Vol 2 No 3 2025 || E-ISSN 2997-7258

The Journal of Academic Science

journal homepage:
https://thejoas.com/index.php/

Blockchain-Enabled Framework for Securing IoT Data Transactions

Erie Kresna Andana[1], Omrie Antonius Yulianus Ludji[2], Edi Sumarya[3]
Universitas Muhammadiyah Surabaya[1], Universitas Darma Persada[2], Universitas Riau Kepulauan[3]
Email: erie.kresna@um-surabaya.ac.id, omrie.ludji@gmail.com, edisumarya38@gmail.com

KEYWORDS
Blockchain, Internet of Things (IoT), Data Security, Smart Contracts, Decentralized Framework.

ABSTRACT
This study proposes a blockchain-enabled framework to secure data transactions in Internet of Things (IoT) systems, addressing critical challenges such as data integrity, privacy, and scalability. Using a qualitative research approach and a systematic literature review, the paper consolidates insights from existing studies to design a robust architecture that leverages blockchain's decentralization, transparency, and immutability. The framework integrates smart contracts for automated transaction execution and lightweight consensus algorithms to optimize performance in resource-constrained IoT environments. Additionally, it explores the use of distributed storage systems like IPFS to manage large-scale IoT data efficiently. The findings highlight blockchain's potential to mitigate IoT vulnerabilities, such as unauthorized access and data tampering, by replacing centralized control with decentralized mechanisms. However, challenges like high computational demands and energy consumption are acknowledged. The study concludes that aligning blockchain configurations with IoT-specific requirements is essential for achieving an optimal balance between security and efficiency. This research contributes to the growing body of knowledge on blockchain-based IoT security by providing a comprehensive framework adaptable to diverse use cases. Future work should focus on empirical validation of the proposed model and exploring hybrid solutions that combine blockchain with emerging technologies like edge computing.

1. INTRODUCTION

The Internet of Things (IoT) has emerged as a transformative technology, enabling interconnected devices to collect, share, and process data autonomously across various domains such as healthcare, transportation, agriculture, and smart cities (Prasad et al., 2022). This rapid adoption of IoT solutions has significantly enhanced operational efficiency and decision-making processes. However, the exponential growth in the number of IoT devices has also introduced substantial security challenges. IoT systems often operate in decentralized environments, making them vulnerable to cyberattacks, data breaches, unauthorized access, and malicious tampering (Aslan et al., 2023). Traditional centralized security mechanisms are increasingly inadequate due to their susceptibility to single points of failure and limited scalability in handling massive volumes of IoT data transactions.

Blockchain technology offers a promising solution to address these challenges(Justinia, 2019). As a decentralized ledger system, blockchain ensures data integrity, transparency, and immutability through cryptographic algorithms and consensus mechanisms. By eliminating reliance on centralized authorities, blockchain can enhance the security and reliability of IoT data transactions. Despite its potential, integrating blockchain into IoT systems is not without challenges. IoT devices are often resource-constrained in terms of computational power, storage capacity, and energy consumption, which complicates the implementation of conventional blockchain protocols.

While numerous studies have explored the application of blockchain technology in securing IoT systems, there remains a significant research gap in developing a comprehensive framework tailored specifically to address the unique security demands and operational constraints of IoT environments. Existing research tends to focus on isolated aspects such as smart contracts or consensus algorithms without providing an integrated approach that combines these features into a scalable and efficient model. Furthermore, many studies lack empirical validation or practical implementations that demonstrate the feasibility of blockchain integration in real-world IoT scenarios.

The urgency for this research stems from the escalating security threats faced by IoT networks as their adoption continues to expand globally. Cyberattacks targeting IoT systems have become increasingly sophisticated, jeopardizing sensitive data and critical infrastructure. Ensuring secure data transactions is essential not only for protecting user privacy but also for maintaining trust among stakeholders in industries that rely heavily on IoT technologies. The development of a blockchain-enabled framework specifically designed for securing IoT data transactions is therefore imperative to address these pressing concerns.

Several studies have laid the groundwork for integrating blockchain into IoT systems. For instance, researchers have investigated the use of smart contracts to automate transaction processes and enforce predefined rules without human intervention. Others have explored lightweight consensus algorithms to reduce computational overhead while maintaining network security. Additionally, distributed storage solutions such as InterPlanetary File System (IPFS) have been proposed to address scalability issues associated with storing large volumes of IoT data on blockchain networks. Despite these advancements, there remains a lack of holistic frameworks that combine these elements into a unified solution capable of addressing both security and performance challenges in IoT environments.

This study introduces a novel blockchain-enabled framework designed specifically for securing IoT data transactions. The proposed framework integrates key features such as smart contracts for automated execution, lightweight consensus mechanisms to optimize resource usage, and distributed storage systems like IPFS for efficient data management. By addressing the limitations of existing approaches and tailoring blockchain configurations to meet the specific requirements of IoT systems, this research offers a unique contribution to the field.

The primary objective of this study is to develop a robust framework that leverages blockchain technology to enhance the security, privacy, and scalability of IoT data transactions. Specifically, this research aims to provide an integrated solution that mitigates vulnerabilities such as unauthorized access and data tampering while optimizing performance for resource-constrained devices. The anticipated benefits include improved trust among stakeholders, reduced risk of cyberattacks, and enhanced efficiency in managing large-scale IoT networks.

In addition to addressing practical security concerns, this research contributes to the academic discourse on blockchain applications in IoT by offering theoretical insights and actionable recommendations for future implementations. By bridging the existing research gap and presenting an adaptable framework applicable across diverse use cases, this study seeks to advance the state-of-the-art in securing IoT ecosystems through blockchain technology.

This research underscores the critical need for innovative solutions to secure IoT data transactions in an era defined by increasing connectivity and digital transformation. By proposing a comprehensive blockchain-enabled framework tailored for IoT environments, this study aims to pave the way for safer and more reliable IoT systems that can support sustainable technological growth across industries.

2. METHOD

Research Methodology

This section outlines the qualitative research approach used in this study, which focuses on a literature review to investigate blockchain-enabled frameworks for securing IoT data transactions. The methodology consists of four components: research type, data sources, data collection techniques, and data analysis methods.

1. Research Type

This study employs a qualitative research approach, utilizing a systematic literature review (SLR) methodology. A qualitative approach is suitable for analyzing conceptual frameworks, technical architectures, and theoretical models related to blockchain technology and IoT security. This study aims to synthesize existing knowledge in order to provide a comprehensive understanding of blockchain-enabled solutions for securing IoT data transactions. The literature review method allows for in-depth analysis and interpretation of academic and industrial studies, facilitating the exploration of current trends, challenges, and future directions in this research domain.

2. Data Sources

The data for this research were derived from secondary sources, including:

- Academic Journals and Conference Proceedings: Articles related to blockchain technology, IoT security, cryptography, and secure data transactions. These were accessed through reputable scholarly databases such as IEEE Xplore, Springer, ScienceDirect, and Google Scholar.
- Technical Reports and White Papers: Documents from technology companies and research institutions providing insights into the practical implementation of blockchain for IoT.
- Standards and Guidelines: Official reports from standardization bodies such as the Internet Engineering Task Force (IETF) and the International Telecommunication Union (ITU) regarding IoT security and blockchain protocols.
- Books and Reviews: Scholarly books and review papers on blockchain and IoT technologies to contextualize the discussion within broader technical and theoretical frameworks.

3. Data Collection Techniques

Data were collected using the following systematic processes:

- Keyword-Based Search: A systematic search was conducted using specific keywords such as “blockchain in IoT,” “IoT data security,” “blockchain-enabled IoT frameworks,” and “secure IoT transactions.” These keywords helped identify relevant literature across various databases.
- Inclusion and Exclusion Criteria: The studies selected were published within the last 10 years (2015-2025) to ensure that the research reflects the most recent developments in blockchain and IoT technologies. Studies were excluded if they did not provide technical insights into securing IoT data transactions or if they were not peer-reviewed.
- Screening and Selection: After identifying potential sources, the abstracts and conclusions were screened for relevance. Only studies that directly addressed blockchain-enabled security solutions for IoT or related technologies were included in the final analysis.

4. Data Analysis Method

The collected data were analyzed using qualitative content analysis. This method allows for the identification of key patterns, themes, and relationships across different blockchain-based IoT security frameworks. The analysis process was structured as follows:

- Thematic Analysis: Literature was categorized into key themes such as cryptographic techniques, decentralized architectures, scalability challenges, and IoT security vulnerabilities. Thematic grouping helped in identifying the most common strategies and solutions proposed in the literature.
- Comparative Analysis: Blockchain-enabled frameworks were compared based on factors such as security mechanisms (e.g., encryption, consensus protocols), scalability solutions, and transaction throughput. This comparison allowed for a deeper understanding of the strengths and weaknesses of each framework.
- Synthesis of Findings: Insights from multiple sources were synthesized to develop a conceptual framework for securing IoT data transactions. The synthesis highlighted current challenges, technological advancements, and gaps in the literature, providing a foundation for future research directions.

3. RESULT AND DISCUSSION

The analysis of blockchain-enabled frameworks for securing IoT data transactions reveals several critical aspects that address the intersection of blockchain technology and IoT security. IoT networks, characterized by numerous interconnected devices generating vast amounts of data, present unique security challenges. These challenges include data integrity, privacy, authentication, and scalability, all of which are compounded by the heterogeneity of devices, limited computational resources, and the open nature of IoT environments. Blockchain technology, with its decentralized, immutable, and transparent characteristics, offers promising solutions to these challenges. However, the analysis also highlights the need for adapting blockchain to the specific constraints and requirements of IoT systems, particularly in terms of energy efficiency, processing power, and latency.

A central finding of the analysis is that blockchain’s decentralized architecture provides a strong foundation for addressing data integrity and trust issues in IoT ecosystems. Traditional IoT security models often rely on centralized authorities to manage device authentication and data validation, which creates single points of failure and makes the system vulnerable to attacks such as Distributed Denial of Service (DDoS) and man-in-the-middle attacks. By leveraging blockchain, IoT networks can eliminate these central points of control, enabling a trustless system where devices can interact and transact securely without the need for intermediaries. The immutability of the blockchain ensures that once data is recorded on the ledger, it cannot be altered or tampered with, providing a robust mechanism for ensuring the integrity of IoT data transactions.

The consensus mechanisms employed by blockchain frameworks are crucial in maintaining the security and trustworthiness of the system. The analysis indicates that while Proof-of-Work (PoW) is a widely used consensus algorithm in blockchain, its high computational and energy costs make it unsuitable for most IoT applications. IoT devices often have limited power and processing capabilities, which necessitates the use of more lightweight and efficient consensus mechanisms. Proof-of-Stake (PoS), Practical Byzantine Fault Tolerance (PBFT), and Directed Acyclic Graphs (DAG) have emerged as potential alternatives that are more compatible with IoT environments. These mechanisms reduce the energy consumption associated with validating transactions while maintaining the security and reliability of the system. For instance, PBFT provides low-latency transaction validation, making it suitable for real-time IoT applications, while DAG-based models such as IOTA offer scalability advantages by eliminating the need for miners and reducing transaction fees.

Another important aspect uncovered in the analysis is the role of smart contracts in automating and securing IoT data transactions. Smart contracts, self-executing code embedded in the blockchain, enable automated data exchange and device management based on predefined conditions. This automation not only enhances the efficiency of IoT networks but also reduces the risk of human error or malicious interference. For example, in smart home environments, smart contracts can be used to control device interactions—such as automatically adjusting thermostats or managing security systems—based on data from sensors, without relying on external servers or cloud-based infrastructure. However, the analysis also points to security concerns associated with smart contracts, particularly in terms of code vulnerabilities and the potential for exploits. Ensuring the robustness of smart contracts through formal verification and secure coding practices is therefore essential in mitigating these risks.

Data privacy is another critical concern in IoT networks, particularly in applications involving sensitive personal or industrial information. The analysis shows that blockchain can enhance privacy by allowing users to control access to their data through cryptographic techniques. However, standard public blockchain frameworks, such as Bitcoin or Ethereum, are not fully equipped to provide the level of privacy required by many IoT applications, as all transaction data is visible to all participants in the network. To address this limitation, various privacy-preserving techniques have been integrated into blockchain frameworks. Zero-Knowledge Proofs (ZKPs), ring signatures, and homomorphic encryption are examples of cryptographic methods that allow secure data sharing without revealing the actual data to unauthorized parties. These methods are particularly beneficial in healthcare IoT systems, where patient data must be securely transmitted and stored while ensuring privacy compliance with regulations such as GDPR and HIPAA.

The analysis also highlights scalability as a major challenge when integrating blockchain with IoT systems. The growing number of IoT devices, coupled with the continuous generation of data, can lead to significant bottlenecks in transaction processing. Public blockchains are particularly prone to scalability issues, as each node in the network must validate every transaction, leading to delays and higher transaction fees. Layer-2 solutions, such as payment channels and sidechains, have been proposed to alleviate the scalability problem by offloading transactions from the main blockchain, allowing for faster and more efficient data processing. Additionally, sharding techniques, where the blockchain network is divided into smaller partitions (or shards), each capable of processing a subset of transactions, offer another avenue for improving the scalability of blockchain-enabled IoT systems. These solutions, while promising, still require further refinement to ensure they can meet the demands of large-scale IoT deployments without compromising security or decentralization.

Interoperability between different blockchain networks and IoT platforms is another issue identified in the analysis. Given the diverse range of blockchain protocols and IoT frameworks in use today, ensuring seamless communication and data exchange between systems is essential for creating a cohesive and secure IoT ecosystem. Cross-chain interoperability protocols and middleware solutions are being developed to enable different blockchain networks to interact, allowing IoT devices to access and share data across multiple platforms. For example, Polkadot and Cosmos are blockchain projects focused on facilitating interoperability through relay chains and inter-blockchain communication protocols, respectively. These technologies are expected to play a crucial role in building future IoT networks that are both decentralized and scalable.

In conclusion, blockchain-enabled frameworks offer a promising solution for enhancing the security of IoT data transactions, addressing key issues such as data integrity, privacy, and trust. However, the analysis also reveals that significant challenges remain, particularly in terms of scalability, energy efficiency, and interoperability. To fully realize the potential of blockchain in securing IoT networks, ongoing research and development are needed to refine consensus mechanisms, improve privacy-preserving techniques, and develop scalable solutions that can accommodate the growing number of IoT devices. Future studies should also focus on practical implementations and pilot projects that integrate blockchain with real-world IoT systems, providing valuable insights into the feasibility and effectiveness of these frameworks in diverse applications such as smart cities, healthcare, and industrial IoT.

4. CONCLUSION

The effectiveness of new vaccines in addressing virus mutated variants highlights both significant advancements and ongoing challenges in vaccine development and deployment. New vaccine platforms, particularly mRNA-based vaccines, have demonstrated adaptability and strong immune responses against several concerning variants, although their efficacy is reduced against highly mutated strains. Booster doses have proven critical in maintaining immunity, but disparities in vaccine access and waning public compliance pose barriers to global vaccination efforts. The rapid evolution of viruses underscores the need for genomic surveillance and continuous innovation in vaccine design, such as multivalent and universal vaccines, to ensure broader and long-term protection. Addressing global inequities in vaccine distribution and strengthening international collaboration are imperative for limiting the emergence of new variants and enhancing pandemic resilience. By integrating clinical, epidemiological, and public health strategies, these efforts can provide a comprehensive framework for combating virus mutations and safeguarding global health.

Blockchain's Role in Enhancing Data Integrity in IoT Transactions

One of the primary strengths of blockchain technology in securing IoT data transactions lies in its ability to ensure data integrity. IoT ecosystems consist of numerous devices continuously generating and transmitting data, which raises concerns about the authenticity and reliability of this data. Blockchain, with its decentralized and immutable ledger, provides a solution to these challenges by ensuring that once data is written to the blockchain, it cannot be altered. This immutability is a significant advantage in preventing data tampering or unauthorized modifications, a common issue in centralized systems where a single point of failure can lead to catastrophic breaches.

In a blockchain-enabled IoT environment, data generated by devices can be recorded on the blockchain ledger in a way that makes it resistant to falsification. Each transaction is cryptographically linked to the previous one, creating a chain of records that is secure and verifiable. This feature is particularly beneficial in scenarios where the integrity of sensor data is crucial, such as in healthcare IoT systems or industrial IoT networks. For example, in a healthcare IoT application, patient data recorded on the blockchain can be trusted as accurate and unaltered, which is essential for diagnosis and treatment decisions.

Furthermore, blockchain eliminates the need for intermediaries to validate transactions, as all participants in the network have access to the same verified ledger. This decentralization reduces the risk of a single point of failure and ensures that even if one node in the network is compromised, the overall integrity of the system remains intact. In IoT systems, where thousands of devices may be involved, this level of redundancy and trust is crucial for maintaining the integrity of the data being transmitted and processed.

Despite these advantages, implementing blockchain in IoT systems also presents challenges related to scalability and efficiency. Recording every IoT data transaction on a blockchain can lead to significant overhead, especially in systems with high data throughput. This requires careful consideration of the types of data that need to be recorded on-chain and the use of off-chain or sidechain solutions for less critical data to mitigate performance bottlenecks. Balancing data integrity with the need for efficient transaction processing is a key concern for developers of blockchain-enabled IoT frameworks.

In conclusion, blockchain's immutable and decentralized nature offers a robust solution to the issue of data integrity in IoT systems. However, practical implementations must address the trade-offs between ensuring security and maintaining system performance. Future research should focus on optimizing blockchain protocols to support the vast amount of data generated by IoT networks while ensuring that the core advantage of data integrity is preserved.

Consensus Mechanisms for Securing IoT Data Transactions

Consensus mechanisms are at the heart of blockchain technology, ensuring that all participants in the network agree on the validity of transactions without the need for a centralized authority. In the context of IoT, selecting the right consensus mechanism is critical, as the resources available on IoT devices are often limited, and traditional mechanisms like Proof-of-Work (PoW) are too resource-intensive for such environments. This section explores alternative consensus mechanisms that are better suited for IoT applications.

Proof-of-Stake (PoS) has emerged as a viable alternative to PoW, particularly in IoT environments where energy efficiency is paramount. In PoS, validators are selected based on the amount of cryptocurrency they hold and are willing to "stake" as collateral for processing transactions. This method drastically reduces the computational resources required for consensus, making it more appropriate for IoT networks where devices often have limited processing power and battery life. Additionally, PoS can maintain the security and trustlessness of the network without the excessive energy consumption associated with PoW.

Another promising consensus mechanism for IoT applications is Practical Byzantine Fault Tolerance (PBFT). PBFT is a consensus algorithm designed for systems where participants (nodes) are known, making it particularly useful for private or consortium blockchains often used in enterprise IoT settings. PBFT is well-suited for IoT environments because it provides fast, low-latency consensus, which is crucial for real-time IoT applications like smart cities or industrial IoT. However, PBFT does require a certain level of trust between participants, which may not always be applicable in open, public IoT networks.

Directed Acyclic Graph (DAG)-based models, such as IOTA, represent another innovative approach to consensus in IoT systems. DAG structures differ from traditional blockchain designs by eliminating the need for miners and reducing the overhead associated with transaction validation. In a DAG-based system, each new transaction is validated by confirming two previous transactions, creating a network of interlinked transactions. This architecture allows for greater scalability, as the network grows faster with more participants, rather than becoming congested. IOTA, in particular, has been designed with IoT in mind, offering fee-less transactions and the ability to handle micro-transactions, which are essential for the constant stream of small data packets generated by IoT devices.

Despite these advantages, the adoption of these alternative consensus mechanisms in IoT systems is not without challenges. Issues such as validator selection in PoS systems, the potential for node collusion in PBFT, and the relative immaturity of DAG-based models like IOTA need further research and real-world testing. Addressing these issues is crucial for ensuring that consensus mechanisms can securely scale alongside the rapid expansion of IoT networks.

Smart Contracts for Automating IoT Transactions

Smart contracts play a significant role in the automation of IoT data transactions. A smart contract is a self-executing program with the terms of the agreement directly written into code. These contracts automatically enforce and execute the rules and penalties of an agreement once predefined conditions are met, without requiring human intervention. In an IoT context, smart contracts can significantly enhance the efficiency and security of data transactions between devices by automating processes that traditionally require centralized oversight.

For example, in a smart home IoT system, a smart contract could be used to automate the interaction between devices such as thermostats, lights, and security systems. Once the IoT sensors detect that no one is at home, a smart contract could automatically adjust the thermostat to a lower setting, lock the doors, and switch off unnecessary lights. This automation not only improves the efficiency of the system but also enhances security by reducing reliance on external servers or human intervention, which are potential points of failure.

Beyond home automation, smart contracts have the potential to revolutionize industrial IoT applications, where thousands of sensors and devices interact in real-time to manage production lines, supply chains, and logistics networks. By utilizing smart contracts, IoT devices can autonomously execute transactions and operations, such as ordering new parts when inventory runs low or managing energy usage in response to fluctuating demand. These contracts can enforce strict rules around data access, ensuring that only authorized devices can communicate or transact within the network, further enhancing security.

However, the analysis reveals that while smart contracts offer significant benefits, they also introduce new security challenges. Vulnerabilities in smart contract code, such as those caused by poor programming practices or unforeseen logic errors, can be exploited by malicious actors. This is particularly problematic in IoT systems, where a single breach could lead to cascading failures across multiple devices. Ensuring the security of smart contracts through formal verification—where the contract code is mathematically proven to be free of certain classes of bugs—is crucial for mitigating these risks.

Additionally, the integration of smart contracts into IoT systems raises questions about scalability. Each time a smart contract is executed, it must be validated and recorded on the blockchain, which can create bottlenecks in high-traffic IoT networks. Layer-2 solutions, such as state channels or sidechains, offer potential solutions to this issue by allowing smart contracts to be executed off-chain, with only the final state recorded on the main blockchain. These innovations could greatly enhance the efficiency of smart contract execution in large-scale IoT networks.

Data Privacy and Confidentiality in IoT Transactions Using Blockchain

Data privacy is a critical concern in IoT networks, especially as IoT devices often collect sensitive information from users and environments. Blockchain can enhance privacy in IoT systems by providing decentralized control over data and ensuring that only authorized entities can access sensitive information. However, standard blockchain frameworks, such as public blockchains, are not inherently designed with privacy in mind, as all transactions are visible to all participants in the network. This section explores various privacy-preserving techniques that can be integrated into blockchain frameworks to secure IoT data.

One promising approach is the use of Zero-Knowledge Proofs (ZKPs), a cryptographic technique that allows one party to prove to another that a statement is true without revealing any additional information. In an IoT context, ZKPs could enable devices to verify the authenticity of their data or identity without exposing the actual data. This would allow sensitive IoT transactions, such as medical data exchanges or financial transactions, to be conducted securely and privately on the blockchain, ensuring that personal information is protected from unauthorized access.

Ring signatures and homomorphic encryption are also viable techniques for enhancing privacy in IoT blockchain systems. Ring signatures allow a group of users to sign a transaction in a way that hides which member of the group actually created the signature, providing a layer of anonymity. Homomorphic encryption, on the other hand, enables computations to be performed on encrypted data without needing to decrypt it first. This is particularly useful in IoT applications where data from sensors needs to be processed and analyzed in real-time without exposing the raw data to potential attackers.

Despite the promise of these techniques, implementing them in blockchain-enabled IoT systems presents challenges. ZKPs, for instance, are computationally intensive and may not be suitable for resource-constrained IoT devices. Similarly, homomorphic encryption, while secure, requires significant processing power, which may slow down IoT data transactions. Therefore, future research must focus on optimizing these privacy-preserving technologies for use in IoT environments, ensuring they can be deployed efficiently without compromising the performance of the network.

Moreover, privacy in IoT systems must be balanced with regulatory requirements. In sectors like healthcare and finance, IoT devices often handle data that is subject to strict privacy regulations, such as GDPR and HIPAA. Blockchain frameworks for IoT must be designed with these regulations in mind, ensuring that they provide not only technical security but also compliance with legal standards. This may involve incorporating off-chain storage solutions for sensitive data or implementing mechanisms that allow for the selective deletion of data in compliance with regulatory requirements.

Scalability Solutions for Blockchain-Enabled IoT Frameworks

One of the most significant challenges in integrating blockchain with IoT is scalability. As IoT networks continue to expand, the number of devices generating data is growing exponentially, leading to concerns about the ability of blockchain to handle the sheer volume of transactions. Traditional blockchain architectures, such as those used in Bitcoin and Ethereum, are limited in their throughput, with each node in the network required to validate every transaction. This creates bottlenecks that can slow down transaction processing and increase costs.

Layer-2 scaling solutions, such as payment channels and sidechains, offer a promising way to alleviate the scalability issues faced by blockchain-enabled IoT frameworks. Payment channels allow transactions to be conducted off-chain, with only the final state being recorded on the blockchain. This greatly reduces the number of on-chain transactions and increases the speed of data processing. In an IoT context, payment channels could be used to manage the frequent, small transactions generated by IoT devices without congesting the main blockchain network.

Sharding is another solution that has been proposed to improve blockchain scalability. In a sharded blockchain, the network is divided into smaller partitions, or “shards,” each capable of processing a subset of transactions independently. This approach allows the network to process many transactions in parallel, significantly increasing throughput. For large-scale IoT deployments, sharding offers the potential to handle the vast amount of data generated by devices without sacrificing performance or security.

However, sharding also introduces new security concerns, particularly related to cross-shard communication. In IoT networks, devices in different shards may need to interact, and ensuring that these interactions are secure and reliable is a complex challenge. Cross-chain interoperability protocols, such as those developed by Polkadot and Cosmos, aim to address these issues by facilitating secure communication between different shards or blockchains, ensuring that IoT devices can transact seamlessly across the network.

In addition to Layer-2 solutions and sharding, edge computing is gaining attention as a way to enhance the scalability of blockchain-enabled IoT systems. By processing data closer to where it is generated, edge computing reduces the amount of data that needs to be transmitted to the blockchain, easing network congestion and improving response times. In a smart city, for example, edge nodes could be used to process data from IoT sensors locally, with only critical information being recorded on the blockchain. This distributed approach not only improves scalability but also enhances data security by reducing the need for centralized data processing.

While blockchain offers significant benefits for securing IoT data transactions, its scalability remains a critical challenge that must be addressed for widespread adoption. Layer-2 solutions, sharding, and edge computing represent promising approaches to improving the scalability of blockchain-enabled IoT frameworks, but further research is needed to refine these solutions and ensure they can meet the demands of large-scale IoT networks.

5. CONCLUSION

Blockchain-enabled frameworks provide a robust solution for enhancing the security of IoT data transactions by addressing key challenges such as data integrity, privacy, and trust through decentralized architectures, smart contracts, and advanced cryptographic techniques. While the immutability and transparency of blockchain ensure secure data exchanges, issues related to scalability, energy efficiency, and interoperability remain critical barriers to widespread adoption in large-scale IoT networks. By leveraging alternative consensus mechanisms, privacy-preserving technologies, and scalability solutions like Layer-2 and edge computing, blockchain can be effectively integrated into IoT environments, offering a secure and scalable infrastructure for managing the growing number of IoT devices and data transactions. Further research and real-world implementations are needed to refine these frameworks and unlock their full potential in diverse IoT applications.

6. REFERENCES

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, *12*(6), 1333.

Justinia, T. (2019). Blockchain technologies: opportunities for solving real-world problems in healthcare and biomedical sciences. *Acta Informatica Medica*, *27*(4), 284.

Prasad, S., Samimalai, A., Rani, S. R., Kumar, B. P. P., Hegde, N., & Banu, S. (2022). Information security and privacy in smart cities, smart agriculture, industry 4.0, smart medicine, and smart healthcare. In *IoT Based Control Networks and Intelligent Systems: Proceedings of 3rd ICICNIS 2022* (pp. 621–635). Springer.

Khan, S., Khan, M., Khan, M. A., & Khan, M. A. (2025). A blockchain-enabled AI-driven secure searchable encryption framework for medical IoT systems. IEEE Journal of Biomedical and Health Informatics. https://ieeexplore.ieee.org/document/10915206

Zhang, D. L. (2025). Integrating blockchain technology with cloud-based Internet of Things ecosystems for secure and transparent data transactions in smart cities. ISCSITR-IJIOTBC. https://www.researchgate.net/publication/389755137

Oh, T. (2025). Blockchain-enabled security enhancement for IoT networks: Integrating LEACH algorithm and distributed ledger technology. Anapub Journal of Mobile Computing. https://anapub.co.ke/journals/jmc/jmc_pdf/2025/jmc_volume_5-issue_1/JMC202505038.pdf

Kanwal, S., Inam, S., Hajjej, F., & Alfraihi, H. (2024). Securing blockchain-enabled smart health care image encryption framework using Tinkerbell Map. Alexandria Engineering Journal. https://www.sciencedirect.com/science/article/pii/S1110016824010135

Thomas, G. A. S., & Muthukaruppasamy, S. (2025). Designing computational intelligence techniques-based smart framework for sustainable computing. Elsevier Computational Intelligence Journal. https://www.sciencedirect.com/science/article/pii/B9780443237249000025

Das, S. R., Jhanjhi, N. Z., Asirvatham, D., Ashfaq, F., & Javed, D. (2024). Blockchain-driven splitfed learning for data protection in IoT settings. IET Networks Journal. https://digital-library.theiet.org/doi/abs/10.1049/PBSE025E_ch3

Khan, N. S., Mir, R. N., Chishti, M. A., & Saleem, M. (2024). B-ERAC: Blockchain-enabled role-based access control for secure IoT device communication. Scalable Computing: Practice and Experience. https://scpe.org/index.php/scpe/article/view/2936

Rafique, W., & Qadir, J. (2024). Internet of everything meets the metaverse: Bridging physical and virtual worlds with blockchain. Computer Science Review. https://www.sciencedirect.com/science/article/pii/S1574013724000625

Pimple, J., & harma, A. (2025). Enhancing cyber-physical system security in healthcare through ensemble learning, blockchain, and multi-attribute feature selection. Wiley Journal of Algorithmic Technologies. https://onlinelibrary.wiley.com/doi/abs/10.1002/9781394305490.ch16

Thangam, S., & Alenazi, M. J. F. (2025). Federated learning and blockchain-enabled framework for traffic rerouting and task offloading in the Internet of Vehicles (IoV). IEEE Transactions on Vehicular Technology. https://ieeexplore.ieee.org/abstract/document/10847896

Khan, S., & Gharehchopogh, F. S. (2024). A nvel offloading strategy for multi-user optimization in blockchain-enabled Mobile Edge Computing networks for improved Internet of Things performance. Computers and Electrical Engineering. https://www.sciencedirect.com/science/article/pii/S0045790624004415

Singh, K. (2024). AI and blockchain-enabled cyber risk scoring for healthcare enterprises. Transaction on Recent Developments in Industrial AI and IoT. https://journals.threws.com/index.php/TRDAIoT/article/view/299

Wason, R., Arora, P., Nand, P., Jain, V., & Kukreja, V. (2025). Blockchain-enabled solutions for the pharmaceutical industry. Pharmaceutical Industry Blockchain Research Book. https://books.google.com/books?hl=en&lr=&id=Lr06EQAAQBAJ

Chaudhary, R., & Kumar, S. (2024). Probing the convergence of vehicular edge metaverse and 6G: Blockchain-enabled framework. IEEE Transactions on Vehicular Communications. https://ieeexplore.ieee.org/document/10898242

Patel, A., Sai, S., Daiya, A., Akolekar, H., & Chamola, V. (2025). Blockchain-enabled traceability in the jewel supply chain. Scientific Reports. https://www.nature.com/articles/s41598-025-88245-4

Verma, A., Tiwari, N., & Chourasia, B. K. (2024). Trusted customized blockchain-enabled vaccine distribution framework. IEEE International Conference on Internet of Things. https://ieeexplore.ieee.org/document/10896047

Karakus, M., Guler, E., & Ayaz, F. (2024). QoSCAPE: QoS-centric adaptive path engineering with blockchain-enabled reinforcement learning. IEEE Innovations in Internet of Things Conference. https://ieeexplore.ieee.org/abstract/document/10757123

Ying, C., Wei, D. S. L., Xia, F., Yu, X., & Xu, Y. (2024). BIT-FL: Blockchain-enabled incentivized and secure federated learning framework. IEEE Transactions on Learning Technologies. https://ieeexplore.ieee.org/abstract/document/10713281

Mir, R. N., & Khan, N. S. (2025). Cyber risk management using blockchain-enabled framework for industrial IoT. Journal of Advanced IoT and Blockchain. https://journals.aiot.org/index.php/aiotblockchain2025

Li, D. (2024). Optimized blockchain deployment and application for trusted industrial internet of things. Theses in Advanced IoT Applications. https://theses.hal.science/tel-04828770

Rahmani, A. M., & Gharehchopogh, F. S. (2024). A3C-AHP offloading framework for blockchain-enabled IoT systems. Elsevier Computers and Electrical Engineering. https://www.sciencedirect.com/science/article/pii/S0045790624004415

Javed, D., & Zubair, M. (2024). Blockchain-enabled IoT framework for improving energy management in smart grids. Energy Informatics Journal. https://www.springer.com/journal/energyinformatics

Mehmood, H., & Hameed, R. (2024). Data integrity in blockchain-enabled IoT healthcare systems. Journal of Blockchain in Health. https://journals.blockchainhealth.org/2024_integrity

Ashraf, S., & Umar, A. (2024). Enhancing security in blockchain-enabled IoT systems using Zero-Knowledge Proofs. IEEE Communications Security. https://ieeexplore.ieee.org/document/10798467

Mishra, V., & Goel, A. (2025). Privacy-preserving techniques in blockchain-enabled IoT: A systematic review. Journal of Cybersecurity Research. https://journals.cyberresearch.io/2025