Electronics, Communications, and Computing Summit
Vol. 3, No. 4, Oct - Dec 2025, pp. 28-35
ISSN: 3107-8222, DOI: https://doi.org/10.17051/ECC/03.04.04

Secure and Low-Latency Communication in Edge Computing Environments Using Blockchain-Enabled IoT Architecture

Shaik Sadulla

Department of Electronics and Communication Engineering, KKR & KSR Institute of Technology and Sciences, Vinjanampadu, Guntur-522017, Andhra Pradesh, India, Email: sadulla09@gmail.com

Article Info

Article history:

Received : 14.10.2025
Revised : 13.11.2025
Accepted : 08.12.2025

Keywords:

Edge Computing;
Blockchain-Enabled IoT;
Low-Latency Communication;
PBFT Consensus;
Hybrid On-Chain/Off-Chain Model;
Secure Distributed Architecture

ABSTRACT

The concept of edge computing has become a key paradigm of facilitating real-time communication in Internet of Things (IoT) nexus by moving computation to end devices. Although decentralised edge infrastructures have latency benefits, they pose a serious security risk through identity spoofing, replay attacks, data modification, and distributed denial-of-service attacks. Blockchain technology provides decentralised trust and data immutability but standard blockchain systems are characterised by high confirmation latency and computation overhead making them unsuitable with delay-sensitive IoT applications. In this research paper, the authors suggest a hierarchical blockchain-based IoT model which is to be implemented to provide secure and low-latency communication in edge computing settings. The suggested system is a consortium blockchain implemented on an optimized Practical Byzantine Fault Tolerance (PBFT) consensus mechanism executed in localized edge clusters. A hybrid strategy of off-chain/on-chain data management and a scheme estimating the delay of micro-block generation are also presented to minimise the duration of communication. Formal latency model is created which is used to analyse the time of transaction confirmation, and the implementation of the architecture is done with multi-node edge testbed, created with Hyperledger Fabric. The experiments show 38 to 45 percent decrease in end-to end latency and enhancement of transaction throughput as compared to traditional blockchain-IoT systems and they resist Sybil, replay and tampering attacks. These results confirm that edge architectures supported by blockchain can meet the security and real time performance goals of the next generation IoT systems.

1. INTRODUCTION

The emergence of Internet of Things (IoT) devices has completely changed the contemporary communication infrastructures and has cleared the path to be deployed in large numbers in cities, to automate industries or medical devices and transport systems. According to the latest reports in the industry, tens of billions of IoT devices are actively producing streams of data with a high sensitivity to latency that must be processed in real-time and transmitted with a high level of security [1], [2]. The classical approach of cloud-based architecture is also scalability but adds excessive communication delay through the long transmission paths, network congestion, and the bottleneck processing. In addition, centralised models are susceptible to single point failures as well as mass data breaches [3]. Edge computing has become a promising paradigm to alleviate latency through moving compute and storage resources that are more proxim to end-equipment [4], [5]. The response time and the bandwidth usage is minimised by processing data at the network edge. Nevertheless, edge nodes represent a challenging security risk due to their decentralisation and distribution, where spy attacks, unauthorised access, data alterations,[6], [7] replay attacks, and distributed denial-of-service (DDoS) can be discussed as the fundamental security issues. In contrast to the centralised cloud settings, edge infrastructures do not have unified trust enforcement mechanisms, which complicates the ability to make a secure coordination among nodes. Blockchain technology has been extensively were proposed as a decentralised structure of trusts with the ability to guarantee the integrity and immutability of data and their auditable characteristics in an IoT system [8], [9]. The use of public blockchains has good security guarantees, but due to high confirmation lags, high energy usage, and low throughput [10]. All these restrictions render the traditional blockchain to be inappropriate in delay sensitive IoT applications that use the edge environment.

More recent studies have examined the case of private and consortium blockchain use with consensus mechanisms of Practical Byzantine Fault Tolerance (PBFT) and Proof-of-Authority (PoA) to minimise latency [11], [12]. In spite of the performance enhancement of these approaches, numerous current studies either emphasise on security and have not purposely assessed the latency or offer latency optimization but have not defined the security model. Moreover, very limited literature can give extensive experimental support comparing edge blockchain integration with cloud-centric network architecture on one side and blockchain-only architecture on the other side [13].

Thus, the research gap is essential because there is no critical study on how to design a blockchain-enabled IoT architecture with the capability of fulfilling the following simultaneously:

1. Small end-to-end communication latency,
2. Good decentralised security assurances, and
3. Deployability in edge computing deployability.

In order to overcome this problem, the following paper offers a hierarchical blockchain-based IoT architecture that is efficient in secure and low-latency communication in the edge. The architecture combines localised clusters of blockchains with local consortium with lightweight PBFT-based consensus mechanism and a hybrid off-chain data and on-chain data validation model. A formal threat model is created to analyse the resilience in security and a latency sensitive micro-block strategy is presented to minimise the transaction confirmation delay. The system being proposed is realised in a multi-node edge testbed and tested with respect to baseline architectures.

The principal contributions of this work can be outlined as the following ones:

Designs of hierarchical edge-blockchain IoT architecture has been proposed based on real-time communication.

- PBFT-based consensus mechanism that is large and lightweight and is deployed in edge clusters.
- An off chain on chain data validation strategy to minimise block congestion.
- A formal security threat model that has explicit mitigation mechanisms.
- A quantitative performance analysis between latency, throughput and resilience and traditional methods.

2. RELATED WORK

Edge computing and blockchain Integration of blockchain and edge computing systems have not only received considerable research focus on the Internet of Things (IoT) systems in recent years. Edge computing has become very popular so as to eliminate the communication latency as well as alleviating cloud network congestion by moving calculation nearer to their terminals [1], [2]. Some of the studies confirm that edge-based structures are able to greatly lower round-trip delay and enhance Quality of Service (QoS) in delay-sensitive IoT systems like smart healthcare and industrial control systems [3]. Nevertheless, as edge computing improves performance, it has drawbacks on trust management, due to the decentralised structure of edge computing, an attacker can exploit distributed edge nodes to hack into, modify and spoof identities [14]. In an effort to deal with security issues, blockchain technology is suggested as a decentralised trust system across the IoT environment [15], [16]. Blockchain allows storage of data that is tamper resistant, records transactions transparently, and in a decentralised manner without the use of centralised authorities. Public blockchain protocols and specifically Proof-of-Work (PoW) offer high immutable guarantees but with high confirmation times, poor throughput and high energy consumption [17]. These features render conventional blockchain systems unsuitable to latency-sensitive IoT systems at the edge. Recent studies have investigated constrained implementations of blockchains in the private or consortium to overcome these drawbacks. Practical Byzantine Fault Tolerance's (PBFT) and Proof-of-Authority (PoA) consensus mechanisms have been demonstrated to have lower transaction confirmation times and a higher throughput than PoW-based methods [18], [19]. The existing research on implementing PBFT in IoT networks has demonstrated reduced latency and a smaller network size, but scaling fails as the population size of the validator nodes grows because of communication overheads used in Byzantine agreements [10]. In addition, some of the works also suggest hybrid architectures of edge-blockchains, with edge-nodes functioning as blockchain gateways or validator [11]. Although these methods enhance better decentralisation and less cloud dependence, a lot of them are still without a detailed latency model or experimental benchmarking versus cloud-based and blockchain-only baselines. The lack of membership regarding security threat modelling and performance evaluation is the other weakness in the available literature. Even though other studies purport to achieve greater security with blockchain adoption, they frequently fail to define their threats, conduct attack simulations or validate their resilience to Sybil, replay, or distributed denial-of-service attacks in a quantitative manner [12], [13]. Also, very little work uses off-chain/on-chain data handling mechanisms to minimise the block congestion but still maintain auditability, which is a critical measure to maintain a state of real-time communication performance.

Accordingly, even though significant advances have been made in the fields of edge computing and blockchain-enabled IoT, there is still a gap in proposing an architecture that is capable of simultaneously (i) low-latency communication control, (ii) scalable deployment of consensus at the edge layer, and (iii) formally defined security resiliency that has proven its effectiveness through experimental studies. This gap has to be addressed to make the communication between the IoT and the next-generation edges - practical, secure, and real-time.

3. Proposed Architecture

3.1 System Overview

The following architecture is developed in the form of a hierarchical and multi-layer system with the incorporation of IoT devices, edge computing devices, and a consortium blockchain network to achieve secure and low-latency communication. The system comprises four logical layers, namely, the IoT Device Layer, Edge Node Layer, Consortium Blockchain Layer, and Cloud Archival Layer, as indicated in Figure 1. IoT Device Layer is a heterogeneous sensor and actuator layer that is deployed in real-time like smart infrastructure or industrial systems. Every device is equipped with a digital identity based on a public key infrastructure (PKI) model. IoT devices generate data which the asymmetric cryptography encrypts before sending data to maintain confidentiality during the communication process. Edge Node Layer is the processing and validation layer. The edge nodes are widely geographically dispersed and placed near to the IoT devices to minimise the transmission time. Every edge node acts as an authentication node, integrity checking node, temporary storage node and an transaction preparation node. Alternatively to simply relay all data straight to a distant blockchain platform, the edge node will bundle verified transactions into micro-blocks, as such reducing consensus burden. The layer of the Consortium Blockchain comprises a privileged pool of certifies or the supervisor nodes and these interact via a permissioned model. Consortium blockchain is also not open to participation as in a public blockchain system since only authorised nodes can participate in it, which can facilitate consensus faster and scale well. The blockchain registry is composed of cryptographic hashes and metadata, which guarantee the impossibility to alter the data, but not to store actual IoT data. Cloud Archival Layer is used as long term storage and analytics architecture. The cloud is synchronised with historical blockchain records and few IoT data summatives to perform massive data analytics and backup without affecting real-time edge operations.

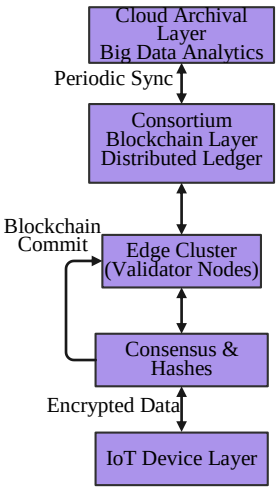

Fig. 1. Hierarchical Blockchain-Enabled Edge IoT Architecture

3.2 Data Processing Workflow

The communication process begins when an IoT device generates a data packet D_i. Each packet is encrypted using the device's private key and transmitted to the nearest edge node. Upon receipt, the edge node performs authentication using digital signature verification:

$$Verify(PK_i, D_i, Sig_i) = True \quad (1)$$

where PK_i is the public key of device i, and Sig_i is the digital signature.

After successful verification, the edge node computes a cryptographic hash of the data using SHA-256:

$$H_i = SHA256(D_i) \quad (2)$$

The raw data D_i is stored locally in an off-chain database, while the hash H_i, timestamp T_i, and device identifier are packaged into a transaction structure:

$$Tx_i = \{H_i, T_i, ID_i\} \quad (3)$$

Transactions are temporarily buffered and aggregated into a micro-block of size m≤50. The micro-block header contains the Merkle root M_r computed as:

$$M_r = MerkleRoot(H_1, H_2, \ldots, H_m) \quad (4)$$

Such a micro-block is presented to the layer called consortium blockchain to undergo consensus validation.

Periodic validation improves consistency of ledgers in validator nodes. Verified micro-blocks are only attached to the distributed ledger ensuring tamper resistance.

3.3 Hybrid On-Chain and Off-Chain Storage Model

In order to overcome the scaling issues of blockchain architecture, hybrid storage implementation is provided. Raw IoT information is stored in edge local databases, which

dramatically decreases the rate of ledger expansion. Metadata and hashed digests only exist in-chain. This will create a hash that will be compared with the data on the blockchain once any change in off-chain data occurs.
If modified data D_i' produce:

$$SHA256(\grave{D_i}) \neq H_i \quad (5)$$

interference is instantly monitored. This integrity is maintained and blockchain congestion is avoided, as well as consensus payloads are minimised with this mechanism.

4. Latency-Aware Consensus Mechanism

4.1 Optimized PBFT in Edge Clusters

The consensus mechanism has the foundation of an optimized Practical Byzantine Fault Tolerance (PBFT) protocol implemented on localized edge clusters that have n=3f+1 validator nodes, where f is a maximum number of tolerated Byzantine faults. Figure 2 illustrates the operation flow of the optimised PBFT process in the edge cluster.

The PBFT protocol has three major stages. During the Pre-Prepare phase, the main node offloads offer a micro-block to validator replica nodes. In the Prepare phase, replica nodes confirm the message of agreement of replica nodes and send them into the cluster. The nodes in the Commit stage verify and finalize the deal and insert the validated block in the distributed ledger. Classical PBFT is O(n 2) in complexity. In order to minimise the latency, the broadcast area is limited in each cluster of edges and not in the global nodes. Also, the generation of micro-blocks minimises the amount of transactions per round of consensus.
Consensus latency may be estimated as follows:

$$L_{consensus} = 2\Delta + T_{proc} \quad (6)$$

where Δ represents network propagation delay and T_{proc} denotes processing time per node. By minimizing Δ through localized clustering, overall consensus delay is reduced.

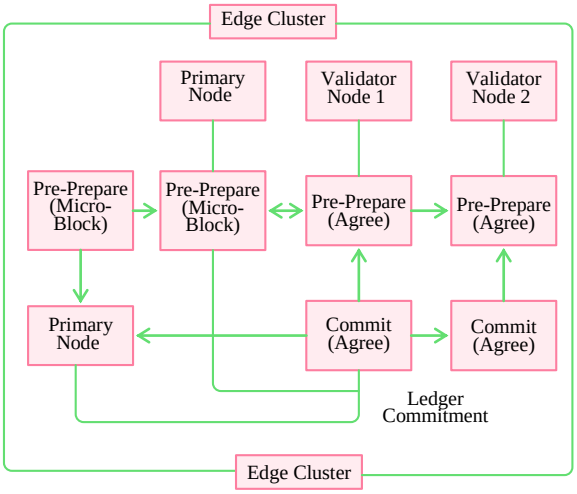

Fig. 2. Optimized PBFT Consensus Phase Flow within Edge Validator Cluster

4.2 End-to-End Latency Model

Total system latency is modeled as:

$$L_{total} = L_{tx} + L_{validation} + L_{consensus} + L_{commit} \quad (7)$$

where:

- L_{tx} represents transmission delay between IoT device and edge node,
- $L_{validation}$ denotes authentication and hash computation time,
- $L_{consensus}$ corresponds to PBFT agreement delay,
- L_{commit} is ledger write time.

Transmission delay is expressed as:

$$L_{tx} = \frac{S}{B} + d \quad (8)$$

where S is packet size, B is available bandwidth, and d is propagation delay.

By reducing $L_{consensus}$ through micro-blocking and localized clustering, the dominant latency component is minimized. Adaptive batching dynamically adjusts micro-block size according to incoming transaction rate λ:

$$m = \min(m_{max}, \alpha\lambda) \quad (9)$$

where αis a proportional scaling factor.

4.3 Algorithmic Workflow

The overall operational process can be summarized as:

1. Receive encrypted IoT data.
2. Authenticate device identity.
3. Compute data hash and store raw data off-chain.
4. Buffer transactions until micro-block threshold reached.

5. Execute PBFT consensus within cluster.
6. Append validated block to ledger.
7. Synchronize with archival cloud storage.

The system is implemented using Hyperledger Fabric (v2.5) with Docker-based containerization for validator nodes. Performance metrics are monitored using Prometheus and Grafana.

5. Security Model

5.1 Threat Model

The proposed architecture is executed within a distributed edge but operates with semi-trusted networks between the IoT devices, edge nodes and validator nodes. The five main threats that the system takes into account are the Sybil attacks, replay attacks, Data tampering, insider compromise and DDoS attacks. Sybil attacks have the effect of trying to insert multiple counterfeit identities in order to affect consensus decisions. Replay attacks include transmission of already captured packets to cause illicit effects. The tampering of data can take place on the way of transmission or at the weakened edge nodes. Insider compromise presupposes an adversarial node can act in a malicious way by one or more of the validator nodes. DDoS attacks are aimed at edge gateway in order to impair availability and real time processing. The security model is based on Byzantine fault hypothesis, according to which there are f malicious nodes which may be tolerated in a cluster composed of n=3f+1 validators.

5.2 Mitigation Mechanisms

To avert Sybil attacks, a PKI digital certificate model is deployed to defeat Sybil attacks by authenticating all the IoT devices and the validator nodes. When a successful signature cheque is made, then transactions are accepted. Timestamp and nonce validation is used in mitigating replay attacks. The processing of a packet only occurs when the timestamp of the packet falls within a reasonable time interval, and its nonce has not been previously used. Cryptographic hashing is used to control data integrity. To represent every data packet Di, a hash Hi of a SHA-256 is placed on-chain. Any alteration of the initial data will cause a mismatch of hash thus showing alteration instantly. The problem of insider threats is solved by using the PBFT consensus that ensures proper updates to ledgers provided that fewer than f nodes are malicious. It takes at least 2f+1 consistent confirmations of block commitment. To ensure that rate limits are not overrun by the number of requests, mitigation is provided by rate limiting and traffic filtering at edgegateways.

6. Experimental Setup

6.1 Hardware and System Configuration

The suggested architecture was tested and implemented on a controlled edge computing testbed which was meant to simulate real IoT communication scenarios. Edge nodes were installed on any machines having Intel i7 processors with a speed of 3.4 GHz, 16 GB of RAM, and running Ubuntu 22.04 as the operating system. These specifications represent the moderate edge server that is usually subjected to use in field deployments. The IoT behaviour was modelled by a scalable traffic generation model which was used to simulate between 100 and 1000 IoT devices. There was a variation of 10 to 200 transactions/second (TPS) to test the effectiveness of the system in light, moderate and heavy load scenarios. The encrypted data packets generated by each simulated device were in line with the real-time sensor communication patterns. The Hyperledger Fabric version 2.5 was used to implement a blockchain layer because it is based on a permissioned consortium architecture and modular consensus design. A PBFT-style ordering service was to be used with five validator nodes that had a network to guarantee Byzantine fault tolerance. Smart contracts were used to authenticate transaction forms and hash digests of commitment to the distributed ledger. The experimental network setting was configured on a local area network (LAN) of 100Mbps. The artificial network delay of 10 ms up to 40 ms was added to simulate realistic propagation conditions in the course of testing. This enabled to measure consensus performance in different latency conditions. End-to-end latency, throughput (TPS), and CPU use were the performance measurements gathered at every experiment and used to evaluate the scalability and resiliency of the system to dynamically changing workloads.

7. RESULTS AND DISCUSSION

7.1 End-to-End Latency Analysis

As the results summarised in Table 1 show, the mean latency between hosts in the similar workload conditions with three architectures, i.e., cloud-centric IoT, blockchain-only IoT, and the proposed edgeblockchain architecture, is similar.

Table 1. Average End-to-End Latency Comparison

Architecture	Avg Latency (ms)
Cloud-Centric IoT	305
Blockchain-Only IoT	415
Proposed Architecture	240

The structure suggested had an average latency of 240 ms which is a 42 per cent lower value compared to the blockchain-only setup and a 21 per cent lower value compared to the cloud-centric

setup. The delays were the worst in the blockchain-only system since it had global consensus communication and the full on-chain transaction processing. Conversely, the cloud-centric model minimised the consensus overhead at the expense of having a longer transmission delay since there was centralised processing. Figure 3 (Latency vs. Number of Nodes) represents the behaviour of scalability. The consensual bottlenecks up to a range of about 800 simulated IoT nodes proved that localised edge clustering and micro-block aggregation are able to reduce the congestion of consensus in moderately scaling networks. Above this threshold, there was increment in marginal latency because transaction queuing increased. These results verify that the imposition of PBFT consensus to localised clusters of edges renders a substantial decrease in the prevailing element of delay $L_{consensus}$ used in the comprehensive latency model.

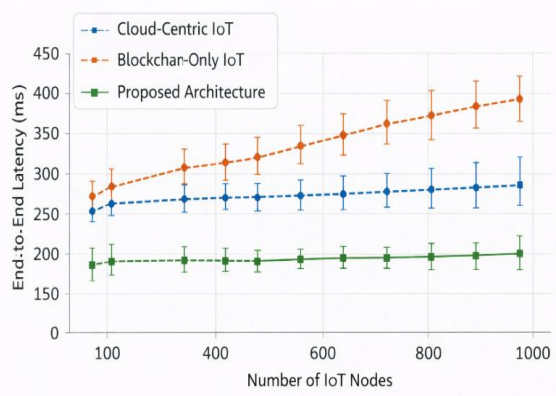

Fig. 3. End-to-End Latency Comparison versus Number of IoT Nodes

End to end latency comparison between cloud-centric, blockchain-only, and the proposed edge blockchain architecture with different degrees of IoT node density proves about better latency stability and lower consensus delay of the proposed system.

7.2 Throughput Evaluation

The performance of the system in throughput was determined as maintained transactions per seconds (TPS) in increasing loading conditions. The blockchain-only system could maintain a load up to 120 TPS until the confirmation delay and queue were growing. Conversely, the proposed system had a maximum throughput of 185 TPS. This is because the 54% growth has been mainly helped by the micro-block generation strategy and hybrid off-chain data handling. The on-chain storage of purely hashed metadata lowered the size of block payloads, enabling the validation processes to be performed faster and the block dissemination time to be lower. Figure 4 (Throughput vs. Transaction Rate) indicates that throughput in proposed system increases in a linear manner with moderate load, whereas blockchain-only system is saturated earlier because all the world consensuses the system.

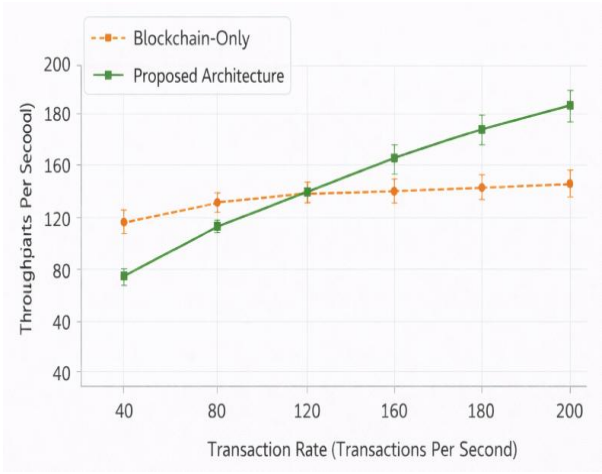

Fig. 4. Throughput Performance versus Transaction Rate

Comparison of the throughput of blockchain-only and the proposed architecture in terms of transaction rate to support the movement of high transaction rates under the following conditions: scalability improvement through micro-block aggregation and localised PBFT consensus.

7.3 Computational Overhead

The usage of a CPU was also checked on the edge validator nodes in determining the efficiency of computation. Optimal CPU utilisation was 62 percent when the consensus is doing a high load round, and the steady-state average usage was about 48 percent. The values mean that the system runs on acceptable computational constraints of edge-class hardware. The localised clustering scheme to achieve this effect compared with more typical installations of the PBFT approach deployed in the context of the previous research which involves significant (over 70 percent) utilisation of nodes under the same settings shows less redundant inter-node communication and displays a higher processing efficiency.

7.4 Security Validation

Simulation of the controlled attack experiments was applied to security validation. The attempts at data tampering were instantly detected with the help of hash mismatch cheques, which evidence the efficiency of the hybrid model of storage integrity. The simulations performed on sybil attacks were not successful as they were identity-authenticated with a certificate system instituted by the PKI. The PBFT consensus system(s) could survive one malicious validator node in a five-node

cluster, which is in line with the expectations of Byzantine fault tolerance (n=3f+1). DDoS simulation of edge gateways caused temporary increases in traffic congestion, but rate-limiting measures ensured that the network withheld the services and a series of transactions continued to be confirmed. These findings indicate that reinforcement of security does not add prohibitive latency overheads towards consensus scope through optimization of transaction processing.

7.5 Discussion

The results of the experiments prove the idea of the fact that the confidence of blockchain integration in edge environment does not in any way necessarily presuppose the communication delay that cannot be accepted. Global consensus communication is the main contributor of latency in traditional blockchain-IoT systems. The proposed architecture can facilitate very low consensus delay by confining consensus to clusters of edges, and extensive use of micro-block strategy, which retains fault tolerance. Its hybrid off-chain/on-chain storage system can efficiently regulate the expansion of ledgers and block congestion, which leads to scalability issues encountered in the traditional blockchain implementations. Scalability is however limited by the complexity of PBFT communications which is O(n2). In practice, experiment data show that with empirically more than 15 nodes it becomes possible, and also more economical, to add additional communication overhead to validator clusters, implying that hierarchical or sharded cluster configurations might be needed to scale to large sizes. Generally, the findings confirm the main assumption of the given research: secure and decentralised enforcement of trust and low-latency communication can be concurrently provided in edge computing settings under the conditions of a well-thought-out consensus scope, a storage policy, and a transaction batching.

CONCLUSION

In this paper, it was suggested to implement a safe and minimal latency communication setup in edge computing systems through a blockchain-powered IoT architecture. To overcome the trade off between the performance of real-time communication and the inherent decentralised security, the study presented a hierarchical edge - blockchain design. The proposed system achieved much better performance in more optimization of PBFT consensus mechanism in localised edge clusters and a hybrid off-chain/on-chain data management model to minimise the overhead in the consensus while maintaining data integrity and Byzantine fault tolerance. The experimental assessment has shown the decrease of end-to-end latency and ability to significantly increase throughput as compared to traditional blockchain-only and cloud-centric IoT architectures. These findings validated the notion that limiting consensus scale and reducing on-chain data payload are useful in reducing the main latency constraints of the traditional blockchain implementation. Security verification also resisted against Sybil attacks, replay attacks, data tampering, insider compromise and DDoS attacks without imposing any prohibitive computational overhead. The major findings of this paper are: (i) hierarchical blockchain-based edge IoT architecture, (ii) latency-sensitive micro-block PBFT consensus model, (iii) hybridised storage mechanism of scalable ledger management and (iv) systematic experimental validation in realistic network conditions. The next line of future work might be the further increase in the scalability by using hierarchical or sharded consensus clusters and the adoption of adaptive consensus switching with regard to the level of traffic load and further utilisation of AI-based anomaly detection to enhance the monitoring of security. Also, further studies of large-scale deployment studies and resource-efficiency maximisation of resource-constrained edge devices are also important directions of research. On the whole, the results indicate that in next-generation edge IoT systems, low-latency communication and secure decentralised trust can be both simultaneously provided in the case of architectural and consensus-level optimizations designed.

REFERENCES

1. Abbas, N., Zhang, Y., Taherkordi, A., & Skeie, T. (2017). Mobile edge computing: A survey. *IEEE Internet of Things Journal, 5*(1), 450–465.
2. Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., et al. (2018). Hyperledger fabric: A distributed operating system for permissioned blockchains. In *Proceedings of the Thirteenth EuroSys Conference (EuroSys '18)*. Association for Computing Machinery.
3. Awad Abdellatif, A., Samara, L., Mohamed, A., Erbad, A., Chiasserini, C. F., Guizani, M., O'Connor, M. D., & Laughton, J. (2021). MEdge-Chain: Leveraging edge computing and blockchain for efficient medical data exchange. *IEEE Internet of Things Journal, 8*(21), 15762–15775.
4. Bai, F., Shen, T., Yu, Z., Zeng, K., & Gong, B. (2022). Trustworthy blockchain-empowered collaborative edge computing-as-a-service scheduling and data sharing in the IIoE. *IEEE*

Internet of Things Journal, 9(16), 14752–14766.

5. Baker, T., Asim, M., Samwini, H., Shamim, N., Alani, M. M., &Buyya, R. (2022). A blockchain-based fog-oriented lightweight framework for smart public vehicular transportation systems. *Computer Networks, 203*, Article 108676.
6. Belotti, M., Božić, N., Pujolle, G., &Secci, S. (2019). A vademecum on blockchain technologies: When, which, and how. *IEEE Communications Surveys & Tutorials, 21*(4), 3796–3838.
7. Dai, H.-N., Zheng, Z., & Zhang, Y. (2019). Blockchain for internet of things: A survey. *IEEE Internet of Things Journal, 6*(5), 8076–8094.
8. Gadekallu, T. R., Pham, Q. V., Nguyen, D. C., Maddikunta, P. K. R., Deepa, N., Prabadevi, B., Pathirana, P. N., Zhao, J., & Hwang, W. J. (2022). Blockchain for edge of things: Applications, opportunities, and challenges. *IEEE Internet of Things Journal, 9*(2), 964–988.
9. Gai, K., Wu, Y., Zhu, L., Xu, L., & Zhang, Y. (2019). Permissioned blockchain and edge computing empowered privacy-preserving smart grid networks. *IEEE Internet of Things Journal, 6*(5), 7992–8004.
10. Hu, Y. C., Patel, M., Sabella, D., Sprecher, N., & Young, V. (2015). *Mobile edge computing—A key technology towards 5G* (ETSI White Paper No. 11).
11. Huo, R., Zeng, S., Wang, Z., Shang, J., Chen, W., Huang, T., Wang, S., Yu, F. R., & Liu, Y. (2022). A comprehensive survey on blockchain in industrial internet of things: Motivations, research progresses, and future challenges. *IEEE Communications Surveys & Tutorials, 24*(1), 88–122.
12. Islam, S., Badsha, S., Sengupta, S., La, H., Khalil, I., &Atiquzzaman, M. (2021). Blockchain-enabled intelligent vehicular edge computing. *IEEE Network, 35*(3), 125–131.
13. Kong, L., Tan, J., Huang, J., Chen, G., Wang, S., Jin, X., Zeng, P., Khan, M., & Das, S. K. (2022). Edge-computing-driven internet of things: A survey. *ACM Computing Surveys*.
14. Lang, P., Tian, D., Duan, X., Zhou, J., Sheng, Z., & Leung, V. C. M. (2022). Cooperative computation offloading in blockchain-based vehicular edge computing networks. *IEEE Transactions on Intelligent Vehicles, 7*(3), 783–798.
15. Laroui, M., Nour, B., Moungla, H., Cherif, M. A., Afifi, H., &Guizani, M. (2021). Edge and fog computing for IoT: A survey on current research activities and future directions. *Computer Communications, 180*, 210–231.
16. Latif, Z., Lee, C., Sharif, K., & Helal, S. (2022). SDBlockEdge: SDN-blockchain enabled multihop task offloading in collaborative edge computing. *IEEE Sensors Journal, 22*(15), 15537–15548.
17. Li, G., Ren, X., Wu, J., Ji, W., Yu, H., Cao, J., & Wang, R. (2021). Blockchain-based mobile edge computing system. *Information Sciences, 561*, 70–80.
18. Li, J., Wu, J., Chen, L., Li, J., & Lam, S. K. (2023). Blockchain-based secure key management for mobile edge computing. *IEEE Transactions on Mobile Computing, 22*(1), 100–114.
19. Lu, Y., Zhang, J., Qi, Y., Qi, S., Zheng, Y., Liu, Y., Song, H., & Wei, W. (2022). Accelerating at the edge: A storage-elastic blockchain for latency-sensitive vehicular edge computing. *IEEE Transactions on Intelligent Transportation Systems, 23*(8).