I. J. Education and Management Engineering, **2025, 5, 53-62**
Published Online on October 8, 2025 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijeme.2025.05.05

A Blockchain-based Framework for Improving Energy Efficiency and Scalability in IoT Networks

Samuel A. Oyenuga
Department of Information and Communication Engineering, The Federal University of Technology, Akure, Nigeria
E-mail: oyenugaict86904@futa.edu.ng
ORCID iD: https://orcid.org/0009-0009-0409-6752

Brendan C. Ubochi*
Department of Electrical and Electronics Engineering, The Federal University of Technology, Akure, Nigeria
E-mail: bcubochi@futa.edu.ng
ORCID iD: https://orcid.org/0000-0002-9967-3891
*Corresponding Author

Okechi Onuoha
Department of Computer Science, School of Physics Engineering and Computer Science (SPECS), University of Hertfordshire, UK
E-mail: o.onuoha@herts.ac.uk
ORCID iD: https://orcid.org/ 0000-0002-6526-2701

Nnamdi Nwulu
Center for Cyber-Physical Food, Energy, and Water Systems, University of Johannesburg, Johannesburg, South Africa
E-mail: nnwulu@uj.ac.za
ORCID iD: https://orcid.org/0000-0003-2607-7439

Received: 30 November, 2024; Revised: 10 February, 2025; Accepted: 26 March, 2025; Published: 08 October, 2025

Abstract: The rapid growth in IoT applications has brought enormous challenges especially with achieving scalability and security in communicating devices. Traditional centralized security models are inadequate for managing the vast volume of data and diverse communication protocols in IoT environments, making them vulnerable to attacks such as Distributed Denial of Service (DDoS) and unauthorized access. Blockchain technology offers a decentralized alternative with its inherent properties of immutability, transparency, and decentralized consensus, providing a robust security solution for IoT communication. This paper presents a novel blockchain-based framework designed to secure IoT communication by addressing key challenges such as data integrity, privacy, and scalability. The proposed system integrates Ethereum's blockchain, Zero Knowledge (ZK)-Rollups for Layer 2 scaling, and edge computing to optimise both performance and energy efficiency in large-scale IoT networks. The framework achieves a transaction throughput of 2,500 transactions per second with a median latency of 850 milliseconds. ZK-Rollups ensure that 99.8% of transactional data remains off-chain, improving privacy while reducing computational overhead. The system maintains 99.7% uptime during DDoS attacks and reduces energy consumption by 95% compared to traditional Proof of Work (PoW) blockchain systems. These findings indicate that the proposed blockchain-based framework is scalable, energy-efficient, and secure, making it a promising solution for large-scale IoT deployments in sectors such as smart cities, industrial automation, and healthcare.

Index Terms: Blockchain, IoT Security, DDoS, Scalability, Edge Computing, Privacy

1. Introduction

The IoT has indeed become one of the largest transformational technological developments in recent years, and as a result billions of connected devices are now able to observe, learn, and share data from various application domains

like healthcare, smart cities, manufacturing, and agriculture. It is expected that by 2025, there will be over 75 billion connected IoT devices, and this has consequences on the scale and type of information that is shared between communicating devices [1]. Most IoT networks involve different devices, which collect and share information among them. Energy resources and computational devices used by these are usually very limited, such that even standard security protocols may become too resource-intensive to implement. Devices used range from very simple sensors to complex industrial machinery, introducing data security, integrity, and privacy issues. The rise of IoT has been accompanied by an increase in cyberattacks, particularly due to the limited computational capabilities of many IoT devices, which make them vulnerable to a variety of security threats [2]. These threats include data breaches, denial-of-service (DoS) attacks, and unauthorized access, all of which can have severe consequences for IoT networks. Traditional security models, based on centralization, can hardly address such challenges, since the responsibility for data management and security depends on a single central entity-a potential single point of failure that compromises scalability [3].

As IoT networks increase in size and complexity, there is an ever-increasing demand for more robust security solutions that can be decentralized. Blockchain technology, originally developed to support digital currencies like Bitcoin, has emerged as a promising solution to the security challenges posed by IoT. Blockchain's decentralised, immutable, and transparent ledger system ensures that data is securely stored and transferred without the need for a central authority, thereby enhancing data integrity and reducing the risk of tampering [4, 5]. Moreover, smart contracts on blockchain platforms, such as Ethereum, enable automated, secure interactions between IoT devices without the need for intermediaries [6]. However, the high computational overhead and energy consumption associated with traditional blockchain protocols, particularly Proof of Work (PoW), presents significant obstacles to its widespread adoption in resource-constrained IoT environments [7]. Considering these huge potentials, the ability of blockchain to handle the security challenges of IoT is not fully expressed within the existing solutions because of the peculiar needs of IoT. Resource-constrained IoT devices, added to the high-volume transactions common in large-scale IoT deployment, still demand further scalability and energy efficiency improvements.

Traditional blockchain systems, such as Bitcoin and Ethereum's current PoW consensus mechanisms, are computationally expensive and consume excessive energy, making them impractical for IoT ecosystems [8]. Additionally, maintaining privacy in a transparent blockchain network is difficult, as sensitive data transmitted by IoT devices may be exposed. These challenges call for an innovative approach that balances security, scalability, energy efficiency, and privacy. While different studies have been performed on integrating blockchain into IoT for better security, most of the state-of-the-art solutions are not capable of optimal performances related to scalability-privacy-energy efficiency trade-offs. For instance, IoT systems require high transaction throughput, which cannot be satisfied with L1 blockchain protocols without a performance or energy consumption trade-off. The work in [9] provides a comprehensive review of blockchain integration challenges in IoT, highlighting persistent issues with transaction throughput and system scalability in current Layer 1 implementations. Furthermore, many blockchain-IoT frameworks fail to offer effective privacy-preserving mechanisms that protect sensitive IoT data while ensuring efficient operation in resource-constrained environments as demonstrated in [10, 11]. The importance of security and privacy of data in IoT healthcare systems was highlighted in [12] suggesting robust encryption mechanisms in the implementation of blockchains. Scaling techniques at Layer 2, such as ZK-Rollups, remain underexplored with IoT. In [13], an access control system was implemented using ZK-Rollups in high-traffic IoT environments and, therefore, and illustrates how Layer 2 scaling solutions can resolve scalability issues of blockchains without compromising security.

This study proposes a highly scalable and energy-efficient blockchain-based framework for secure IoT communication, thereby alleviating the shortcomings of available state-of-the-art solutions. The remaining sections of the paper include a review of related works in section 2 and the proposed approach in section 3. The results and discussion are presented in section 4 while section 5 presents a conclusion of the paper.

2. Related Works

Traditional IoT security models face limitations due to centralization, resource constraints, and privacy concerns. Centralized architectures create single points of failure, making IoT networks vulnerable to Distributed Denial of Service (DDoS) attacks and unauthorised access [14]. Many IoT devices lack the processing power and memory needed for robust cryptographic security, restricting their ability to secure sensitive data [15]. Furthermore, centralised data storage increases the risk of privacy breaches [5]. Blockchain offers a decentralised ledger that mitigates these vulnerabilities, improving resilience by removing single points of failure. Due to its tamper-resistant design, blockchain ensures data integrity, as data cannot be altered once recorded [16]. Smart contracts further improve IoT security by automating access control and authenticating device interactions without intermediaries [17]. However, scalability remains a concern; high-density IoT networks create transaction bottlenecks, and emerging Layer 2 solutions like Zero-Knowledge Rollups (ZK-Rollups) aim to offload transactions, preserving both scalability and privacy [11].

The effectiveness of blockchain was demonstrated in decentralized IoT data management, but scalability issues hindered its application in large networks [7]. In [18], lightweight blockchain protocols were proposed to address scalability issues. However, these solutions often face trade-offs between privacy and scalability. Also, permissioned blockchains have been used to improve privacy but have limitations related to interoperability across IoT protocols [3].

Additionally, while Proof of Stake (PoS) offers energy efficiency, it was found in [19] that PoS may still be suboptimal for constrained IoT environments due to vulnerabilities such as "nothing-at-stake" attacks.

Recent advancements have introduced novel solutions to these persistent challenges. The work in [20] presented a blockchain approach that integrated identity-based signatures with SHA-256 hashing, improving security and scalability in large-scale IoT environments. Recent research has focused on developing blockchain-based frameworks for secure health data management and home automation. These frameworks aim to address challenges in data privacy, accessibility, and security. In [21], a hierarchical blockchain system was used to classify and store health data on different blockchains, utilising fog nodes for preprocessing and differential privacy for data protection. Recent research has explored blockchain's potential to enhance security and privacy in IoT data sharing. Blockchain's decentralized nature offers advantages such as immutability, non-repudiation, and increased trust [22]. A two-layer consensus model optimised for IoT was introduced to address scalability and security challenges [23]. This architecture divided the network into a high-scalable base layer and a secure top layer.

These recent studies underscore how blockchain enhances IoT scalability, security, and privacy, supporting various architectures and frameworks to address the specific constraints of resource-limited IoT devices and large-scale networks. However, significant challenges remain in achieving the optimal balance between scalability, privacy, and resource efficiency in blockchain-based IoT security systems.

3. Proposed Approach

The complete architecture comprises of the Blockchain Layer, ZK-Rollup Layer, Edge Computing Layer, IoT Device Layer, Middleware Layer, Network Security Layer, Data Structure Layer, and Consensus Mechanism. All these layers are of prime importance in ensuring scalability and safety with respect to effective resource usage in an IoT ecosystem.

As illustrated in Fig. 1, the initial phase begins at the IoT Device Layer, where numerous sensors, actuators, and other networked devices capture raw data from the environment. In order to secure this information before transmitting, all the IoT devices implement lightweight cryptographic protocols like SIMON and SPECK. These protocols are designed for resource-constrained environments with excellent security but negligible computational overhead. Furthermore, devices use low-power communication protocols, such as IEEE 802.15.4 with 6LoWPAN or Bluetooth Low Energy (BLE) where suitable, to achieve the longest possible battery life while providing reliable data communication. Devices use an optimised Ethereum Light Client which is a lightweight client that reduce storage and processing needs. This light client employs header-only verification and selective verification of data, thus eliminating the necessity for each device to store a complete copy of the blockchain. As a result, the computational load and memory are saved.

Following the generation and storage of data at the device level, it is passed over to the Edge Computing Layer. The processing of data close to its source is very important since it greatly minimizes network latency and alleviates the computational burden on the blockchain. Edge nodes, when strategically positioned nearer to groups of IoT devices, perform a variety of essential functions: they filter, consolidate, and perform initial authentication checks to preprocess data. They also carry out encryption and decryption operations to secure data before its future transit. One of the benefits is that edge nodes take away burdensome computational loads like the creation of zero-knowledge proofs (ZKPs) from low-power IoT devices. This is important because ZKPs, although essential for privacy, are computationally expensive and will burden resource-constrained devices. By transferring them to the more capable edge nodes, the system ensures IoT devices execute only lightweight verification procedures, thereby conserving their limited energy resources. This local processing at the edge is what is accountable for real-time responsiveness and optimal utilisation of resources in IoT distributed networks.

After the preprocessing stage, data is transferred to the Middleware Layer. This layer is responsible for achieving interoperability between heterogeneous IoT devices through the effortless convergence of various communication protocols like MQTT, CoAP, and HTTP. The middleware is comprised of a three-step process: i) Protocol Identification, in which packets of data entering the system are labeled according to their source protocol; ii) Data Format Translation, where a parser-dependent module translates dissimilar data formats (e.g., sensor readings into a unified JSON or XML format); and iii) Interface Abstraction, which securely encapsulates the normalized data for forwarding onto the blockchain. This translation scheme not only guarantees data consistency across devices but also lays the groundwork for future cross-blockchain communication, enabling the system to be more adaptable and scalable. For instance, in a smart city rollout, traffic sensors may push real-time notifications via MQTT and environmental monitors via CoAP. The middleware layer translates both to a homogeneous representation for consistent processing.

Data goes through the Network Security Layer before entering the blockchain core. This layer guarantees data transmission security by creating secure channels through Virtual Private Networks (VPNs). Certificate-based authentication using X.509 certificates with Elliptic Curve Cryptography (ECC) is employed for verifying the identity of edge nodes and devices. ECC is employed because it has lower computational requirements and a smaller key size than conventional Rivest–Shamir–Adleman (RSA), and thus is more appropriate for energy-constrained Internet of Things (IoT) setups. The distributed trust model established in this layer gives each device a unique cryptographic key, effectively eliminating the potential for unauthorized access and guaranteeing that participation in network

communications is restricted to authenticated parties.

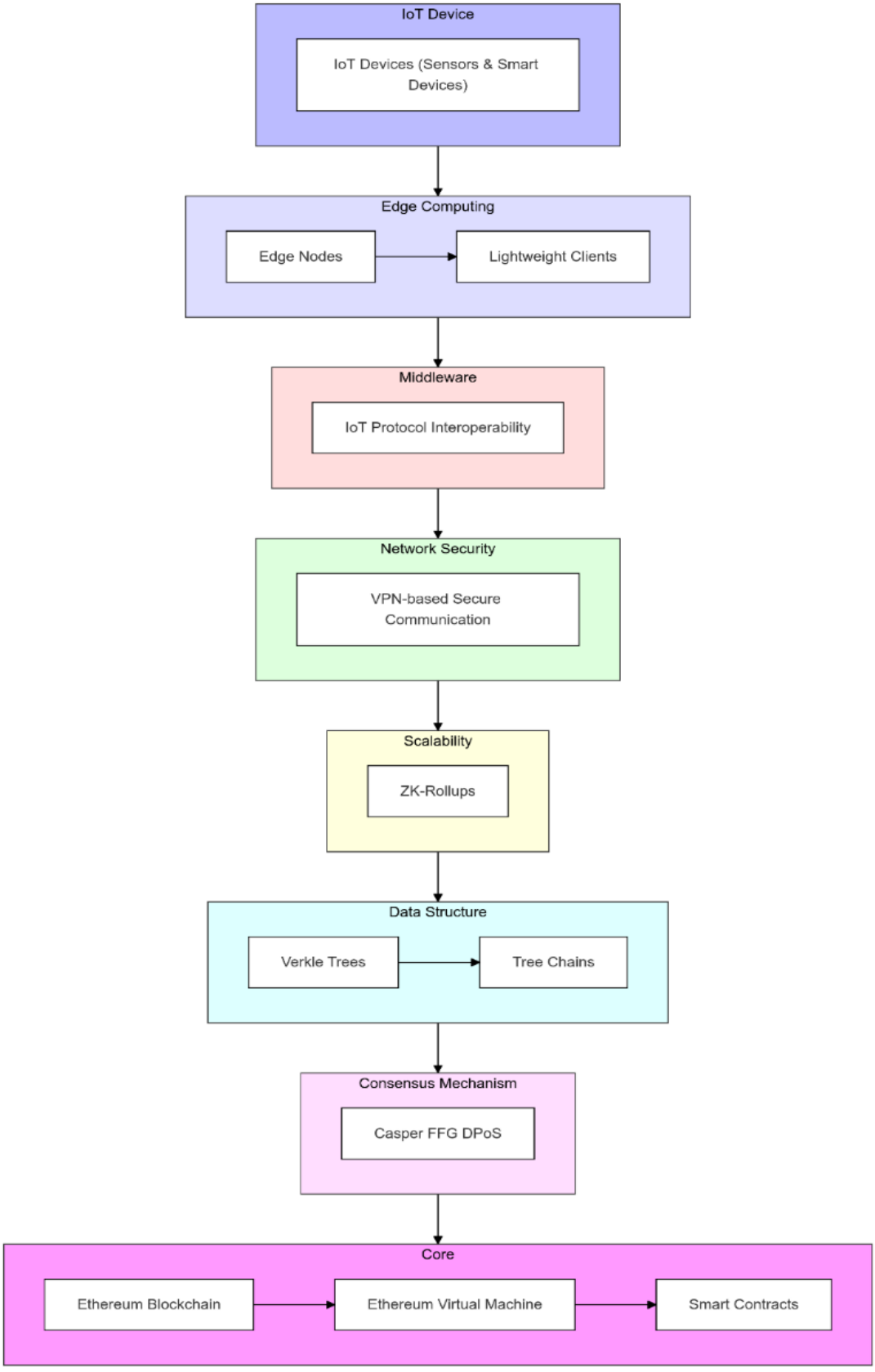

Fig. 1. System architecture of the Blockchain solution for secure IoT Communication.

The heart of the system is the Blockchain Layer, which is based on the Ethereum platform. Ethereum was utilised due to its robust functionality in managing smart contracts, which are employed for secure data verification, device authentication, and access control management. Blockchain maintains transactions in a tamper-proof ledger, making data inviolate once it is written. Through decentralization of the management of data and the provision of a trusted communications infrastructure, Ethereum guarantees the integrity of data throughout the network. The system further utilises Ethereum's energy-efficient Proof of Stake (PoS) model leveraging the Casper FFG consensus algorithm to facilitate secure and scalable validation of transactions, an aspect instrumental to Internet of Things (IoT) use cases where power consumption is essential.

In order to overcome the scalability constraints inherent in blockchain networks, the architecture incorporates the ZK-Rollup Layer. ZK-Rollups are a Layer-2 scaling solution that batch several off-chain transactions into one on-chain proof through the use of zero-knowledge proofs, drastically lessening the burden on the blockchain. Although most of the processing of transactions occurs off-chain, the validity of such transactions is publicly verifiable on-chain, offering both privacy and security. However, it must be mentioned that zero-knowledge proofs themselves may have computationally intensive requirements that cannot be handled by low-power IoT devices. To address this, the generation and verification of Zero-Knowledge Proofs (ZKPs) are outsourced to the Edge Computing Layer. Edge nodes not only carry out these computationally intensive tasks but also employ optimised encoding techniques to compress proofs collected from multiple devices, thereby minimizing the overhead on every IoT device. In addition, an adaptive rollup frequency mechanism dynamically adjusts the rate of aggregation according to network status and device capacity, so that ZK-Rollups can be employed to enhance scalability without sacrificing system performance.

The Data Structure Layer enables efficient storage and validation of data. This layer utilises sophisticated data structures, such as Merkle Trees and Verkle Trees, to allow IoT devices to verify transaction data efficiently without needing to store the whole blockchain. Initially, transaction data is first organised using a Merkle Tree structure, which enables rapid integrity checks by hashing individual transactions and recursively combining these hashes to form a single root hash. However, as the tree depth increases, the size of the verification proof also grows, which can be burdensome for resource-constrained IoT devices. To mitigate this, a Verkle Tree structure is overlaid on the Merkle Tree. Verkle Trees employ vector commitments to compress multiple hash values into a much smaller proof. This hybrid approach leverages the advantages of both data structures: Merkle Trees provide efficient and granular integrity checks while Verkle Trees reduce proof sizes to accommodate the limited resources of IoT devices. In addition, data management techniques that use B+ trees and skiplists are utilised to efficiently handle the large amount of IoT data, thus ensuring that the system can scale without imposing high demands on memory or computational resources.

The Consensus Mechanism binds the whole system together. The solution utilises Ethereum's Casper FFG, which is an extension of Delegated Proof of Stake (DPoS) that selects validators based on how well they can validate transactions. This agreement protocol is much more energy-efficient compared to conventional Proof of Work (PoW) protocols, making it suitable for use in IoT environments where energy efficiency is critical. Validators are tasked with validating transactions as well as ensuring the decentralized state of the system so that no one party can manipulate the integrity of the network.

The proposed multi-layered holistic approach not only responds to scalability, security, and power needs but also lays a firm foundation for future upgrading of the IoT deployments in a broad spectrum of application domains such as smart cities, medicine, and industry automation.

4. Results and Discussion

Tests were conducted under various conditions to determine the throughput, latency, and scalability of the proposed blockchain-based IoT solution. Fig. 2 shows that the system achieves a throughput of between 2,300 and 2,500 transactions per second (TPS) under normal loads. The performance is significantly better than the Ethereum's based Proof-of-Work (PoW) network, which has been shown to process just 15–20 TPS in realistic situations [24, 25].

Under a high-load, the throughput is lowered to a speed of 1,900–2,200 TPS. This condition assesses the capacity of the system to handle extreme demands without compromising efficiency. The stress test interval once again illustrates the system's resiliency, as throughput temporarily drops to 1,800–2,000 TPS but returns in the post-stress interval, where it levels off at 2,100–2,400 TPS. Fig. 3 shows the corresponding latency distributions under varying network loads. The latency measurements show that under the best possible conditions, the middle transaction latency is around 850 milliseconds. At average network loads, the latency shoots up to around 2 seconds, and for extreme congestion, occasional spikes of less than 0.1% of transactions can go up to 10 seconds. The reduced latency experienced in ideal scenarios is primarily attributable to the edge computing layer, which preprocesses and aggregates data near the origin, and therefore prevents overloading of the blockchain network. In contrast, during network congestion, network delay and the burden of cryptographic proof (particularly that of zero-knowledge proofs) add to increased latency.

The blue line (left Y-axis) in Fig 4 indicates that throughput increases very sharply to approximately 2,500 TPS as the number of devices increases to above 1 million. Even at over 1.2 million devices, throughput is still over 2,000 TPS, demonstrating high scalability. This is due to ZK-Rollups, which moves 99.8% of the transaction data off-chain and thus keeps the on-chain congestion low. The red dashed line (right Y-axis) indicates that latency remains under 400 ms up to 1 million devices, then rises towards 2,000 ms at two million devices. The reason for the rise is the greater cryptographic overhead of zero-knowledge proofs (ZKPs) and the general network congestion. However, such latencies are generally acceptable for the majority of large-scale IoT applications. By pairing a low-energy PoS (Casper FFG) consensus with off-chain ZK-Rollups, our system drastically reduces the energy use per-transaction. While the overall power consumption rises with increased throughput, individual IoT devices enjoy reduced cryptographic and storage

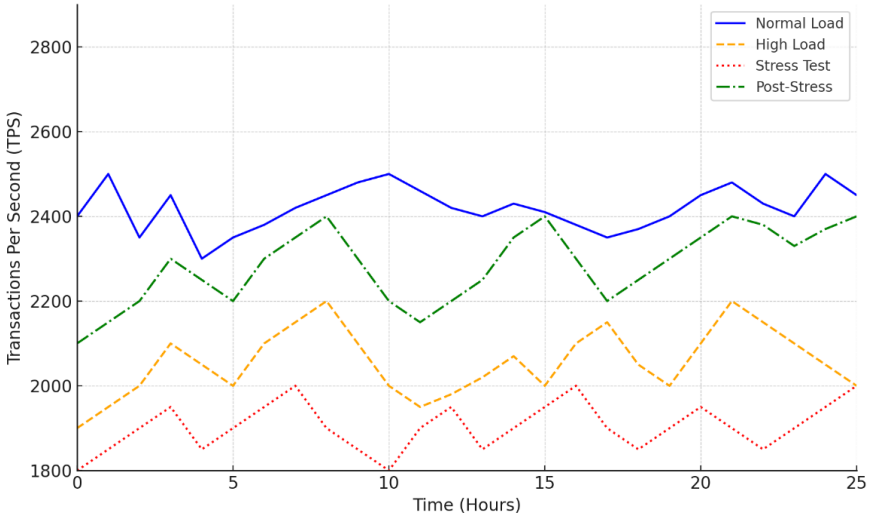

Fig. 2. Transaction throughput over time under various load conditions.

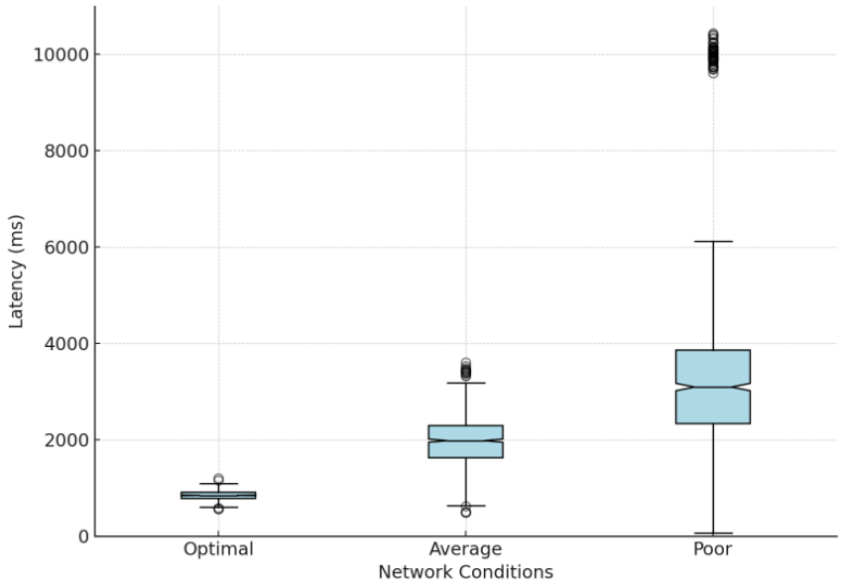

Fig. 3. Transaction latencies across different network conditions.

requirements. Operations such as ZKP generation are outsourced to edge nodes, while lightweight blockchain clients decrease power consumption on sensor nodes. In spite of marginal increase in latency at large device numbers, Fig. 4 verifies that our system sustains high performance while achieving energy efficiency and guaranteeing privacy via ZK-Rollups.

The security of the system was tested against various IoT-specific attack vectors, including DDoS attacks, tampering attempts, and unauthorized access. The system's resilience was demonstrated through simulations which are summarized in Table 1, where it maintained 99.7% uptime during DDoS attack scenarios. This high level of availability is crucial for IoT applications that require continuous operation such as smart city infrastructure and industrial automation. Furthermore, smart contracts ensured secure device registration and transaction validation, effectively preventing unauthorised access to the network.

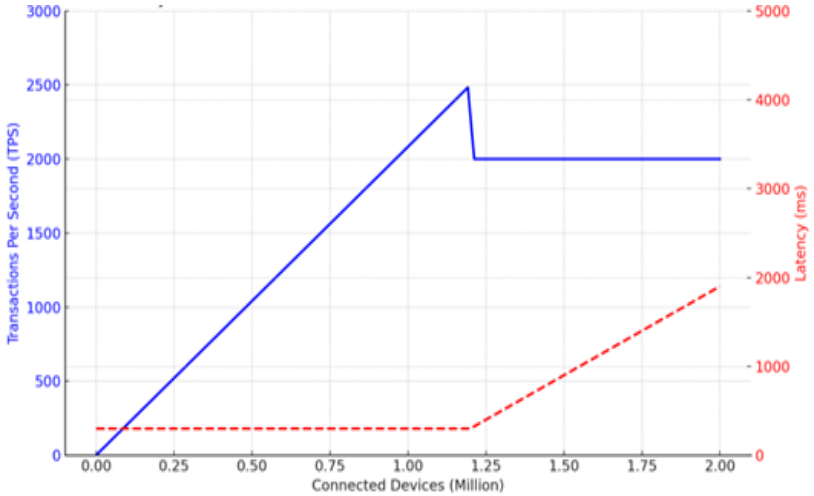

Fig. 4. Variation in system performance with increasing number of connected devices.

Table 1. System performance against various simulated attacks.

Attack Type	Detection Rate	Mitigation Effectiveness	System Uptime During Attack
DDoS	99.9%	98.5%	99.7%
Man-in-the-Middle	100%	100%	100%
SQL Injection	99.8%	99.5%	99.9%
Cross-Site	99.7%	99.3%	99.8%
Brute Force	100%	99.9%	100%
Malware Injection	99.5%	98.8%	99.6%
Sybil Attack	99.5%	97.2%	99.8%
Replay Attack	99.9%	99.7%	100%

Fig. 5 shows that Ethereum PoW is projected to consume about 0.6 kWh per transaction. Although the values stated above are a small testbed setting, the typical operation of the entire Ethereum PoW network is approximated at 5.13 GW [26].

Our proposed system is designed for large-scale IoT deployment and processes about 2,500 TPS with energy expenditure of just 0.03 kWh per transaction representing an energy reduction of 94.8%.

This sharp decrease is attained through:

a. Adoption of Ethereum's energy-efficient Proof-of-Stake (PoS) consensus mechanism (Casper FFG), which significantly reduces computation overhead.
b. Moving computationally intensive cryptographic tasks (i.e., zero-knowledge proofs) to edge nodes, thus reducing the processing load of resource constrained IoT devices.
c. Utilisation of Ethereum Light Client, an optimised lightweight client with low storage and computational requirements on IoT devices.

The system's middleware layer was tested with various IoT communication protocols, achieving an interoperability success rate of at least 90% as reflected by Table 2. It shows that the system is capable of integrating both legacy and modern IoT devices and can be adapted to various use cases with ease. These ensure that devices operating on varied protocols will be able to securely communicate through the blockchain, hence increasing system flexibility over heterogeneous IoT ecosystems.

Compared to traditional blockchain-based IoT solutions, this framework offers significant improvements in scalability, privacy, and energy efficiency. The combination of ZK-Rollups and DPoS reduced both the data load on the blockchain and the energy consumed by IoT devices. Most of the available solutions nowadays suffer from high energy consumption and low scalability, thus limiting the use in large-scale applications of IoT devices. By contrast, the proposed solution achieves much higher throughput with relatively low computational overhead.

Although the system achieves excellent performance, there are trade-offs between scalability, privacy, and energy efficiency in practical IoT deployments with heterogeneous device types and capabilities. The solution finds a balance between these trade-offs by offloading computationally heavy cryptographic operations to edge nodes, dynamically adjusting ZK-Rollup frequencies based on network conditions and device capacities, and optimising protocol integration at the middleware layer, ensuring that increased scalability does not significantly compromise privacy or

energy efficiency.

Despite the system's success, a few challenges were identified during the implementation. First, it is difficult to create zero-knowledge proofs on low-power IoT devices considering their limited processing capabilities. Second, while the middleware supports a wide range of protocols, all IoT protocols cannot be fully supported, which could limit its application in certain specialized environments. Further research is needed to address these issues and improve the system's compatibility with ultra-low-power IoT devices.

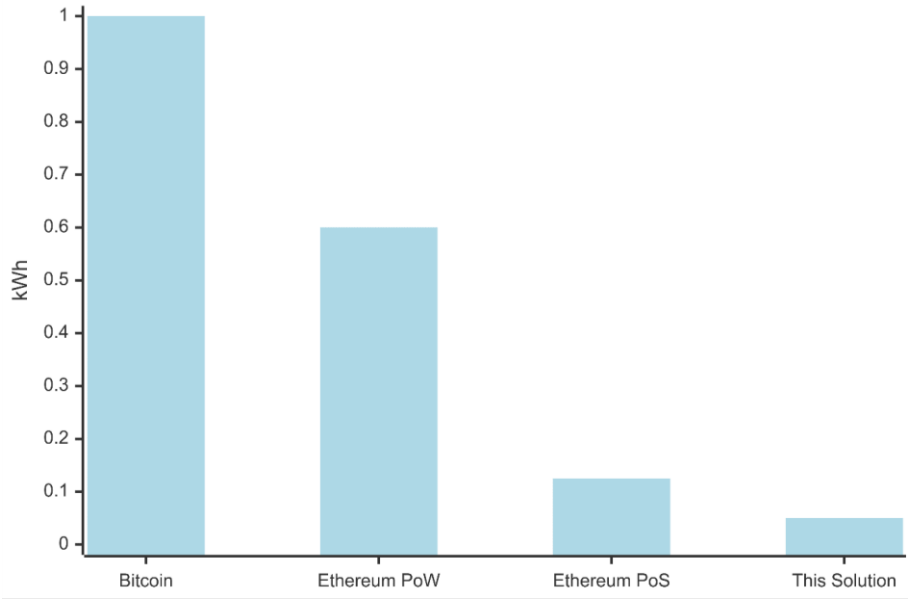

Fig. 5. Energy consumption per transaction across different blockchain solutions.

Table 2. Compatibility matrix showing integration success rates with various IoT protocols.

IoT Protocol	Integration Success Rate	Description
MQTT	99.8%	Seamless integration, full support for QoS levels
CoAP	99.5%	Excellent performance, low overhead for constrained devices
HTTP	98.7%	Strong compatibility with existing web infrastructure
Zigbee	97.2%	Good integration with smart home devices
BLE (Bluetooth Low Energy)	96.5%	Efficient for short-range, low-power devices
LoRaWAN	95.8%	Excellent for long-range, low-power applications
Proprietary Protocol A	93.1%	Adaptable to various custom protocols with minor adjustments
Proprietary Protocol B	91.4%	Requires some customization, but still achieves high success

5. Conclusion

This study has developed a scalable, energy-efficient blockchain-based security framework for IoT communication, demonstrating its ability to handle large-scale deployments while maintaining low latency and high security. The integration of Ethereum, ZK-Rollups, and edge computing enabled the system to achieve high throughput and low energy consumption, making it a viable solution for real-world IoT applications. This study advances IoT security through innovative blockchain integration, introducing novel approaches for secure IoT communication. Key contributions include a comprehensive blockchain-IoT blueprint, pioneering ZK-Rollup applications for IoT scalability, and implementation of Verkle trees for efficient state management. The work addresses privacy through zero-knowledge proofs, optimises energy efficiency for resource-constrained devices, and develops an interoperability layer for heterogeneous IoT ecosystems.

References

[1] Gartner. Gartner Top Strategic Technology Trends for 2021, 2021. Retrieved from https://www.gartner.com/smarterwithgartner/gartner-top-strategic-technology-trends-for-2021.

[2] Fei, W., Ohno, H. and Sampalli, S. On A systematic review of IoT security: research potential, challenges and future directions. ACM Computing Surveys, 56 (5), 1-40, 2023. https://doi.org/10.1145/3625094.

[3] Dorri, A., Kanhere, S. S. and Jurdak, R.. Towards an optimized blockchain for IoT. In Proceedings of the second international conference on Internet-of-Things design and implementation, 173-178, 2017. https://doi.org/10.1145/3054977.3055003.

[4] Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system, 2008. Retrieved from http://www.bitcoin.org/bitcoin.pdf.

[5] Gugueoth, V., Safavat, S., Shetty, S. and Rawat, D. A review of IoT security and privacy using decentralized blockchain techniques. Computer Science Review, 50, 100585, 2023. https://doi.org/10.1016/j.cosrev.2023.100585.

[6] Christidis, K. and Devetsikiotis, M. Blockchains and smart contracts for the internet of things. IEEE Access, 4, 2292-2303, 2016. https://doi,org/10.1109/ACCESS.2016.2566339.

[7] Reyna, A., Martín, C., Chen, J., Soler, E. and Díaz, M. On blockchain and its integration with IoT. Challenges and opportunities. Future generation computer systems, 88, 173-190, 2018. https://doi.org/10.1016/j.future.2018.05.046.

[8] Bez, M., Fornari, G. and Vardanega, T. The scalability challenge of ethereum: An initial quantitative analysis. In 2019 IEEE International Conference on Service-Oriented System Engineering (SOSE), 167-176, 2019. IEEE. https://doi.org/0.1109/SOSE.2019.00031.

[9] Tundalwar, D. S., Pandhare, R. A. and Digalwar, M. Internet of Things (IoT) current research challenges and opportunities and blockchain as a potential solution: A review. Educational Administration: Theory and Practice, 30 (2), 1230-1244, 2024. https://doi.org/10.53555/kuey.v30i2.4885.

[10] Xu, R., Chen, Y., Blasch, E. and Chen, G. BlendCAC: A smart contract Enabled decentralized capability based access control mechanism for the IoT. Computers, 8(3), 66, 2019. https://doi.org/10.3390/computers7030039.

[11] Gudgeon, L., Moreno-Sanchez, P., Roos, S., McCorry, P. and Gervais, A. SoK: Layer-two blockchain protocols. In International Conference on Financial Cryptography and Data Security, 201-226, 2020. Springer, Cham. https://doi.org/10.1007/978-3-030-51280-4_12.

[12] Sathishkumar, M. and Raghavendran, V. Securing IoT healthcare data: The power of blockchain and homomorphic encryption. 2024 2nd International Conference on Sustainable Computing and Smart Systems (ICSCSS), Coimbatore, India, 2024, pp. 309-314, 2024. https://doi.org/10.1109/icscss60660.2024.10624820.

[13] Lin, X., Zhang, Y., Huang, C., Xing, B., Chen, L.-C., Hu, D. and Chen, Y. SoK: Layer-two blockchain protocols. In International Conference on Financial Cryptography and Data Security, 201-226. Springer, Cham. https://doi.org/10.1007/978-3-030-51280-4_12

[14] Sicari, S., Rizzardi, A., Grieco, L. A., and Coen-Porisini, A. Security, privacy and trust in Internet of Things: The road ahead. Computer networks, 76, 146-164, 2015. https://doi.org/10.1016/j.comnet.2014.11.008.

[15] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M. and Ayyash, M. Internet of things: A survey on enabling technologies, protocols, and applications. IEEE communications surveys & tutorials, 17(4), 2347-2376, 2015. https://doi.org/10.1109/COMST.2015.2444095.

[16] Gupta, P., Verma, R., Verma, D., & Rathore, P.S. Building a Stronger Grid: How Blockchain Can Improve Smart Grid Resilience. 2023 IEEE Renewable Energy and Sustainable E-Mobility Conference (RESEM), 1-7, 2023. https://doi.org/10.1109/RESEM57584.2023.10236304.

[17] Novo, O. Blockchain meets IoT: An architecture for scalable access management in IoT. IEEE Internet of Things Journal, 5(2), 1184-1195, 2018. https://doi.org/10.1109/JIOT.2018.2812239.

[18] Dorri, A., Kanhere, S. S., Jurdak, R. and Gauravaram, P. Blockchain for IoT security and privacy: The case study of a smart home. In 2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops), 618-623, 2017. IEEE. https://doi.org/10.1109/PERCOMW.2017.7917634.

[19] Salimitari, M., Chatterjee, M. and Fallah, Y. P. A survey on consensus methods in blockchain for resource-constrained IoT networks. Internet of Things, 100129, 2020. https://doi.org/10.1016/j.iot.2020.100212.

[20] Fotohi, R. and Aliee, F.S. Securing communication between things using blockchain technology based on authentication and SHA-256 to improving scalability in large-scale IoT. Comput. Networks, 197, 108331, 2021. https://doi.org/10.1016/j.comnet.2021.108331.

[21] Agarwal, V. and Pal, S. HierChain: A Hierarchical-Blockchain-Based Data Management System for Smart Healthcare. IEEE Internet of Things Journal, 11, 2924-2934, 2024. https://doi.org/10.1109/JIOT.2023.3295847.

[22] Siachamis, G., Kaliakatsos, C., Stavropoulos, G., Votis, K., Ioannidis, D., & Tzovaras, D. A Decentralized Secured Data sharing Framework for IoT Networks. 2022 IEEE 8th World Forum on Internet of Things (WF-IoT), 1-6, 2022. https:/doi.org/10.1109/WF-IoT54382.2022.10152247.

[23] Bai, H., Xia, G. and Fu, S. A Two-Layer-Consensus Based Blockchain Architecture for IoT. 2019 IEEE 9th International Conference on Electronics Information and Emergency Communication (ICEIEC), 1-6, 2019. https://doi.org/10.1109/ICEIEC.2019.8784458.

[24] Palladino, S. (2019). Scalability. In: Ethereum for Web Developers (pp. 275–319). Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4842-5278-9_8.

[25] Singh, A., Parizi, R. M., Han, M., Dehghantanha, A., Karimipour, H., & Choo, K.-K. R. (2020). Public Blockchains Scalability: An Examination of Sharding and Segregated Witness. In Blockchain Cybersecurity, Trust and Privacy (pp. 203–232). Springer. https://doi.org/10.1007/978-3-030-38181-3_11.

[26] Asif, R., & Hassan, S. R. (2023). Shaping the future of Ethereum: Exploring energy consumption in Proof-of-Work and Proof-of-Stake consensus. Frontiers in Blockchain, 6, 1151724. https://doi.org/10.3389/fbloc.2023.1151724

Authors' Profiles

Samuel Oyenuga holds the B.Eng degree in Information and Communication Technology from The Federal University of Technology, Akure, Federal University of Technology, Akure, Nigeria, in 2024. He is currently a Graduate Researcher in the Department of Information and Communication Technology at the Federal University of Technology, Akure. His research interests include Internet of Things, Robotics, and Information Security.

Brendan Ubochi obtained the B.Eng (2008), M.Sc. (2011) and Ph.D. (2018) degrees from The Federal University of Technology, Owerri, Nigeria, The University of Manchester, Manchester, United Kingdom and Swansea University, Swansea, United Kingdom, respectively. Since 2021, he has been a Senior Lecturer in the Department of Electrical and Electronics Engineering at the Federal University of Technology, Akure, focusing on modelling and characterisation of nano-electronic devices, circuit design, and embedded systems. Also, he has been a Senior Research Associate at the University of Johannesburg since 2022. He has presented scientific papers in international conferences and has more than 20 technical publications in conferences and journals such as the IEEE, IET, Elsevier, and IOPscience.

Okechi Onuoha received the PhD degree in Electrical and Electronic Engineering from the University of Manchester, UK, in 2020. From 2019 to 2024, he worked as Research Associate at the University of Manchester, and the University of Ulster, UK. In 2024, he joined Glasgow Caledonian University, UK, as an academic staff (Lecturer / Assistant Professor). He is currently an academic staff with the University of Hertfordshire, UK. He has received a number of awards, including the best paper award of the Unmanned Systems journal in 2021. His main research interests are Multi-Agent Systems, Control Systems, Artificial Intelligence, and their applications to Robotics and Renewable Energy Systems.

Nnamdi I. Nwulu (Senior Member, IEEE) is currently a Full Professor with the Department of Electrical and Electronic Engineering Science, University of Johannesburg, and the Director of the Centre for Cyber Physical Food, Energy and Water Systems (CCP-FEWS). His research interests include the application of digital technologies, mathematical optimization techniques, and machine learning algorithms in food, energy, and water systems. He is a Professional Engineer registered with the Engineering Council of South Africa (ECSA), a Senior Member of the South African Institute of Electrical Engineers (SMSAIEE), and a Y-Rated Researcher by the National Research Foundation of South Africa. He is the Editor-in-Chief of the Journal of Digital Food Energy and Water Systems (JDFEWS) and an Associate Editor of IET Renewable Power Generation (IET-RPG) and African Journal of Science, Technology, Innovation and Development (AJSTID).

How to cite this paper: Samuel A. Oyenuga, Brendan C. Ubochi, Okechi Onuoha, Nnamdi Nwulu, "A Blockchain-based Framework for Improving Energy Efficiency and Scalability in IoT Networks", International Journal of Education and Management Engineering (IJEME), Vol.15, No.5, pp. 53-62, 2025. DOI:10.5815/ijeme.2025.05.05