaction process for unhampered blockchain agreement without mediator participation. Executed cross-blockchain transactions still face difficulties from complex protocols and escrow mechanisms which require many resources and the blockchain variation in transaction formats. Research efforts will centre on enhancing cross-link communication security measures as well as privacy protection and developing quicker consensus methods and standardized transaction formats for blockchains to easily integrate with one another[11].

"On blockchain and its integration with IoT. Challenges and Opportunities " examines how Blockchain resolves security problems as well as privacy concerns while handling IoT networks which continue their rapid growth expansion. The research explores the capabilities of Blockchain systems especially its distributed nature and unchangeable properties and trust less function as security enhancers for IoT systems that safeguard user data. The paper analyses Blockchain-IoT solutions while detailing the main problems involving resource limits together with delay issues and scalability challenges and privacy concerns and regulatory compliance matters. Scientific analysis examines how combining edge and fog computing with Blockchain technology forms a system that supports reduced latency and stronger scalability along with local data processing capabilities. The performance enhancement of resource-constrained IoT domains requires privacy-preserving Blockchain protocols which combine zero-knowledge proofs with lightweight consensus mechanisms[2].

The research paper “A Lightweight Hash-Based Blockchain Architecture for Industrial IoT” explores whether conventional Blockchain architecture works properly within limited Industrial IoT (IIoT) environments. The research tackles issues of high resource usage and latency and scalability through development of a lightweight hash-based Blockchain architecture for IIoT deployments. A streamlined hash function framework uses QUARK and SPONGENT and PHOTON hash functions for keeping operations resource lean. This system faces several drawbacks that impair its performance because it fails to guarantee privacy effectively while encountering scalability problems at scale and requiring specific hash functions that lead to traffic-related latency. Research will combine edge computing with zero-knowledge proofs and parallel hash functions to boost industrial Internet of Things privacy standards during implementation while achieving standardization across IIoT sectors[10].

Tikiri—Towards a Lightweight Blockchain for IoT provides an overview of the resource-efficient Blockchain solution geared toward IoT system requirements. Tikiri provides solutions to the three main Blockchain system problems related to high computational requirements and low transaction speed and scalability limitations. The network depends on Apache Kafka for consensus while using a microservices structure to enhance speed. The Tikiri system processes real-time transactions by means of a parallel operational method through the Validate-Execute-Group model. The platform faces several drawbacks consisting of privacy risks combined with traffic-related scalability problems and its dependence on external components along with complex system architecture. Future research will target three main objectives: distributed database integration for scalability along with privacy protocol enhancement and implementation of sharding-based consensus mechanisms and MQTT-based IoT secure device-to-device communication support[3].

The research paper " A Secure Communicating Things Network Framework for Industrial IoT using Blockchain Technology" introduces a Blockchain-enabled communicating things network framework which defends Industrial IoT (IIoT) networks by preventing data tampering along with unauthorized access and cyberattacks. Blockchain technologies work within the framework to leverage its protective capabilities with decentralized computing and cryptographic methods to strengthen IIoT device authentication and protect both data integrity and access protocols. The framework requires additional attention due to its poor scalability alongside delayed operations at high traffic conditions or resource shortages and privacy risks. Scientific inquiry integrates edge computing approaches to reduce delay times while establishing zero-knowledge proofs along with consensus mechanism enhancements to maximize energy use and developing protective protocols for critical IIoT infrastructure[6].

The research "A Lightweight Blockchain-Based IoT Identity Management Approach" introduces a lightweight consortium Blockchain-based framework to manage IoT identities. The framework replaces traditional centralized identity management singularity by spreading authority responsibilities over different organizations. Through distributed governance the framework enables secure privacy protections and decentralized governance in addition to identity management operations like verification and revocation. The main obstacles to this framework include difficulties in making it scalable along with problems related to privacy protection as well as challenges with connecting dispersed IoT systems. System testing in different IoT environments also poses challenges. Research in the future will investigate self-registering procedures in combination with multi-factor identity checks and new decentralized identity retrieval systems and improved privacy features implemented through zero-knowledge proofs[8].

The research paper ’LightChain: A Lightweight Blockchain System for Industrial Internet of Things’ introduces LightChain as an economical Blockchain solution designed for Industrial Internet of Things platforms. Standard Blockchain technology does not function well for IIoT because it demands excessive computational resources and network bandwidth. LightChain implements Synergistic Multiple Proof (SMP) consensus to optimize computation function and introduces a compact data format known as LightBlock. The solution features the Unrelated Block Offloading Filter (UBOF) which creates optimized blockchain development processes. In addition to these benefits the solution still faces challenges because of expansive network limits, privacy issues and requirements to run SMP and workload capacity of UBOF and increased implementation difficulty. Future research investigates how edge computing fits with blockchain systems and better privacy features and consensus protocol transformations and will validate LightChain through industrial-wide testing[5].

The article "Unleashing the Power of Internet of Things and Blockchain" conducts research on IoT-Blockchain through Latent Dirichlet Allocation (LDA) while surveying 4455 articles for analysis. The research study determines 14 thematic areas where IoT security stands alongside data privacy and healthcare management and energy optimization of wireless sensor networks. Three main problems exist in this research: it applies broad topics to the information, depends on summaries rather than full papers, and shows database filter selection bias while facing technological advancements. The future of research will focus on enhancing topic modelling approaches alongside privacy-protecting Blockchain protocol development and IoT-specific consensus solutions for new work across disciplines including climate forecasting and financial and urban development services[7].

III. Future Trends and Research Directions

Emerging Technologies:

Developing dynamic adaptive blockchain-based security protocol: The rapid development of IoT security threats necessitates the development of an adaptive security protocol capable of replying to newly evolved attack vectors and in that manner, the robustness of the blockchain based IoT solutions must be also considered. Towards predicting and counteracting security vulnerabilities of blockchain-IoT systems: The integration of blockchain and IoT systems needs to be more secure and data privacy should be up to the mark and mitigating potential vulnerabilities in blockchain and IoT systems upfront is proactiveness that increases security.

Examines blockchain as a method to improve IoT entry among “multi-cloud” and “edge computing” environments : As edge and cloud computing grow in scale and distributed devices proliferate in IoT systems, blockchain may offer improved security and interoperability for access control in these environments. Solutions on how blockchain can be used to enable edge computing in IoT and IIoT: Blockchain can significantly change the way data security, privacy and latency are enhanced in IoT systems by decentralizing processing at edge, and thus is an essential element to increase security and performance in the overall operation of IoT networks.

Exploring the possibility of integrating emerging technologies with learning and Blockchain systems: The integration of advanced technologies like edge and quantum computing with blockchain in IoT systems can improve computational efficiency and provide enhanced security and interoperability. Investigating the potential for blockchain to increase IoT entry control in “multi cloud” and “edge computing” platform : For cloud and edge computing which are ubiquitous, access control mechanisms should adapt. Understanding how Blockchain and AI can be integrated to produce intelligent and self-learning access control systems for IoT: It can improve the effectiveness and efficiency of access control system in IoT environment.

Lightweight Blockchain Solutions:

With an increasing number of IoT devices came the need to scale in order to accommodate the increasing data load and scalability, a basic requirement to securing and participating within large IoT ecosystems consideration for securing and interoperating within large IoT ecosystems.

Interoperable Frameworks:

Federated Blockchain model exploring the capabilities to increase data sharing and privacy in IoT and IIoT Ecosystems: Federated blockchain models complement large scale applications in IoT and blockchain because it improves scalability, interoperability and privacy to ensure secure and efficient data sharing. Relative studies of various Blockchain architectures for the entry control in IoT: Eventually, this will help in determining the most efficient and best models for implementation in case of specific use cases. Investigating dedicated IoT friendly blockchain consensus algorithms that will increase system performance and security.

Sustainability Concerns:

Specifically exploiting the best beneficial consensus algorithm for IoT environments. The proposed technique directly relates to the need of developing efficient “consensus algorithms” for enhancing the security and performance in blockchain based IoT devices to attain scalability and necessary processing of real time transactions. Looking into the portability problem of blockchain powered security solutions. With the bump in IoT objects likely to come an increased data load, a blockchain based security solution needs to be able to accommodate that sweeping growth. Investigations of how Zero Knowledge Proofs offer themselves as a means to facilitate access control in blockchain systems. Further helps improve user privacy because it lets users prove they can get to a resource without exposing who they are.

IV. CONCLUSION

Blockchain and IoT Integration can be seamlessly transformed to enhance data security and interoperability. Blockchain attempts to address this with the decentralization, immutability and transparency of blockchain in order to solve the problems of tampering of data, managing identities and privacy issues in IoT. Also, it makes IoT system safer, cuts the risks of Distributed Denial of Service (DDoS) attacks, and encrypts data sharing between devices. This convergence is applied to many areas. Blockchain secures data and service sharing in smart manufacturing; meanwhile, in healthcare it secures data management. Energy systems use blockchain for decentralized trading and grid management, supply chains benefit from increased transparency and traceability. Blockchain also improves smart cities by improving infrastructure and Wireless Sensor Networks (WSNs) with more efficiency and security. However, challenges persist. Blockchains are not able to scale to the massive data generated by the IoT, and have performance and constraints on network bandwidth, which make it impossible to perform real time functionality. Nevertheless, key barriers to overcome are un/reliable communication, block inconsistency and interoperability gaps between systems. Emerging solutions that bridge lightweight blockchain architecture, collaborate with edge computing and double chained security models can help overcome these hurdles. Future technology like 6G in the plans to increase the scalability and the interoperability for fast and reliable processes. The last part which is integrating IoT and blockchain is emerging to make industry revolutionize with secure, efficient and interconnected ecosystems are creating the space for innovation and resilience.

REFERENCES

1. Xu, L. D., Lu, Y., & Li, L. (2021). Embedding blockchain technology into IoT for security: A survey. *IEEE Internet of Things Journal, 8*(13), 10452–10473. https://doi.org/10.1109/JIOT.2021.3060508
2. Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT: Challenges and opportunities. *Future Generation Computer Systems, 88*, 173–190. https://doi.org/10.1016/j.future.2018.05.046
3. Bandara, E., Tosh, D., Foytik, P., Shetty, S., Ranasinghe, N., & De Zoysa, K. (2021). Tikiri—Towards a lightweight blockchain for IoT. *Future Generation Computer Systems, 119*, 154–165. https://doi.org/10.1016/j.future.2021.02.006
4. Sensors, J. O. (2024). Retracted: Next generation IoT and blockchain integration. *Journal of Sensors, 2024*, 1. https://doi.org/10.1155/2024/9896189
5. Liu, Y., Wang, K., Lin, Y., & Xu, W. (2019). LightChain: A lightweight blockchain system for industrial Internet of Things. *IEEE Transactions on Industrial Informatics, 15*(6), 3571–3581. https://doi.org/10.1109/TII.2019.2904049
6. Rathee, G., Sharma, A., Kumar, R., & Iqbal, R. (2019). A secure communicating things network framework for industrial IoT using blockchain technology. *Ad Hoc Networks, 94*, 101933. https://doi.org/10.1016/j.adhoc.2019.101933
7. Rejeb, A., et al. (2024). Unleashing the power of Internet of Things and blockchain: A comprehensive analysis and future directions. *Internet of Things and Cyber-Physical Systems, 4*, 1–18. https://doi.org/10.1016/j.iotcps.2023.06.003
8. Bouras, M. A., Lu, Q., Dhelim, S., & Ning, H. (2021). A lightweight blockchain-based IoT identity management approach. *Future Internet, 13*(2), 24. https://doi.org/10.3390/fi13020024
9. Muzammal, S. M., & Murugesan, R. K. (2018). A study on leveraging blockchain technology for IoT security enhancement. In *2018 Fourth International Conference on Advances in Computing, Communication & Automation (ICACCA)* (pp. 1–6). IEEE. https://doi.org/10.1109/ICACCAF.2018.8776806
10. Seok, B., Park, J., & Park, J. H. (2019). A lightweight hash-based blockchain architecture for industrial IoT. *Applied Sciences, 9*(18), 3740. https://doi.org/10.3390/app9183740
11. Kan, L., Wei, Y., Muhammad, A. H., Siyuan, W., Gao, L. C., & Kai, H. (2018). A multiple blockchains architecture on inter-blockchain communication. In *2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)* (pp. 139–145). IEEE. https://doi.org/10.1109/QRS-C.2018.00037
12. Bai, L., Hu, M., Liu, M., & Wang, J. (2019). BPIIoT: A light-weighted blockchain-based platform for industrial IoT. *IEEE Access, 7*, 58381–58393. https://doi.org/10.1109/ACCESS.2019.2914223
13. Al-Shammari, N. K., Syed, T. H., & Syed, M. B. (2021). An Edge–IoT framework and prototype based on blockchain for smart healthcare applications. Engineering, Technology & Applied Science Research, 11(4), 7326-7331.