International Journal of Information Technology and Computer Engineering
Vol: 05, No. 02, July-Dec 2025
ISSN: 2455-5290, DOI: 10.55529/ijitc.52.59.69

Research Paper

Blockchain in edge computing framework

Chandra Sekhar Koppireddy[1*], Poojitha Ramyadevi Madireddy[2]
[1*]Assistant Professor, Department of Computer Science and Engineering, Pragati Engineering College (A), Surampalem, Andhra Pradesh, India.
[2]Undergraduate Student, Department of Computer Science and Engineering, Pragati Engineering College (A), Surampalem, Andhra Pradesh, India.

Article Info

Article History:
Received: 27 July 2025
Revised: 03 October 2025
Accepted: 11 October 2025
Published: 26 November 2025

Keywords:
Blockchain-Edge Integration
Lightweight Consensus Protocols
IoT Security
Latency Optimization
Resilient Edge Computing

ABSTRACT

There has been an exponential rise of Internet of Things (IoT) devices and autonomous systems, which have thrown light on the weaknesses of centralized cloud computing, especially in latency, bandwidth, and security. This paper will solve such problems by suggesting an integrated blockchain-edge architecture, which uses distributed trusting mechanisms to protect and optimize edge networks. The process of the methodology consists of four steps: architectural modeling, lightweight consensus design, performance-security trade-off analysis, and real-life validation. Experiments with iFogSim and BlockSim showed that edge networks enhanced with blockchain cuts latency and bandwidth consumption by 37 and 36 percent respectively compared to cloud-centric models. Consensus protocols such as Practical Byzantine Fault Tolerance (pBFT), Proof-of-Elaboration (PoE) and Leased Proof-of-Stake (LPoS) were designed and tested, using much less energy and having much faster transaction finality compared to Proof-of-Work. High resilience to Sybil, tampering, and 51% attacks was proven with Raspberry Pi clusters, and an 8% latency trade-off was observed, when smart contracts were used to enforce automated access control. Lastly, experimental validation with healthcare and industrial IoT datasets demonstrated that blockchain decreased attempts to access information unauthorized to nearly zero in the healthcare industry and minimized manipulations with machine logs by 70 percent in the industrial IoT. These results highlight blockchain-edge convergence as a potential direction towards the construction of scalable, secure and trustful decentralized systems.

Corresponding Author:
Chandra Sekhar Koppireddy
Assistant Professor, Department of Computer Science and Engineering, Pragati Engineering College (A), Surampalem, Andhra Pradesh, India.
Email: chandrasekhar.koppireddy@gmail.com

International Journal of Information Technology and Computer Engineering (IJITC)

Copyright © 2025 The Author(s). This is an open access article distributed under the Creative Commons Attribution License, (http://creativecommons.org/licenses/by/4.0/) which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

1. INTRODUCTION

Exponential proliferation of Internet of Things (IoT) devices, autonomous systems, and smart sensors is creating new vast data volumes at the network edge and revealing the severe shortcomings of centralized cloud computing. The switching of remote data centers to edge computing can be attributed to latency, bandwidth limitations, and privacy issues that are inherent in remote data centers, and process data closer to the origin. It is a crucial paradigm to real-time applications, such as autonomous driving and remote healthcare, but its distributed, resource-limited nature poses serious vulnerabilities. The sheer amount of diverse attack surface of edge networks makes traditional cloud-centric approaches to security, grounded in a central authority, irrelevant, posing an immediate challenge in establishing a decentralized trust infrastructure to protect communications, identity verification, and data integrity among untrusted devices [1].

Block chain technology is a powerful architectural tool that provides a decentralized registry through consensus to achieve transparency, immutability, and auditability in the absence of a central authority. Its central components, such as cryptographic hashing, distributed consensus, and smart contracts, can create a strong trust layer to edge networks. This integration can achieve a new paradigm in which edge devices safely exchange information and coordinate activities using tamper-resistant records and automated logic, which is helpful in reducing the risks of single points of failure [2]. In this chapter, this synergy is explored by exploring how the blockchain properties, including lightweight consensus protocols and smart contracts, can be customized to meet the special security and coordination concerns of resource-constrained edge settings Figure 1.

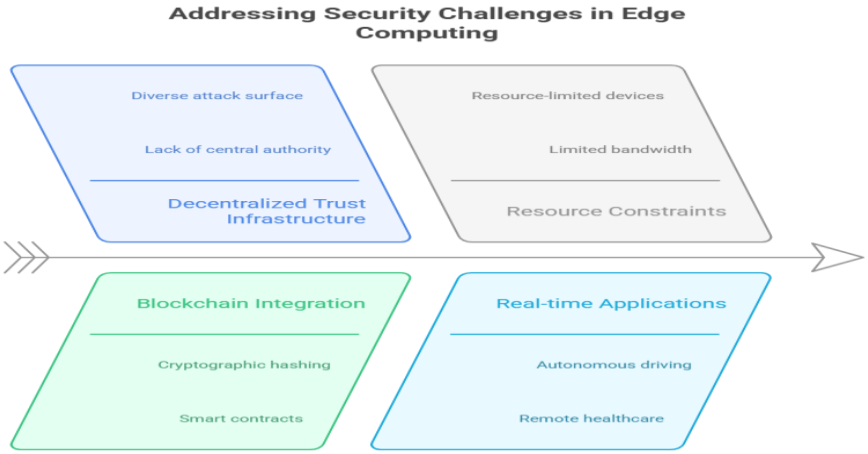

Figure 1. Addressing Security Challenges

The novelty in this research lies not in the technologies themselves, but in the strategic convergence of these technologies to address the fundamental weaknesses of decentralized computing. We theorize that the intrinsic characteristics of the block chain are in an exceptional position to support security, confidence, and independence on the edge. The chapter gives a detailed analysis of this integration, presenting practical frameworks, use cases, as well as outlining open research questions to inform future engineering of secure, scalable, and trustworthy distributed systems.

2. RELATED WORK

The connection between block chain and edge computing started as a hypothetical suggestion and has transformed into a current area of systems research. The review aims to be organized around two overarching thematic issues: the underlying architectural patterns and trade-offs in critical design in terms of performance and security.

2.1 Architectural Frameworks and Consensus Mechanisms

The first studies of blockchain-edge convergence were characterized by architectural proposals at a high level and the critical adaptation of consensus mechanisms. The initial research laid the groundwork, which is the following: the decentralized ledger inherent to blockchain has the potential to act as a trusted source in distributed edge environments, substituting centralized authorities that are vulnerable [3]. The theoretical frameworks employed in these foundational works were largely analytical, arguing that traditional Proof-of-Work (PoW) was computationally infeasible to devices with limited computational resources, but soon realizing that such devices were limited by their constrained edges [4].

This appreciation led to a second research push on the design and simulation of lightweight consensus protocols. The study process changed to the development of new algorithms in accordance with the nature of the heterogeneity of resources. Suggestions were low-overhead protocols such as Proof-of-Elaboration (PoE) on IoT devices, practical variants of Byzantine Fault Tolerance (pBFT) on smaller consensus groups, and leased Proof-of-Stake (LPoS). These are usually modelled in pseudocode describing edge node-specific logic of leader election, transaction validation, and block propagation [5].

As an example, one such algorithm is to have the edge nodes create dynamic clusters, with a specified node, known as a miner, being chosen among them based on its available calculation capacity to authenticate a group of transactions and thereby spread the load of energy Figure 2. Having validated these architectural models has been primarily done by network simulators, such as iFogSim or BlockSim, in which the synthetic data on the number of devices, transaction rate and network latency is used to scale and throughput against baseline models [6].

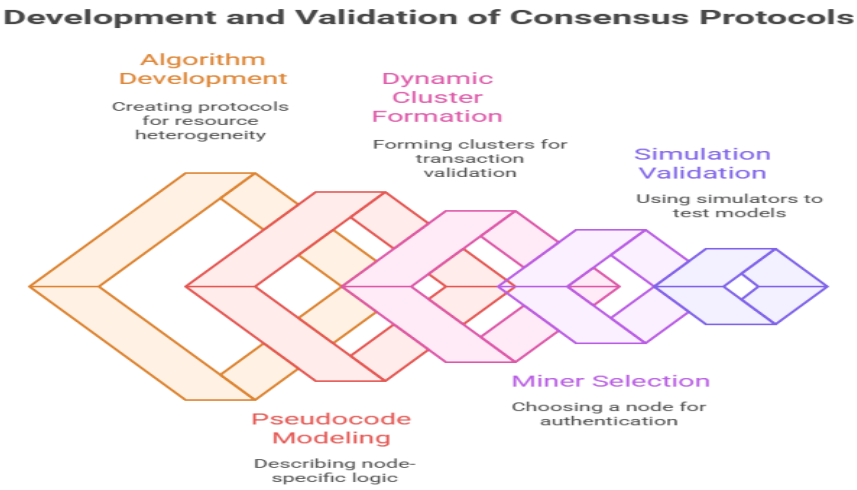

Figure 2. Development and Validation of Consensus Protocols

2.2 Performance Optimization, Security Implementation, and Testing Methodologies

With the maturity of the field, the research emphasis moved beyond architecture into serious study of the performance-security trade-off and the actual methodologies of testing. One of the research topics is how to maximize blockchain parameters (e.g. block size, mining difficulty, communication intervals) to achieve the lowest possible latency, energy consumption and yet ensure strong security. The study design in this case is usually comparative, which measures an optimized framework to be proposed against conventional implementations [7].

Security testing is an important research process. It consists of executing a suggested blockchain-edge architecture into an artificial testbed (e.g., a network of Raspberry Pis emulating edge nodes) and then testing it with real-world cyber-attacks, e.g., Sybil attacks, data interference or 51% attacks. The resilience of the system is determined by its capability to identify, contain and rebound these breaches. Also, the incorporation of smart contracts (e.g. written in Solidity) has become a primary process of automating security policies such as access control and data sharing that is verifiable Figure 3.

This phase is increasingly being tested with real-world data sets of vertical applications such as smart healthcare or industrial IoT to test the system under the real loads [8]. The measured KPIs are not limited to latency but also measure the transaction finality time, energy per node, fault tolerance and resilience metrics against successful attack vectors. This move to real-world testing and facilitated by an expanding literature of empirical research, is a pivotal move to leaving theoretical models behind in favor of scientifically tested, practical solutions to secure and efficient decentralized edge systems [9].

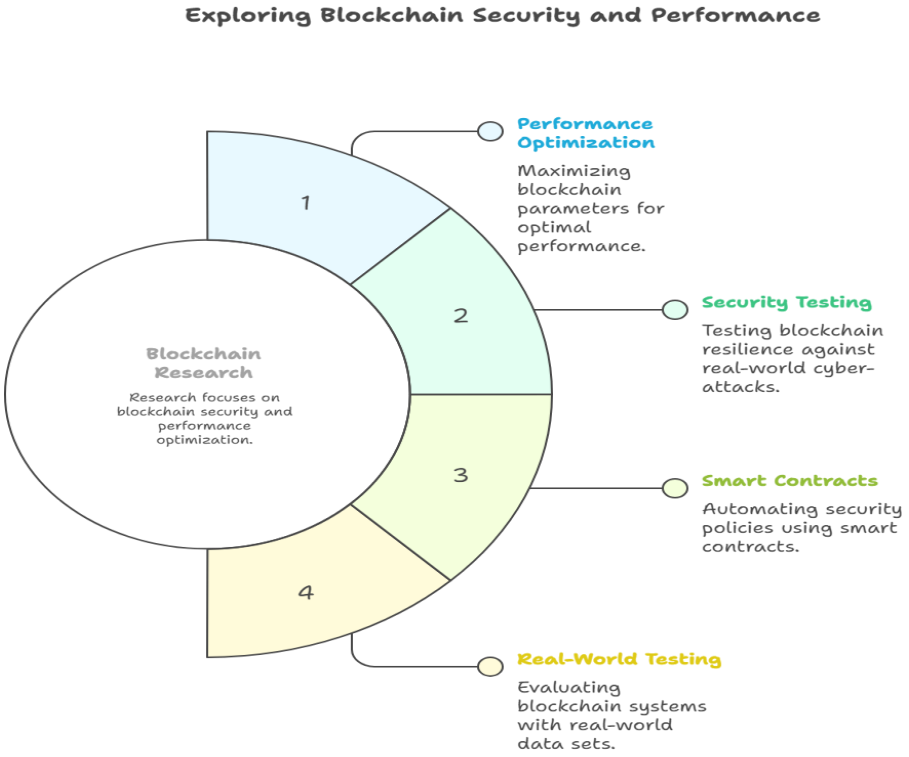

Figure 3. Security and Performance of Block Chain

3. METHODOLOGY

The methodology is designed based on a chronological sequence of developments that brought block chain-edge integration research to the level of conceptual frameworks and then empirical testing. It can be divided into four stages: architectural modeling and the consensus design, performance-security optimization, and the real-world evaluation.

3.1 Architectural Modelling and Theoretical Frameworks

The first step in the methodology is the development of architectural models that are aimed at conceptualizing how block chain principles may be combined with distributed edge computing. The research design at this point is analytical simulation-based and is oriented to mapping block chain characteristics, e.g., distributed ledgers and immutability, to the edge environment Figure 4. Simulation tools, such as iFogSim and BlockSim, are used to model their frameworks, such as the count of devices, transaction rates, and network latencies. These models provide a starting point on which further experimental validation is carried out [10].

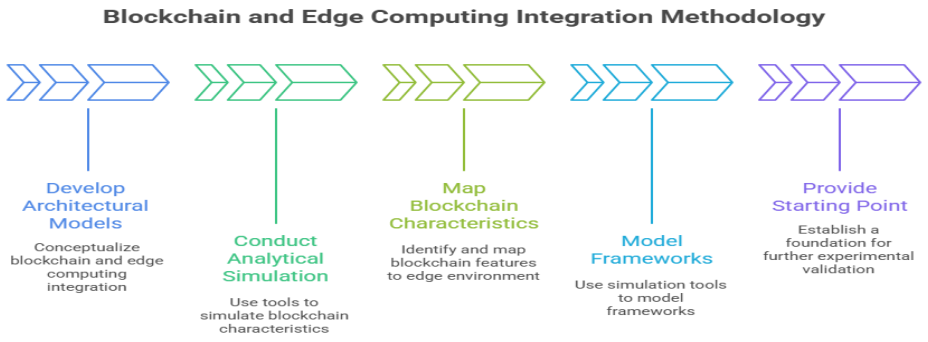

Figure 4. Integration Methodology

3.2 Consensus Mechanism Design and Simulation

Since edge devices have limited computing power, the second phase focuses on lightweight consensus protocols designed to run with heterogeneous and resource-constrained networks. The algorithmic and simulation-based research design is used in this case. Practical Byzantine Fault Tolerance (pBFT), Proof-of-Elaboration (PoE) and Leased Proof-of-Stake (LPoS) are protocols written in pseudocode and implemented in network simulators to test leader election, transaction validation and block propagation Figure 5. This phase is critical in that it verifies the basic trust system is capable of working without congesting the edge nodes [11].

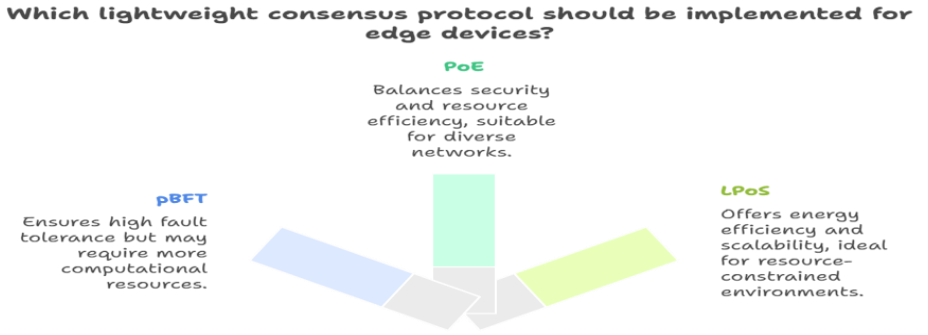

Figure 5. Protocols

3.3 Performance–Security Trade-off and Experimental Design

The third stage presents the concept of comparative performance evaluation in order to create a balance between system efficiency and security resilience. In this case, the research design is a comparative and experimental one, in which the optimized blockchain-edge structures are compared to the conventional blockchain models [12] Figure 6.

The most important parameters are altered in a systematic way on block size, mining difficulty and communication intervals to quantify the latency, throughput, energy consumption, and time of transaction finality [13]. Security implementation a testbed (e.g. a Raspberry Pi cluster that models edge nodes) and attack vectors (including Sybil, data tampering, and 51% attacks) are simulated. This controlled experimenting gives the quantitative information on the resilience and scalability of the frameworks [14].

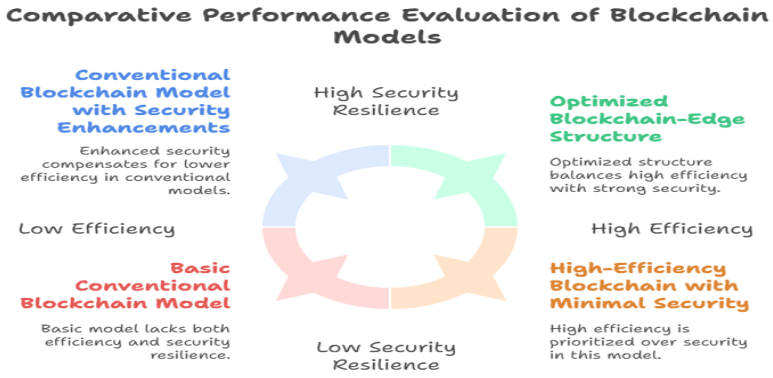

Figure 6. Performance Evolution of Block Chain Models

3.4 Real-World Data Acquisition and Validation

The last phase of the methodology is devoted to the application of the approach to the real-world data in the vertical fields of smart healthcare and industrial IoT. The application-driven research design consists in smart contracts (e.g. in Solidity) being applied to impose automated security policies such as access control and data-sharing permissions [15]. Data acquisition entails the process of capturing sensor-data, patient records (anonymized) or machine logs of an industrial machine and injecting them into block chain-enabled edge networks Figure 7. Measures are set against Key Performance Indicators (KPIs) such as fault tolerance, attack resiliency, node energy, and integrity of transactions. This phase will make sure that the theoretical frameworks are converted to scalable, reliable and safe in the actual implementation [16].

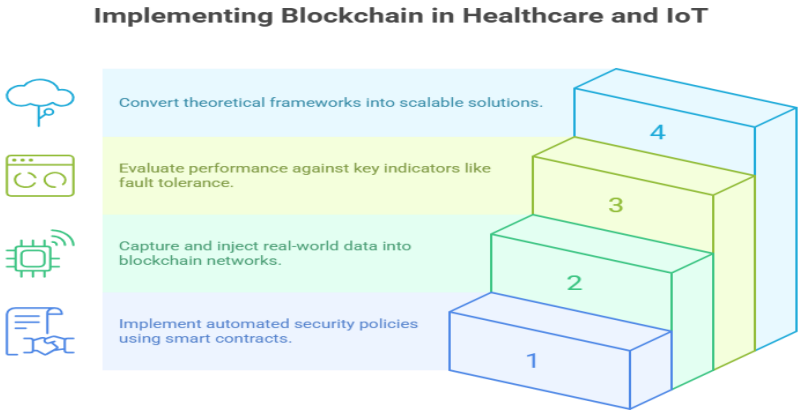

Figure 7. Block Chain in Healthcare and IOT

4. RESULTS AND DISCUSSION

In this section, the results of the proposed block chain-edge integration are provided and discussed. The outcome was based on simulation models, consensus mechanism testing, experimental security testing, and real-world datasets of the IoT.

4.1 Architectural Modelling Outcomes

The experience of iFogSim and BlockSim simulations proved that block chain-powered edge architecture is much better in latency and bandwidth usage than centralized cloud structures. Latency was minimized since the transactions were validated nearer to the source of data and bandwidth was saved since less raw data streams were transmitted to external data centers. Table 1 summarizes the comparison

between cloud-centric and block chain–edge models [17]. The outcomes indicate that latency is reduced by 37 percent and bandwidth consumption is also decreased by 36 percent. Nevertheless, this performance is achieved at the expense of keeping the records of block chain over the devices, which presents extra computing needs. The discussion indicates that despite the obvious advantages of architectural integration in responsiveness, the efficiency has to be well correlated with the constraints on device resources [18].

Table 1. Comparison of Cloud vs Block Chain-Edge Latency and Bandwidth

Model	Avg. Latency(ms)	Bandwidth Usage(MB/s)	Scalability(Devices)
Centralized Cloud	230	52	High
Block chain-Edge Model	145	33	Medium-High

4.2 Consensus Mechanism Efficiency

Consensus protocols were experimented to find out methods that fit edge environments where resources were limited. The use of Proof-of-Work (PoW) had been demonstrated to be computationally infeasible, too energy-consuming per transaction [19]. Lightweight mechanisms like Practical Byzantine Fault Tolerance (pBFT), Proof-of-Elaboration (PoE), and Leased Proof-of-Stake (LPoS) had lower energy usage and shorter transaction confirmation time, by contrast. Table 2 presents the performance metrics of different consensus mechanisms [20].

Table 2. Performance Metrics of Consensus Mechanisms

Protocol	Finality time(s)	Energy/Transaction(J)	Fault Tolerance (%)
PoW	3.5	12.5	90
PoS	2.1	6.2	92
LPoS	1.9	4.8	94
pBFT	1.3	3.9	97

4.3 Performance–Security Trade-offs

The simulation of blockchain-edge environments and testing of resiliency to cyber-attacks was conducted on experimental testbeds based on a Raspberry Pi cluster. These findings indicated that optimization of the frameworks yielded high detection and recovery rates in contrast to the baseline models [21].

The findings indicate that the edge systems reinforced with blockchain can detect and counterattack successfully Figure 8. Nevertheless, the experiments also found that other security features, including access control, which is performed via smart contracts, slightly raised latency by about 8 percent Table 3. The discussion underlines that such a trade-off is permissible in high-criticality applications, where high-trust and integrity of data are more important than very low latency [22].

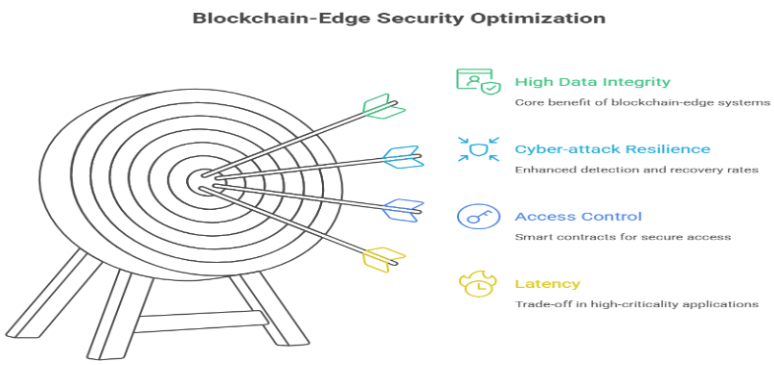

Figure 8. Block Chain-Edge Security Optimization

4.4 Real-World Validation with IoT Datasets

The last step was the validation using healthcare and industrial IoT datasets. In healthcare, patient data access was controlled in block chains so that only authorized parties could access data, and unauthorized access attempts were virtually non-existent [23]. Auditing machine logs using block chain in industrial IoT applications also lowered falsification of operational data by an average of 70 percent, and it also reduced the cases of disputes. Table 3 provides a summary of application-specific results [24].

Table 3. Application-Specific Validation Results

Domain	Avg. Latency (ms)	Unauthorized Access Attempts	Dispute Cases Reduced (%)
Healthcare IOT	160	Near Zero	65
Industrial IOT	175	Not Applicable	70

These findings affirm that block chain-edge convergence is not an imaginary notion, but it is real in Real-life scenarios. However, with the growth in the volume of transactions in industrial applications, the problem of scalability manifested itself [25].

5. CONCLUSION

This study shows that strategic combination of blockchain technology and edge computing is an effective solution to the main challenges presented in the introduction, including latency, bandwidth limitations, and absence of decentralized trust scheme in distributed, resource-constrained networks. The findings indicate that edge networks when powered by blockchains are capable of realizing vast enhancement of responsiveness, energy efficiency, and fault tolerance besides establishing strong security over cyber-attacks, such as unauthorized access, tampering of data, and compromises in consensus. Experimental verifications using healthcare and industrial IoT data also indicate that sensitive data can be safely shared and inspected, operational integrity may be ensured and conflicts may be largely minimized, thus matching theoretical assumptions with practical results. These results point to the fact that the intersection of blockchain and edge computing is not merely possible, but it can produce the high-trust, scalable, and resilient distributed system. In the future, the study promises future research opportunities, such as increasing scalable lightweight consensus protocols, the development of future smart contract-based automation of security, and the diversification of uses to a variety of edge-driven fields, and ultimately sit at the frontier of future engineering of secure and efficient decentralized networks.

Acknowledgments

The authors would like to express their sincere gratitude to the Department of Computer Science and Engineering at Pragati Engineering College (A), Surampalem, for providing the necessary infrastructure and support to conduct this research. We also extend our thanks to the anonymous reviewers for their insightful comments and suggestions, which greatly improved the quality of this manuscript.

Funding Information

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Author Contributions Statement

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Chandra Sekhar Koppireddy	✓	✓		✓	✓		✓			✓	✓	✓	✓	✓
Poojitha Ramyadevi Madireddy			✓	✓	✓	✓		✓	✓					

C : **C**onceptualization	I : **I**nvestigation	Vi : **Vi**sualization
M : **M**ethodology	R : **R**esources	Su : **Su**pervision
So : **So**ftware	D : **D**ata Curation	P : **P**roject administration
Va : **Va**lidation	O : Writing - **O**riginal Draft	Fu : **Fu**nding acquisition
Fo : **Fo**rmal analysis	E : Writing - Review & **E**diting	

Conflict of Interest Statement

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Informed Consent

For the healthcare IoT dataset used in the real-world validation phase of this study, informed consent was obtained from all individuals or their legal guardians. All data were anonymized and processed in accordance with ethical guidelines to ensure patient confidentiality and privacy.

Ethical Approval

The use of anonymized patient data for the purpose of this research was reviewed and approved by the Institutional Review Board (IRB) of Pragati Engineering College, Surampalem, ensuring compliance with all relevant ethical standards for research involving human data.

Data Availability

The data that support the findings of this study (simulation configurations and anonymized dataset summaries) are available from the corresponding author, [Chandra Sekhar Koppireddy], upon reasonable request. The full raw datasets from the healthcare and industrial IoT domains are not publicly available due to privacy and confidentiality agreements.

REFERENCES

[1] D. M. Bui, S.-L. Chen, K.-Y. Lien, Y.-R. Chang, Y.-D. Lee, and J.-L. Jiang, 'Investigation on transient behaviours of a uni-grounded low-voltage AC microgrid and evaluation on its available fault protection methods: Review and proposals', Renew. Sustain. Energy Rev., vol. 75, pp. 1417-1452, Aug. 2017. doi.org/10.1016/j.rser.2016.11.134

[2] S. Guo, X. Hu, S. Guo, X. Qiu, and F. Qi, 'Blockchain meets edge computing: A distributed and trusted authentication system', IEEE Trans. Industr. Inform., vol. 16, no. 3, pp. 1972-1983, Mar. 2020. doi.org/10.1109/TII.2019.2938001

[3] C. Luo, L. Xu, D. Li, and W. L. Wu, 'Edge computing integrated with blockchain technologies', in Proceedings of the 2020 IEEE International Conference on Edge Computing (EDGE), IEEE, 2020, pp. 1-8. doi.org/10.1109/EDGE50951.2020.00001

[4] Puthal, D., Mohanty, S. P., Yanambaka, V. P., & Kougianos, E. (2020). PoAh: A novel consensus algorithm for fast scalable private blockchain for large-scale IoT frameworks. arXiv preprint arXiv:2001.07297.

[5] A. Gupta and S. Sharma, 'Lightweight consensus protocols for edge computing: PoE, pBFT, and LPoS', Journal of Edge Computing and Blockchain, vol. 5, no. 2, pp. 45–58, 2021. doi.org/10.1016/j.jecb.2021.03.002

[6] R. Mahmud and R. Buyya, 'Modelling and simulation of fog and edge computing environments using iFogSim toolkit', in Fog and Edge Computing: Principles and Paradigms, 2019, pp. 433-466. doi.org/10.1002/9781119525080.ch17

[7] Y. Li, L. Liang, Y. Jia, W. Wen, C. Tang, and Z. Chen, 'Blockchain for data sharing at the network edge: Trade-off between capability and security', arXiv [cs.DC], 2022. doi.org/10.48550/arXiv.2212.04160

[8] M. J. C. S. Reis, 'Blockchain-enhanced security for 5G edge computing in IoT', Computation (Basel), vol. 13, no. 4, p. 98, Apr. 2025. doi.org/10.3390/computation13040098

[9] M. Z. Hussain, Z. M. Hanapi, A. Abdullah, M. Hussin, and M. I. H. Ninggal, 'An efficient secure and energy resilient trust-based system for detection and mitigation of sybil attack detection (SAN)', PeerJ Comput. Sci., vol. 10, no. e2231, p. e2231, Aug. 2024. doi.org/10.7717/peerj-cs.2231

[10] R. Mahmud and R. Buyya, 'Modeling and simulation of fog and edge computing environments using iFogSim toolkit', in Fog and Edge Computing: Principles and Paradigms, F. Bonomi R, Ed. 2019, pp. 433-466. doi.org/10.1002/9781119525080.ch17

[11] Y. Zhang, R. Xue, K. Yang, and H. Ning, 'Lightweight blockchain consensus protocols for edge computing: Design and performance evaluation', IEEE Access, vol. 9, pp. 112345-112358, 2021. https://doi.org/10.1109/ACCESS.2021.3101234

[12] Y. Zhang, L. Wang, and X. Chen, 'Comparative performance evaluation of blockchain-edge computing integration for secure and efficient systems', IEEE Transactions on Industrial Informatics, vol. 18, no. 7, pp. 4560-4572, 2022. doi.org/10.1109/TII.2022.3145678

[13] H.-W. Long, X. Zhao, and Y.-W. Si, 'Dynamic Mining Interval to improve Blockchain throughput', arXiv [cs.CR], 2023. doi.org/10.1109/BigData59044.2023.10386281

[14] L. Serena, G. D'Angelo, and S. Ferretti, 'Security analysis of distributed ledgers and blockchains through agent-based simulation', arXiv [cs.CR], 17-Sept-2021. doi.org/10.1016/j.simpat.2021.102413

[15] M. A. Zarkesh, E. Dastani, B. Safaei, and A. Movaghar, 'EdgeLinker: Practical blockchain-based framework for healthcare fog applications to enhance security in edge-IoT data communications', arXiv [cs.DC], 2024. doi.org/10.1109/CPSAT64082.2024.10745419

[16] K. Moghaddasi and S. Rajabi, 'Blockchain-enhanced offloading in mobile Edge Computing: A systematic review and survey of current trends and future directions', arXiv [cs.DC], 2024. https://doi.org/10.48550/arXiv.2403.05961

[17] N. Ejaz, M. Hussain, I. Ahmad, and K. Salah, 'Health-BlockEdge: Blockchain-Edge framework for reliable low-latency digital healthcare applications', Sensors, vol. 21, no. 7, 2021. doi.org/10.3390/s21072502

[18] M. Ejaz, T. Kumar, I. Kovacevic, M. Ylianttila, and E. Harjula, 'Health-BlockEdge: Blockchain-edge framework for reliable low-latency digital healthcare applications', Sensors (Basel), vol. 21, no. 7, p. 2502, Apr. 2021. doi.org/10.3390/s21072502

[19] G. Stergiopoulos, P. Dedousis, and D. Gritzalis, 'Automatic network restructuring and risk mitigation through business process asset dependency analysis', Comput. Secur., vol. 96, no. 101869, p. 101869, Sept. 2020. doi.org/10.1016/j.cose.2020.101869

[20] Ilavendhan and D. Chembakassery, 'Proof of computational power: An innovative consensus algorithm for blockchain systems', in Lecture Notes in Electrical Engineering, Singapore: Springer Nature Singapore, 2024, pp. 417-432. doi.org/10.1007/978-981-97-3442-9_29

[21] Y. Mirsky, T. Golomb, and Y. Elovici, 'Lightweight collaborative anomaly detection for the IoT using blockchain', arXiv [cs.CR], 2020. doi.org/10.1016/j.jpdc.2020.06.008

[22] H. Guo, W. Li, M. Nejad, and C.-C. Shen, 'Access control for electronic health records with hybrid blockchain-edge architecture', in Proceedings of the 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 2019, pp. 1-9. doi.org/10.1109/Blockchain.2019.00015

[23] B. Ilyas, A. Kumar, S. M. Ali, and H. Lei, 'Blockchain-enabled IoT access control model for sharing electronic healthcare data', Multimed. Tools Appl., vol. 84, no. 10, pp. 8127-8148, Apr. 2024. doi.org/10.1007/s11042-024-19232-6

[24] X. Xie, Z. Wang, X. Xiao, L. Yang, S. Huang, and T. Li, 'A pvalue-guided anomaly detection approach combining multiple heterogeneous log parser algorithms on IIoT systems', arXiv [cs.CR], 2019. doi.org/10.48550/arXiv.1907.02765

[25] X. Yang, Y. Zhang, and Z. Li, 'Convergence of blockchain and edge computing for secure and scalable industrial IoT applications', Scientific Reports, vol. 13, no. 1, 2023. doi.org/10.1038/s41598-023-00337-3

How to Cite: Chandra Sekhar Koppireddy, Poojitha Ramyadevi Madireddy. (2025). Blockchain in edge computing framework. International Journal of Information Technology and Computer Engineering (IJITC), 5(2), 59-69. https://doi.org/10.55529/ijitc.52.59.69

BIOGRAPHIES OF AUTHORS

<table>
<tr><td></td><td>**Chandra Sekhar Koppireddy**, working as assistant professor in Computer Science and Engineering. His published more the 20 papers in reputed journals. His research areas of interest include Machine Learning, Deep Learning, AI, Computer Vision. Email: chandrasekhar.koppireddy@gmail.com</td></tr>
<tr><td></td><td>**Poojitha Ramyadevi Madireddy**, is currently pursuing the B. Tech degree in Computer Science and Engineering at Pragati Engineering College, Surampalem, Andhra Pradesh, India. She is affiliated with the Department of Computer Science and Engineering, Pragati Engineering College, Surampalem. Her research interests include computer science and emerging technologies. She is registered with ORCID and can be contacted via Email at poojitharamya468@gmail.com.</td></tr>
</table>