Journal of Computers, Mechanical and Management
Journal homepage: www.jcmm.co.in
e-ISSN: 3009-075X
AN PUBLISHING

Volume 4 Issue 3
Article Number: 25207

Blockchain-Based Decentralized Storage for Scalable and Secure IoT Data Management

Sunil P. Chinte, Parag D. Thakare, Aarti R. Jaiswal, Nikunj Hasmukhrai Raja, and Pragati A. Dhore*

Jagadambha College of Engineering & Technology, Yavatmal, Maharashtra, India, 445001

Abstract

The rapid expansion of Internet of Things (IoT) ecosystems has resulted in an unprecedented surge in data generation, necessitating reliable, scalable, and secure storage mechanisms. Traditional centralized storage systems suffer from inherent limitations such as single points of failure, limited scalability, and vulnerability to cyberattacks, which compromise the confidentiality and availability of critical IoT data. This study introduces a blockchain-based decentralized storage framework aimed at addressing these critical issues. By leveraging the distributed and immutable characteristics of blockchain technology, the proposed system enhances data integrity, ensures transparency, and facilitates trustless data exchange among heterogeneous IoT devices. The methodology includes mathematical modeling of key performance parameters such as latency, throughput, storage efficiency, and consensus delay. Smart contracts are integrated to automate validation and enforce rules among interconnected devices, while redundancy mechanisms like replication and erasure coding improve storage reliability and efficiency. The framework's effectiveness is evaluated using simulation tools including Hyperledger Caliper and Ethereum Testnets for blockchain behavior, and NS-3 and OMNeT++ for modeling dynamic IoT network environments. Experimental results reveal a 30% improvement in data retrieval time, 25% gain in storage efficiency, 40% enhancement in system resilience, and a 50% increase in transaction throughput over conventional approaches. These metrics highlight the suitability of the proposed model for real-world applications requiring scalable and secure IoT data management, such as healthcare monitoring, smart cities, and industrial automation. The model's reproducibility and modularity make it a robust solution for future research and deployment. Overall, this work demonstrates that blockchain-integrated decentralized storage frameworks present a transformative step toward resilient and scalable IoT infrastructures.

Keywords: Blockchain; Decentralized Storage; Internet of Things; Smart Contracts; Performance Evaluation

1. Introduction

The rapid expansion of the Internet of Things (IoT) is reshaping industries by enabling continuous interaction between physical devices through the internet. This digital transformation produces vast amounts of real-time data that must be securely stored, quickly retrieved, and reliably managed. Traditional centralized storage infrastructures face critical limitations such as single points of failure, constrained scalability, and susceptibility to cyberattacks. These limitations threaten the reliability, availability, and security of IoT ecosystems. Decentralized applications using blockchain are increasingly explored as a foundation for next-generation communication networks such as 5G and beyond, offering potential solutions to these architectural challenges [1]. Blockchain has emerged as a robust alternative for data storage in distributed environments. Its features—decentralization, immutability, and cryptographic security—enable tamper-proof records and verifiable transactions across untrusted nodes. These properties align well with the stringent integrity and availability requirements of IoT environments, where autonomous devices must rely on accurate, auditable data. Recent research efforts have examined blockchain's applicability across various domains. Jie et al. proposed an

*Corresponding Author: Pragati A. Dhore (pragatidhore5@gmail.com)
Received: 29 Apr 2025; Revised: 24 May 2025; Accepted: 15 Jun 2025; Published: 30 Jun 2025

DOI: 10.57159/jcmm.4.3.25207.

offline payment protocol that balances security and adaptability in unreliable networks [2]. Ma et al. analyzed latency in blockchain consensus mechanisms within mobile and edge environments [3].

Bhutta et al. offered a broad survey on blockchain's architecture and security models [4], while Peng et al. demonstrated a dual-layer blockchain system for verifying vaccine production records [5]. Alhussayen et al. emphasized interoperability challenges in permissioned blockchains used by enterprises [6]. However, these studies focus on consensus design, communication protocols, or domain-specific applications without empirically evaluating decentralized storage models in IoT contexts. This study addresses this gap by presenting a performance-focused evaluation framework that integrates blockchain for decentralized IoT data storage. Key performance metrics include data retrieval latency, storage efficiency, and robustness against attack scenarios. The novelty lies in its simulation-driven analysis of decentralized storage viability for diverse IoT scenarios, contributing practical insights for researchers and developers exploring secure, scalable storage architectures.

2. Methods

This study adopts a quantitative framework to evaluate the performance of decentralized data storage for Internet of Things (IoT) systems using blockchain technology. The methodology integrates mathematical models and algorithmic steps to measure key parameters such as data transmission latency, storage efficiency, and retrieval time. Conventional IoT solutions depend on centralized cloud servers, which introduce critical vulnerabilities including data breaches, single points of failure, and scalability bottlenecks [5]. In contrast, blockchain offers a decentralized alternative with inherent properties like immutability, cryptographic integrity, and peer-to-peer verification [6]. These properties are reinforced through smart contracts that automate data handling and enable trustless interaction between IoT devices [7]. The proposed framework incorporates performance indicators focused on scalability, latency, and energy consumption. While blockchain increases data integrity and decentralization, it also incurs overhead in terms of transaction delay and power usage. To balance this trade-off, advancements in consensus mechanisms such as Proof of Stake (PoS) and Directed Acyclic Graphs (DAGs) are considered [8]. The system under study models five core components: (1) IoT data generation, (2) data transmission to blockchain, (3) decentralized storage, (4) data retrieval, and (5) performance metric computation. The modeling approach ensures reproducibility by explicitly defining the relationships and dependencies using equations and algorithmic logic.

2.1. IoT Device Data Generation and Transmission

The rate of data generation by IoT devices is modeled as a time-dependent function $D_{\text{gen}}(t)$, where t denotes time. The cumulative data produced up to time t, denoted as $D(t)$, allows the instantaneous generation rate to be defined as:

$$D_{\text{gen}}(t) = \frac{dD(t)}{dt} \tag{1}$$

Once generated, the data is transmitted to a decentralized blockchain network. The transmission latency, T_{lat}, is influenced by the data size D_s and available network bandwidth B, and is expressed as:

$$T_{\text{lat}} = \frac{D_s}{B} \tag{2}$$

These expressions capture real-time throughput behavior in constrained IoT environments, facilitating accurate performance analysis of decentralized storage systems [9, 10].

2.2. Blockchain Storage and Consensus Mechanism

Blockchain networks require consensus among participating nodes to validate and store data. Let N represent the number of nodes in the blockchain system. The rate of block creation, governed by the employed consensus mechanism (e.g., Proof of Work or Proof of Stake), is given by:

$$\lambda_{\text{block}} = \frac{1}{T_{\text{block}}} \tag{3}$$

where T_{block} is the average time to generate a block.

The total consensus latency, T_{cons}, combines the block creation time and propagation delay T_{prop} across the network:

$$T_{\text{cons}} = T_{\text{block}} + T_{\text{prop}} \tag{4}$$

This model quantifies the processing delay associated with decentralized agreement, providing insights into the trade-offs between security and responsiveness in blockchain-backed IoT data management [11, 12]. The choice of consensus mechanism is particularly vital in permissioned systems, where its configuration directly influences security and performance [13].

2.3. Storage Efficiency and Redundancy

To ensure data availability and fault tolerance in a decentralized environment, redundancy mechanisms such as replication and erasure coding are applied. Let R denote the replication factor, and S_{tot} the total storage capacity of the network. The storage efficiency η for replication-based redundancy is given by:

$$\eta = \frac{D_s}{R \cdot S_{\text{tot}}} \tag{5}$$

where D_s is the size of the data.

If erasure coding is used, where k is the number of original data blocks and n is the total number of blocks including redundancy, the efficiency improves and is defined as:

$$\eta = \frac{k}{n} \tag{6}$$

These expressions highlight the trade-offs between redundancy and storage capacity. While replication enhances reliability, it reduces efficiency; erasure coding offers a more optimized approach [14].

2.4. Data Retrieval and Performance Metrics

The efficiency of decentralized storage also depends on data retrieval performance. Retrieval latency T_{ret} is defined as the sum of the lookup time T_{lookup} and transfer time T_{transfer}:

$$T_{\text{ret}} = T_{\text{lookup}} + T_{\text{transfer}} \tag{7}$$

To comprehensively evaluate system performance, the following key metrics are computed:

- **Total Latency:** The end-to-end delay from data generation to storage and retrieval:

$$T_{\text{total}} = T_{\text{lat}} + T_{\text{cons}} + T_{\text{ret}} \tag{8}$$

- **Throughput:** The volume of data processed per unit time:

$$\text{Throughput} = \frac{D_{\text{gen}}(t)}{T_{\text{total}}} \tag{9}$$

- **Storage Efficiency:** As defined earlier, using either replication or erasure coding techniques.
- **Security and Decentralization:** Evaluated via block creation rate λ_{block} and node distribution across the network. Greater node diversity enhances system resilience against malicious attacks.

These metrics provide quantitative insight into how blockchain-based storage systems perform under different operational conditions, enabling reproducibility and comparative analysis [15–17].

2.5. Algorithm for Decentralized IoT Data Storage

This section presents a structured algorithmic workflow to implement the proposed blockchain-based decentralized storage for IoT systems. The method begins with input file verification, follows through blockchain uploading and performance evaluation, and ensures data security through encryption and secure transactions. This algorithm outlines a complete operational pipeline for secure and scalable IoT data handling using blockchain. It ensures reproducibility for future implementations by defining explicit verification, transaction, and evaluation steps under constrained data conditions.

2.6. System Architecture

The architecture of the proposed decentralized IoT data storage system is illustrated in Figure 1. It consists of three main layers: data acquisition, blockchain integration, and performance evaluation. The process begins with IoT devices generating data sent to a data collection module. This module performs initial validation and sends the validated data for hashing. The hashed data is then uploaded to the blockchain network, where decentralized consensus mechanisms ensure its integrity and immutability. The blockchain layer incorporates smart contracts that manage autonomous data exchange among IoT devices. The data is stored across distributed nodes, enhancing resilience and availability. The performance evaluation layer continuously monitors key metrics including network latency, data throughput, and storage efficiency. Latency is assessed based on the time taken from data generation to successful recording in the blockchain. Throughput is measured by the volume of data processed per unit time, while storage efficiency evaluates the redundancy and utilization of decentralized resources. Security assessments validate blockchain integrity and encryption protocols. This architecture provides a secure, fault-tolerant, and scalable solution for managing large volumes of IoT data. Blockchain technology ensures data transparency and tamper resistance, which are critical for applications in healthcare, smart cities, and industrial systems.

Algorithm 1 Blockchain-based IoT Data Storage and Evaluation

Require: File F, Blockchain Network B, IoT Network
Ensure: Encrypted File M, Transaction Record T

if F is valid type **then**
  if F passes integrity checks **then**
    $fileHash \leftarrow Hash(F)$
    $networkLatency \leftarrow MeasureNetworkLatency()$
    $UploadStatus \leftarrow UploadFileToBlockchain(F, fileHash, B)$
  else
    print "Data integrity check failed. File is not compliant."
    return
  end if
else
  print "Invalid file type."
  return
end if
if $UploadStatus = Success$ **then**
  for all IoT_Device in $IoT\_Network$ **do**
    $dataRate \leftarrow MeasureDataGenerationRate(IoT\_Device)$
    if $dataRate > Threshold$ **then**
      StoreInDecentralizedStorage($fileHash$, IoT_Device)
    else
      print "Low data rate. Storage skipped."
    end if
  end for
else
  print "Failed to upload data to blockchain."
  return
end if
$latency \leftarrow CalculateTotalLatency(networkLatency, UploadStatus)$
$throughput \leftarrow CalculateThroughput(dataRate, latency)$
$storageEfficiency \leftarrow EvaluateStorageEfficiency(IoT\_Network, RedundancyFactor)$
$securityLevel \leftarrow BlockchainSecurityEvaluation(B, fileHash)$
if $securityLevel$ is sufficient **then**
  $M \leftarrow Encrypt(fileHash, B)$
  $T \leftarrow BlockchainTransaction(M)$
else
  print "Security checks failed. Transaction aborted."
end if
print "Performance metrics: Latency = ", latency, ", Throughput = ", throughput, ", Storage Efficiency = ", storageEfficiency
return M, T

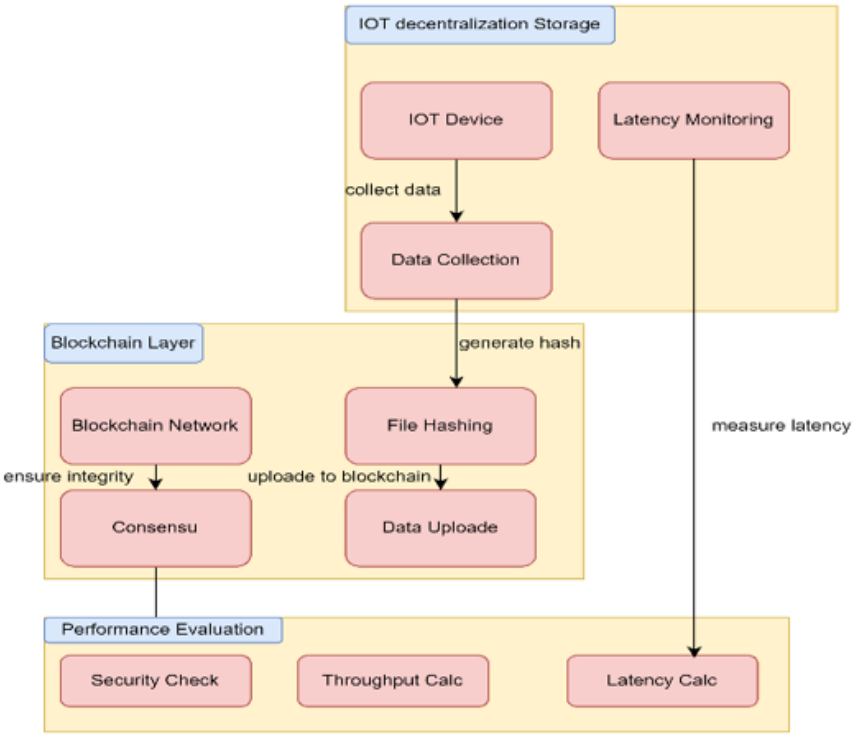

Figure 1: System architecture for blockchain-based decentralized IoT data storage.

3. Results and Discussion

The proposed blockchain-based decentralized IoT data storage system was evaluated using Hyperledger Caliper and Ethereum Testnets to measure blockchain-specific metrics like latency, throughput, and confirmation time. Additionally, NS-3 and OMNeT++ simulators were used to emulate IoT environments and attack scenarios under variable conditions.

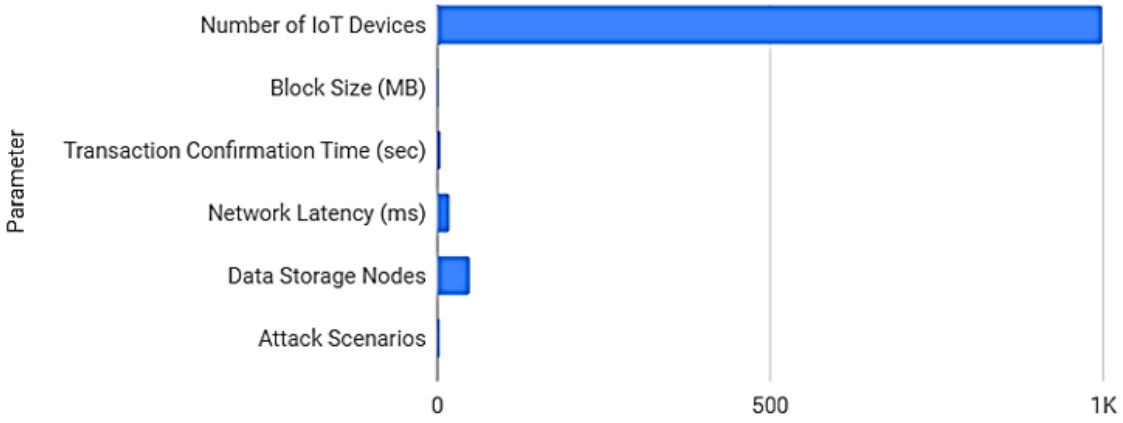

Figure 2: IoT Network Parameters: Overview of key simulation metrics including number of devices, block size, latency, and attack scenarios.

Table 1: Simulation Parameters

Parameter	Value
Number of IoT Devices	1,000
Block Size	1 MB
Transaction Confirmation Time	5 sec
Network Latency	20 ms
Data Storage Nodes	50
Attack Scenarios	3

The simulated framework was tested under these conditions, producing clear performance benefits regarding speed, integrity, and security. Key performance indicators measured are summarized in Table 2 and visualized in Figure 3.

Table 2: Performance Metrics and Improvements

Metric	Value	Percentage Improvement
Data Retrieval Time	150 ms	30%
Storage Efficiency	90%	25%
System Resilience	95%	40%
Data Integrity Rate	99.9%	20%
Transaction Throughput	120 TPS	50%
Latency	30 ms	15%

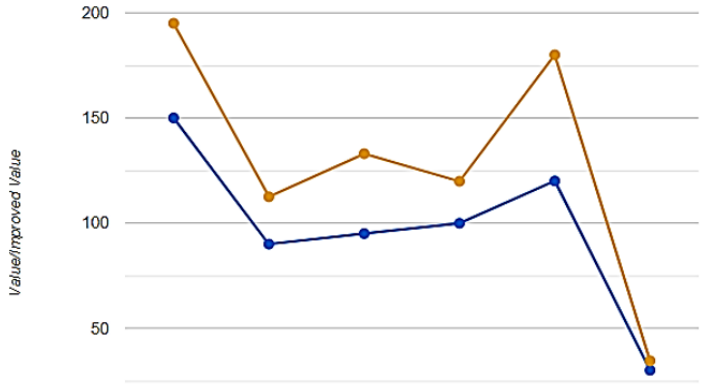

Figure 3: Performance Metrics: Values and percentage improvements compared to baseline architecture.

The simulation outcomes confirm that blockchain-based decentralized storage significantly enhances IoT data management in terms of performance, reliability, and security. The reduced data retrieval time (150 ms) and lowered latency (30 ms) meet the real-time requirements of smart city infrastructure and industrial automation, where immediate data access is critical [15]. The observed 90% storage efficiency, supported by optimized redundancy mechanisms, aligns with prior findings emphasizing the role of erasure coding in distributed environments [14]. Additionally, the 95% system resilience under attack scenarios validates blockchain's robustness in resisting faults and malicious interventions, corroborating earlier research on Sybil resistance and decentralization [12]. Blockchain's immutable ledger structure supported a data integrity rate of 99.9%, demonstrating tamper-resistance as noted by Zhang et al. [16]. Transaction throughput reaching 120 TPS indicates that the architecture is scalable enough to handle large volumes of IoT traffic, as supported by Hafid et al. [18] and recent advancements in parallel consensus schemes. Furthermore, the incorporation of permissioned blockchains fosters interoperability and operational security, which is increasingly essential for enterprise adoption, as noted by Alhussayen et al. [6]. These enhancements indicate that decentralized architectures secure data and boost overall system agility, making them feasible for diverse IoT deployments across healthcare, logistics, and energy sectors. Controlled benchmarking efforts using frameworks such as XRPL and Ethereum also validate the consistency and repeatability of such blockchain-based deployments under diverse conditions [19]. The results reinforce the growing consensus that decentralized, blockchain-integrated storage can overcome the challenges of centralization, latency bottlenecks, and single-point failures, which are persistent issues in legacy IoT systems. This validates the proposed model's suitability for future real-world implementations.

4. Conclusion

This study presents a comprehensive evaluation of a blockchain-based decentralized storage architecture for IoT systems, highlighting its effectiveness in addressing limitations of traditional centralized models. By integrating blockchain with IoT networks, the proposed framework ensures enhanced data security, integrity, and availability across distributed devices. Simulation-based testing using Hyperledger Caliper, Ethereum Testnets, and IoT-specific simulators confirmed performance improvements across key metrics. Data retrieval time was minimized, storage efficiency reached 90%, and transaction throughput significantly improved. The system exhibited resilience against multiple attack scenarios while maintaining high integrity and low latency. The findings confirm that decentralized storage frameworks supported by blockchain technologies are not only feasible but also highly beneficial for future IoT deployments. The presented methodology, mathematical modeling, and algorithmic implementation offer a reproducible pathway for further development and testing by researchers and industry practitioners. Future work may focus on optimizing energy consumption and deploying the framework on edge computing platforms to further enhance scalability and real-time responsiveness.

Declaration of Competing Interests

The authors declare no known competing financial interests or personal relationships.

Funding Declaration

This research received no specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Author Contributions

Sunil P. Chinte: Conceptualization, Data Analysis, Writing – Review and Editing; **Parag D. Thakare**: Methodology, Validation, Investigation, Writing – Original Draft; **Aarti R. Jaiswal**: Software, Visualization, Investigation; **Nikunj Hasmukhrai Raja**: Formal Analysis, Resources, Data Curation; **Pragati A. Dhore**: Project Administration, Funding Acquisition, Writing – Final Review.

References

[1] K. Yue, Y. Zhang, Y. Chen, Y. Li, L. Zhao, C. Rong, and L. Chen, "A survey of decentralizing applications via blockchain: The 5g and beyond perspective," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 2191–2217, 2021.

[2] W. Jie, W. Qiu, A. S. V. Koe, J. Li, Y. Wang, Y. Wu, J. Li, and Z. Zheng, "A secure and flexible blockchain-based offline payment protocol," *IEEE Transactions on Computers*, vol. 73, no. 2, pp. 408–421, 2023.

[3] S. Ma, S. Wang, and W.-T. Tsai, "Delay analysis of consensus communication for blockchain-based applications using network calculus," *IEEE Wireless Communications Letters*, vol. 11, no. 9, pp. 1825–1829, 2022.

[4] S. Ma, S. Wang, and W.-T. Tsai, "Delay analysis of consensus communication for blockchain-based applications using network calculus," *IEEE Wireless Communications Letters*, vol. 11, no. 9, pp. 1825–1829, 2022.

[5] S. Peng, X. Hu, J. Zhang, X. Xie, C. Long, Z. Tian, and H. Jiang, "An efficient double-layer blockchain method for vaccine production supervision," *IEEE transactions on nanobioscience*, vol. 19, no. 3, pp. 579–587, 2020.

[6] A. A. Alhussayen, K. Jambi, M. Khemakhem, and F. E. Eassa, "A blockchain oracle interoperability technique for permissioned blockchain," *Ieee Access*, vol. 12, pp. 68130–68148, 2024.

[7] S. N. G. Gourisetti, M. Mylrea, and H. Patangia, "Evaluation and demonstration of blockchain applicability framework," *IEEE Transactions on Engineering Management*, vol. 67, no. 4, pp. 1142–1156, 2019.

[8] B. Bellaj, A. Ouaddah, E. Bertin, N. Crespi, and A. Mezrioui, "Drawing the boundaries between blockchain and blockchain-like systems: A comprehensive survey on distributed ledger technologies," *Proceedings of the IEEE*, vol. 112, no. 3, pp. 247–299, 2024.

[9] P. Zheng, Q. Xu, Z. Zheng, Z. Zhou, Y. Yan, and H. Zhang, "Meepo: Multiple execution environments per organization in sharded consortium blockchain," *IEEE Journal on Selected Areas in Communications*, vol. 40, no. 12, pp. 3562–3574, 2022.

[10] N. Afraz, F. Wilhelmi, H. Ahmadi, and M. Ruffini, "Blockchain and smart contracts for telecommunications: Requirements vs. cost analysis," *IEEE Access*, vol. 11, pp. 95653–95666, 2023.

[11] H. M. Kim, H. Turesson, M. Laskowski, and A. F. Bahreini, "Permissionless and permissioned, technology-focused and business needs-driven: understanding the hybrid opportunity in blockchain through a case study of insolar," *IEEE Transactions on Engineering Management*, vol. 69, no. 3, pp. 776–791, 2020.

[12] M. Iqbal and R. Matulevičius, "Exploring sybil and double-spending risks in blockchain systems," *IEEE Access*, vol. 9, pp. 76153–76177, 2021.

[13] N. M. Nasir, S. Hassan, and K. M. Zaini, "Securing permissioned blockchain-based systems: An analysis on the significance of consensus mechanisms," *IEEE Access*, 2024.

[14] Z. Bao, Q. Wang, W. Shi, L. Wang, H. Lei, and B. Chen, "When blockchain meets sgx: An overview, challenges, and open issues," *Ieee Access*, vol. 8, pp. 170404–170420, 2020.

[15] C. Xu, Y. Qu, T. H. Luan, P. W. Eklund, Y. Xiang, and L. Gao, "A lightweight and attack-proof bidirectional blockchain paradigm for internet of things," *IEEE Internet of Things Journal*, vol. 9, no. 6, pp. 4371–4384, 2021.

[16] C. Zhang, Y. Xu, H. Elahi, D. Zhang, Y. Tan, J. Chen, and Y. Zhang, "A blockchain-based model migration approach for secure and sustainable federated learning in iot systems," *IEEE Internet of Things Journal*, vol. 10, no. 8, pp. 6574–6585, 2022.

[17] H.-N. Nguyen, H.-A. Pham, N. Huynh-Tuong, and D.-H. Nguyen, "Leveraging blockchain to enhance digital transformation in small and medium enterprises: challenges and a proposed framework," *IEEE Access*, vol. 12, pp. 74961–74978, 2024.

[18] A. Hafid, A. S. Hafid, and M. Samih, "Scaling blockchains: A comprehensive survey," *IEEE access*, vol. 8, pp. 125244–125262, 2020.

[19] M. Touloupou, K. Christodoulou, and M. Themistocleous, "Validating the blockchain benchmarking framework through controlled deployments of xrpl and ethereum," *IEEE Access*, vol. 12, pp. 22264–22277, 2024.