information

Article

An Enhanced Multi-Layer Blockchain Security Model for Improved Latency and Scalability

Basem Mohamed Elomda [1], Taher Abouzaid Abdelaty Abdelbary [1,*], Hesham Ahmed Hassan [1,2], Kamal S. Hamza [1] and Qasem Kharma [3]

[1] Egyptian e-Learning University, 33 El Messaha St., Dokki District, Giza 12611, Egypt; bmohamed@eelu.edu.eg or b.ibrahim@ammanu.edu.jo (B.M.E.); h.hassan@fci-cu.edu.eg (H.A.H.); khamza@eelu.edu.eg (K.S.H.)
[2] Faculty of Computers and Artificial Intelligence, Cairo 12613, Egypt
[3] Al-Ahliyya Amman University, Al-Saro, Al-Salt St., Amman 19111, Jordan; q.kharma@ammanu.edu.jo
* Correspondence: taher.elbary@gmail.com

Abstract: The Multi-Layer Blockchain Security Model (MLBSM) proposed in 2024 was designed to safeguard Internet of Things (IoT) networks, as well as similar network architectures, against transaction privacy leakage in public blockchain systems. MLBSM also addresses critical issues like latency, ensuring faster transaction speeds through clustering and parallel processing. This paper presents a new extension to the Multi-Layer Blockchain Security Model (MLBSM). The proposed model is called the Enhanced Multi-Layer Blockchain Security Model (EMLBSM). The proposed EMLBSM will solve latency issues by compressing and reducing the layers of the MLBSM through merging layer2 and layer3 in the MLBSM. This paper describes the required enhanced solution for latency and scalability problems that were found in the MLBSM.

Keywords: Enhanced Multi-Layer Blockchain Security Model; latency; Internet of Things; cryptography; Ethereum; Hyperledger Fabric Scalability; verification

check for updates

Academic Editor: Ge Yu

Received: 23 January 2025
Revised: 2 March 2025
Accepted: 10 March 2025
Published: 18 March 2025

Citation: Elomda, B.M.; Abdelbary, T.A.A.; Hassan, H.A.; Hamza, K.S.; Kharma, Q. An Enhanced Multi-Layer Blockchain Security Model for Improved Latency and Scalability. *Information* **2025**, *16*, 241. https://doi.org/10.3390/info16030241

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Blockchain technology facilitates the decentralization of information, with the application of cryptographic algorithms providing enhanced security and ensuring data integrity and reliability [1]. Blockchain technology is driving transformative advancements across various industries by improving security, transparency, and operational efficiency [2]. This review critically analyzes the growing importance of blockchain technology and explores key challenges, such as scalability, energy consumption, interoperability, and regulatory compliance, which represent substantial obstacles to its widespread adoption.

The Multiple Layer Blockchain Model (MLBSM) for Internet of Things (IoT) systems offers a robust solution to the unique challenges faced by IoT networks, such as security, privacy, and scalability [3]. MLBSM consists of four layers: the first layer is public blockchain, which facilitates connectivity and interoperability between different blockchain networks or systems; the second layer is local blockchains that are designed to serve a specific group of participants within a defined network or organization. To address the latency issue identified in the MLBSM, the proposed model, called the Enhanced Multi-Layer Blockchain Security Model (EMLBSM), introduces an optimized approach that significantly reduces transaction processing time. By incorporating a hierarchical structure, the model distributes transaction loads across multiple layers, enabling parallel processing and minimizing the strain on any single node. This reduces bottlenecks typically associated with high-volume

transactions in traditional blockchain networks. Additionally, the MLBSM employs a clustering technique, where related nodes are grouped to process transactions locally within their respective clusters before synchronizing with the broader network. This localized processing improves response times and enhances overall throughput [2]. Furthermore, the model uses adaptive consensus algorithms that dynamically adjust based on network conditions, allowing for faster validation and block propagation. The leakage of transaction privacy in public blockchain networks, particularly when integrated with IoT networks [3], has led to the exposure of sensitive data across the network, as well as the synchronization of this information, making it accessible and propagate across distributed nodes. Additionally, there are significant privacy concerns regarding public data, as transactions may reveal sensitive information about the parties involved. With its ability to maintain transparency, security, and privacy, the proposed model, EMLBSM, provides a promising framework for future IoT systems, enabling secure, scalable, and efficient communication between devices in a decentralized network. As IoT continues to expand, this approach will play a key role in facilitating the integration of blockchain technology, ensuring both the protection and the effective functioning of connected devices [4].

This paper is organized as follows: Section 2 shows the related work and theoretical background of recent security models, both based on blockchain and IOT. Also, Section 3 describes how the MLBSM uses its features and the opportunity of improvements to overcome the latency issues in the proposed model. The proposed EMLBSM is introduced in Section 4 by displaying its design and layers and their functions. The implementation and analysis of the proposed model is given in Section 5. Section 6 describes the security analysis and results of the proposed model, showing a comparison with other models in the same field. Finally, Section 7 concludes the paper and the results of the new model.

2. Related Works

The adoption of multi-layer blockchain security models have garnered significant attention due to their potential in enhancing security, scalability, and efficiency within decentralized systems. Recent advancements in blockchain technology have led to the development of multi-layer blockchain models that integrate different layers to optimize performance across a range of applications. These models are especially beneficial in decentralized environments such as IoT, smart cities, healthcare, and autonomous systems, where the need for secure and efficient transactions is paramount. The following literature review of a detailed examination of key research between 2020 and 2024 is summarized in Table 1:

1. Wan et al. (2019) proposed the Multi-Layer Blockchain Architecture for Secure and Scalable Cloud Systems, which integrates a private blockchain for local data processing and a public blockchain for final data storage and validation. An additional security layer provides advanced encryption techniques to protect data while ensuring that transactions are secure and scalable. The hierarchical structure significantly improves transaction throughput and reduces the risk of data breaches [5].
2. Zhang et al. (2020) proposed a multi-layer blockchain security model for IoT systems to address security challenges such as data privacy and trustworthiness. The model utilized both public and private blockchains to ensure data integrity and confidentiality, offering scalability with its two-layer architecture [6].
3. Paik et al. (2021) designed a multi-layer security framework for blockchain-based healthcare systems, focusing on patient data privacy and access control. The model integrated Layer 1 public blockchains with Layer 2 private blockchains to enhance both security and data availability. The authors emphasized how their approach outperforms existing models in terms of data access latency and trustworthiness [7].

4. Wang et al. (2022) presented a multi-layer blockchain architecture designed for smart cities, incorporating blockchain layers for secure data transmission, transactional security, and smart contract validation. The authors specifically addressed scalability and transaction throughput issues by reducing the load on the public blockchain with Layer 2 solutions [8].
5. Kumar et al. (2023) proposed a multi-layered blockchain model for secure IoT communications. This model introduced an additional layer for data encryption and multi-user authentication based on PKI, leveraging Layer 3 to provide robust security mechanisms. Their approach also enhanced scalability by offloading transaction processing to local blockchains [9].
6. TA.Bary et al. (2024) proposed the Multi-Layer Blockchain Security Model (MLBSM), which offers an effective solution for safeguarding IoT networks and similar decentralized systems, ensuring the prevention of transaction privacy leakage for all users within a public blockchain network. The integration of the clustering concept enhances the multi-layer architecture, facilitating its efficient implementation. Using this approach, the model can achieve high levels of security and transparency, thereby protecting user privacy across diverse technological environments [3].

Table 1. Conclusions drawn from the studies on multi-layer blockchain security models.

Study	Key Features	Security Focus	Scalability	Latency/ Performance
Wan et al. [5]	Multi-layer architecture for cloud systems with private and public blockchain layers	Advanced Encryption	High scalability, enhanced security	Improved throughput, reduced delay
Zhang et al. (2020) [6]	Multi-layer blockchain for IoT	Data privacy, Integrity	Scalable by integrating private and public chains	Improved latency and performance through Layer 2
Li et al. (2021) [7]	Multi-layer security for healthcare data management	Data privacy, Access control	High scalability with Layer 2 private blockchains	Reduced access latency and faster transactions
Wang et al. (2022) [8]	Blockchain for smart cities	Data transmission, Smart contract security	Enhanced scalability with Layer 2 solutions	Reduced blockchain load and enhanced throughput
Kumar et al. (2023) [9]	IoT security with multi-layered blockchain	Data encryption, Multi-user authentication	High scalability by leveraging Layer 2 blockchains	Enhanced performance and security through Layer 3
TA.Bary, et al. (2024) [3]	Multi-Layer Blockchain Security Model (MLBSM)	Data encryption, Multi-user authentication	High scalability through Layer 3 (Local blockchain)	Enhanced performance and security until 100 [TpS]

3. Multi-Layer Blockchain Security Model (MLBSM)

The MLBSM was designed to support various security configurations across different contexts. It incorporates elements such as IoT devices with limited resources, the protection of sensitive data, high-risk scenarios, and information sharing [3]. The flexibility of security configurations is influenced by factors like the effectiveness of cryptographic methods, the lifespan of keys (from short to long term), and the use of lightweight cryptography. Additionally, security options are shaped by the selection of session keys for encryption and authentication, the use of cached session keys (which can be singular, multiple, or unlimited), key ownership by different entities, and the stability of underlying protocols like TCP and UDP.

The authentication process consists of two parts: local authentication and authorization within the infrastructure layer, and the assignment of rights to objects using smart contracts. The multi-layer approach, a form of network aggregation, divides the IoT network into multiple layers. This structure integrates local authentication services with a globally distributed blockchain-based framework, isolating the need for external authorities. The system effectively addresses latency and scalability issues, driven by two primary factors: the growing volume of data traffic and the rapid increase in the number of IoT devices. By employing a multi-layered design, it creates multiple clusters that help alleviate scalability challenges.

4. Enhanced Multi-Layer Blockchain Security Model (EMLBSM)

The proposed EMLBSM consists of three layers as follows: Layer 1 is responsible for the core functions that ensure decentralization, security, and data integrity. Layer 2 in the EMLBSM is a result of merging Layer 2 and Layer 3 of the MLBSM to reduce the time spent on data propagation between layers, leading to faster transaction confirmation and an overall reduction in latency. Finally, Layer 3 ensures the integrity, confidentiality, and authenticity of the data and transactions across the IoT network and introduces a security algorithm that enables the handling of complex transactions, involving several inputs and outputs. In the proposed model, Layer 2 handles basic security and data integrity at the blockchain level, while Layer 3 facilitates off-chain transaction processing and validation. By combining the two, transactions can be processed more efficiently, with critical data stored on-chain for security and non-essential data managed off-chain to reduce network congestion. Figure 1 shows the proposed Enhanced Multi-Layer Blockchain Security Model (EMLBSM).

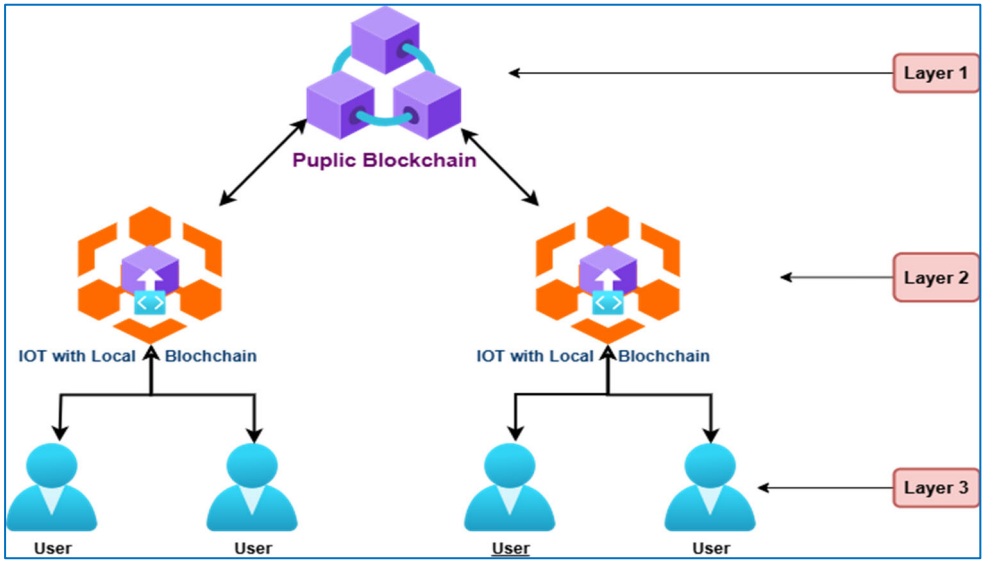

Figure 1. Improved model (EMLBSM) for the Internet of Things.

4.1. Layer1: Public Blockchain

Layer 1, in the context of a public blockchain, refers to the foundational blockchain infrastructure that provides fundamental functionalities such as decentralization, consensus mechanisms, data integrity, and security. This layer is responsible for the core functions that ensure decentralization, security, and data integrity. It implements the consensus mechanism for transaction validation, employs cryptographic techniques to secure data, and supports smart contracts for decentralized applications [3]. As the primary layer, it is responsible for the key operations that allow for a public blockchain to function efficiently and securely in an open environment where anyone can participate. This layer is responsible for the implementation of the consensus mechanism, which allows for nodes in the network to agree on the validity of transactions and the state of the blockchain. Layer 1 is responsible for ensuring the accuracy and immutability of data within the blockchain. Each transaction on the blockchain is cryptographically signed by the sender, providing authentication. Transactions are then validated by network nodes through the consensus mechanism, ensuring that only legitimate transactions are added to the ledger. Also, it manages the process of creating blocks in the blockchain. This involves the gathering of transactions from the network, validating them, and appending them to the existing chain.

4.2. Layer2: IOT with Local Blockchain

This layer is a result of merging Layer 2 and Layer 3 of the MLBSM. This merger reduces the time spent on data propagation between layers, leading to faster transaction confirmation and an overall reduction in latency. Furthermore, the unified approach enhances scalability by allowing for the system to manage a larger volume of transactions without overloading the network. With fewer bottlenecks and more efficient resource allocation, the model is better equipped to scale with the growing number of IoT devices and increasing data traffic. The hybrid architecture also ensures that security and privacy are maintained while providing the flexibility to support high-throughput operations in dynamic IoT environments. Figure 2 describes the merging process resulting in the unified layer.

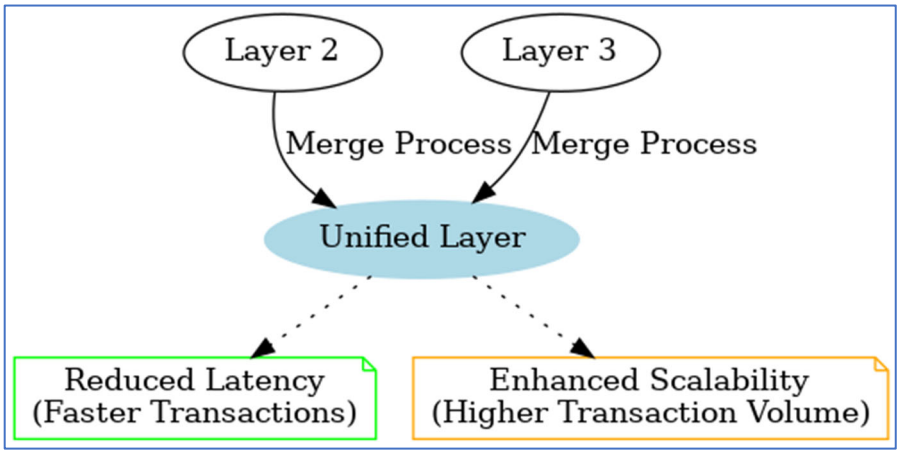

Figure 2. The unified layer is the result of merging Layer2 and 3 in the MLBSM.

Layer 2 enhances the performance and scalability of the network while preserving its core security and decentralization benefits [3]. One of the primary advantages of this layer in this model is its ability to significantly reduce latency. Traditional public blockchains often suffer from high transaction processing times, as all transactions must be validated by the entire network before they are added to the blockchain. By allowing for IoT devices to conduct transactions on their local blockchain, this layer minimizes the need for

constant communication with Layer 1, effectively reducing the delays associated with transaction validation and block propagation. This layer also addresses scalability challenges by offloading transaction processing from Layer 1 to the local blockchain, allowing for IoT networks to scale more effectively. It also can batch multiple transactions from IoT devices into a single, aggregated transaction. This reduces the number of interactions with the main blockchain, significantly increasing the throughput of the system. Within the local blockchain, IoT devices can use lightweight consensus mechanisms (e.g., Proof of Authority or federated Byzantine agreement) that are less resource-intensive than the mechanisms used in Layer 1. This allows for faster and more efficient consensus within the local network, ensuring that the scalability bottleneck is shifted away from the public blockchain. From the security side, this layer maintains strong security by leveraging cryptographic techniques and smart contract functionalities while isolating sensitive IoT transactions at the local level. Even though IoT devices may have limited resources, the use of lightweight cryptographic algorithms ensures that transactions are secure without significantly impacting performance.

4.3. Layer3: Authorization and Authentication by Users

Layer 3, as in the MLBSM, introduces an advanced security and authentication framework that allows for multiple users within an IoT ecosystem to conduct simultaneous transactions with multiple inputs and outputs. This layer builds on the fundamental security provided by Layers 1 and 2 by incorporating a multi-user authentication mechanism and leveraging Public Key Infrastructure (PKI) to establish secure communication channels. It ensures the integrity, confidentiality, and authenticity of data and transactions across the IoT network. To support multiple users engaging in simultaneous transactions, Layer 3 introduces a security algorithm that enables the handling of complex transactions involving several inputs and outputs. The algorithm ensures that all transaction participants are authenticated and that the integrity of the transaction data is preserved throughout the process. PKI plays a crucial role in establishing secure communication channels within the IoT ecosystem by ensuring the authenticity of participants and encrypting data transmission. PKI involves generating and managing digital certificates, public and private key pairs, and certificate authorities (CAs) to validate devices and encrypt communication, creating a secure environment for transactions.

5. Implementation and Analysis

Recall from the above sections that the EMLBSM aims to effectively address key challenges related to latency, scalability, and security. By leveraging a combination of public blockchains, local blockchains, and PKI for authentication and encryption, this model achieves improved performance and ensures data integrity across the entire system. While there are some complexities and overheads involved, the model offers significant benefits in terms of transaction efficiency, real-time processing, and scalability, making it well-suited for large-scale IoT deployments. The flow of data between layers shown in Figure 3.

The proposed model demonstrates significant applicability in large-scale Internet of Things (IoT) ecosystems, such as those found in smart cities, autonomous vehicles, and industrial IoT environments. By utilizing local blockchains (Layer 2), the model enhances real-time data processing by alleviating the computational burden on the public blockchain (Layer 1) and facilitating higher transaction throughput. The ability to aggregate transactions at the local blockchain level substantially reduces system latency, a critical factor for time-sensitive applications such as healthcare monitoring, smart grid management, and autonomous vehicle operations. Moreover, the model's scalability ensures that, as

the number of IoT devices grows, the system can maintain operational efficiency without compromising performance or transaction speed.

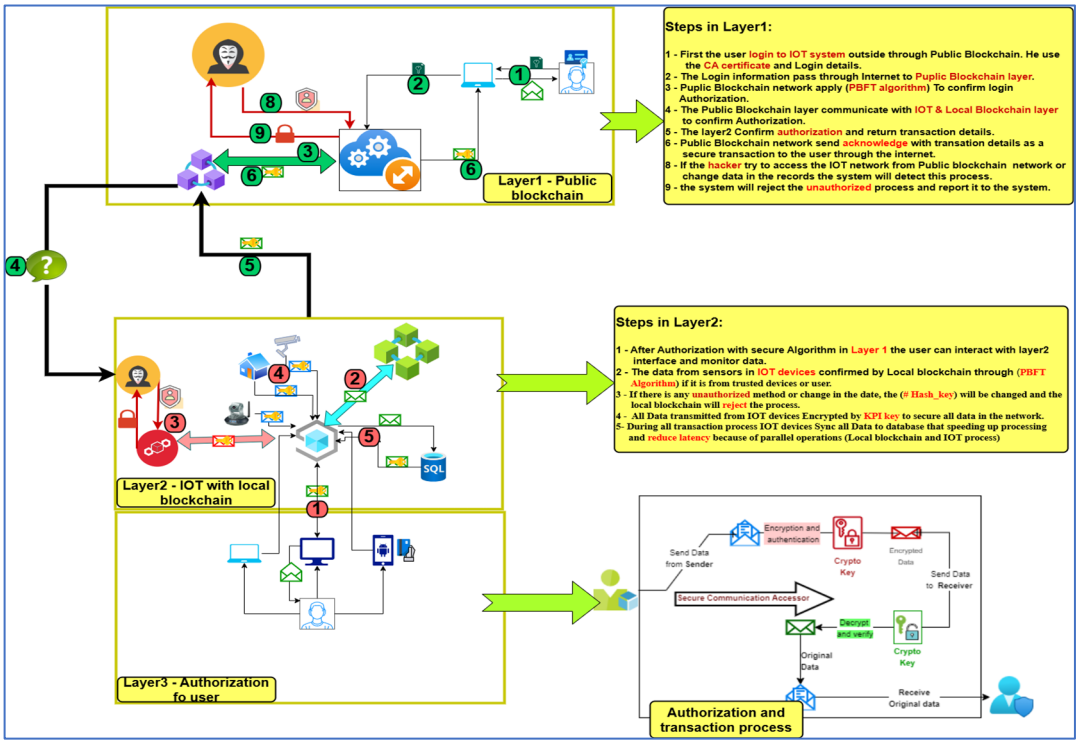

Figure 3. Data flow in the EMLBSM's layers.

The integration of Public Key Infrastructure (PKI) within the model ensures robust security for communication between IoT devices, preserving the confidentiality, integrity, and authenticity of the data transmitted across distributed systems. Furthermore, the combination of public and local blockchains offers a flexible architecture that can be tailored to various IoT environments, allowing for customizable levels of decentralization and security depending on the specific requirements of the application.

5.1. Blockchain Implementation

The blockchain implementation in the proposed model forms the core of the security and integrity verification mechanism. The model utilizes a public blockchain (Layer 1) for decentralized and immutable data storage, while IoT with local blockchains (Layer 2) handles transactions and processes at the edge, reducing congestion on the public blockchain. In addition to that, PKI-based security is applied to ensure the integrity of each transaction across the layers.

- Layer 1: Public blockchain: In this layer, a traditional public blockchain like Ethereum or a similar distributed ledger technology is used to store the final validated transactions. The Layer 1 blockchain ensures that, once data are committed, they cannot be altered or tampered with, providing transparency and trust within the IoT ecosystem.
- Layer 2: Local blockchain for IoT devices: Each IoT device or group of devices operates a local blockchain where it can perform most of the transaction processing locally. These local blockchains are linked to Layer 1 and submit aggregated, validated data periodically. This reduces the burden on the public blockchain and enhances performance, particularly for IoT systems where high-frequency data generation occurs.

- Layer 3: Multi-user authentication and PKI security: The third layer ensures the integrity of communications between devices and users by employing public–private key pairs and digital certificates for authentication and encryption. Each device and/or user is issued a digital certificate by a trusted certificate authority (CA), enabling secure communication channels. This ensures that only authenticated devices can interact with the network and that their transactions are securely recorded on the blockchain.

5.2. Security Implementation

Security is a critical aspect of any IoT system, and this model leverages several techniques to maintain the confidentiality, integrity, and authenticity of data and transactions.

- Encryption and data integrity: PKI provides the foundation for encrypting communications and securing sensitive data. Every message or transaction sent across the network is encrypted using the recipient's public key, ensuring confidentiality. Additionally, digital signatures are used to verify the authenticity of the transaction and ensure that it has not been tampered with.
- Multi-user authentication: The system supports multiple users or devices, allowing for them to securely authenticate and interact with the blockchain. This is achieved using a combination of PKI for individual authentication and a smart contract system for authorizing specific actions, ensuring that unauthorized users or devices are not able to initiate fraudulent transactions.
- Secure communication channels: All interactions within the IoT ecosystem are protected by secure communication channels using encryption. This prevents man-in-the-middle attacks and ensures that only legitimate devices can access the network and perform transactions.

5.3. Performance Estimation

The performance of the model is estimated based on key metrics such as transaction throughput, latency, and scalability under varying loads.

- Transaction throughput: By using local blockchains (Layer 2) for IoT devices, the system significantly reduces the number of transactions that need to be processed on the public blockchain (Layer 1). This increases throughput by allowing for high-frequency transactions to be managed locally and by only submitting aggregated data to the main blockchain. The system can manage thousands or even millions of IoT device transactions without bottlenecks.
- Latency reduction: One of the key advantages of this multi-layer model is the reduction in latency. Layer 2 local blockchains allow for transactions to be processed locally in real time, meaning that IoT devices can perform actions and exchange data without waiting for global consensus. This leads to faster response times, particularly important for real-time applications like autonomous vehicles, smart grids, and industrial IoT.
- Scalability enhanced: With the introduction of local blockchains in Layer 2, scalability is enhanced by offloading transactional processing from the main blockchain. This allows for the system to grow without being constrained by the limitations of the public blockchain's transaction processing capacity. Additionally, the clustering of IoT devices in Layer 2 creates a hierarchical structure that further improves scalability by reducing the volume of data that need to be propagated to Layer 1.

5.4. Reducing Latency

The multi-layer architecture helps significantly reduce latency by minimizing the interactions between IoT devices and the public blockchain [8]. Local blockchains (Layer 2)

allow for faster transaction processing within the IoT network, as they do not need to wait for global consensus to be achieved on every single transaction. This reduces the time it takes for IoT devices to perform actions and exchange data, enabling real-time processing for critical IoT applications.

- Edge processing: Edge computing principles are used to process data at or near the source, reducing the time required to send data to a centralized cloud server or public blockchain. Local blockchains manage most operations autonomously, reducing dependency on Layer 1 and improving response time.
- Transaction batching and aggregation: Instead of sending individual transactions to the blockchain, Layer 2 allows for transaction batching, where multiple IoT device actions are grouped into a single transaction. This reduces the number of interactions with Layer 1 and reduces the overall processing time for the entire system.

5.5. Scalability

Scalability is a crucial factor for any IoT system, as the number of connected devices grows exponentially. The model's architecture provides a scalable solution by introducing local blockchains (Layer 2) that manage a significant portion of the transaction processing, thus preventing overload on the public blockchain.

- Clustered IoT devices: IoT devices are grouped into clusters, with each cluster operating a local blockchain. This hierarchical approach helps scale the system by reducing the load on the main blockchain and allowing for each cluster to independently process transactions. This method also minimizes the amount of data that need to be propagated, thus improving scalability.
- Offloading transaction processing: Local blockchains process a large volume of transactions and only submit critical data to Layer 1. This reduces congestion and ensures that the public blockchain is not overwhelmed by high-frequency data from IoT devices. This mechanism allows for the system to scale without compromising on transaction speed or security.

6. Security Analysis and Results of the EMLBSM

The proposed model, built on Hyperledger Blockchain technology, demonstrates superior performance without latency compared to MLBSM approaches. This superiority is substantiated using a comparative analysis of the metrics presented in Table 2.

The table highlights the diverse approaches in IoT blockchain research, with EMLBSM emerging as the most comprehensive framework. It addresses all key metrics, including latency, scalability, and authentication, while employing energy-efficient consensus mechanisms like PBFT and PoC. Other frameworks offer specialized features but often lack scalability, flexibility, or energy efficiency, underscoring the need for more holistic solutions in future research.

In contrast to the previous results obtained from the MLBSM, which exhibited results nearly identical to those of the (H. Honar et al., 2021) model [14], where the graphs illustrated the relationship between latency (minimum, average, and maximum) and transactions per second, up to 100 transactions, as well as throughput, there were key differences that distinguished our prior model from Houshyar's. The MLBSM demonstrated superior privacy protection, preventing the leakage of user data. Additionally, the application domain of our model was different, as it was designed for Blockchain security in IoT networks, while Houshyar's model focused on cellular-enabled IoT networks. Consequently, it was necessary to enhance the model's performance to address latency issues, particularly under increasing transaction rates. This improvement is clearly reflected in the updated results presented in Figures 4 and 5.

Table 2. Analysis of (IOT) systems vs. proposed model in case of security and latency concerns [3].

References	IoT Application	Framework Privacy	Heterogeneity and Flexibility	Authentication	Scalability	Latency Issue	Implemented Consensus	Implemented Blockchain
[5]	Industrial IoT	✓	✓	x	x	x	PoW	Private
[10]	Smart Grids and Smart Cities	x	✓	x	✓	✓	PoW	Private
[11]	Microgrids, Smart Grids, Vehicle-to-Grids	✓	x	x	x	✓	PoW	Consortium
[12]	Industrial IoT, Energy Harvesting networks	✓	✓	x	x	x	PoW	Consortium
[13]	e-Health Application	✓	x	x	x	x	PoW	Public
[14]	IoT 5G MBS Multi-Layer Security	✓	✓	✓	✓	x	PBFT, PoC	Consortium
[15]	Multi-Layer Aggregate Verification (MLAV)	✓	✓	x	✓	x	PoW	Consortium
[3]	Multi-Layer Blockchain Security (MLBSM)	✓	✓	✓	✓	x	PBFT, PoC	Consortium
	Enhanced Multi-Layer Blockchain Scurity (EMLBSM)	✓	✓	✓	✓	✓	PBFT, PoC	Consortium

PoW: Proof of Work; PoS: Proof of Stack; PBFT: Practical Byzantine Fault Tolerance. PoC: Proof of capacity.

To address the latency requirements associated with specific input loads in the EMLBSM, it is essential to allocate resources within the blockchain network appropriately. An additional experiment was conducted to evaluate the performance of the System Under Test (SUT). This investigation included multiple rounds of benchmarking, each with varying transaction sending rates. Benchmarking spanned a range of 3000 transactions per second (T/S) to measure the maximum, average, and minimum transaction latencies and throughput, with transmission rates varying from 30 to 500 T/S. The transaction latency metrics, including the maximum, average, and minimum values for each test phase, are presented in Figure 4. Throughout the experiments, the average latency consistently remained below one second. However, when the sending rate exceeded 2000 T/S, the average latency demonstrated an upward trend. The transaction throughput at different transmission rates is shown in Figure 5. Throughput maintained a consistent rate of 100% up to a transmission rate of 220 T/S. Beyond this point, throughput declined as the sending rate approached the SUT's maximum transmission capacity of 220 T/S.

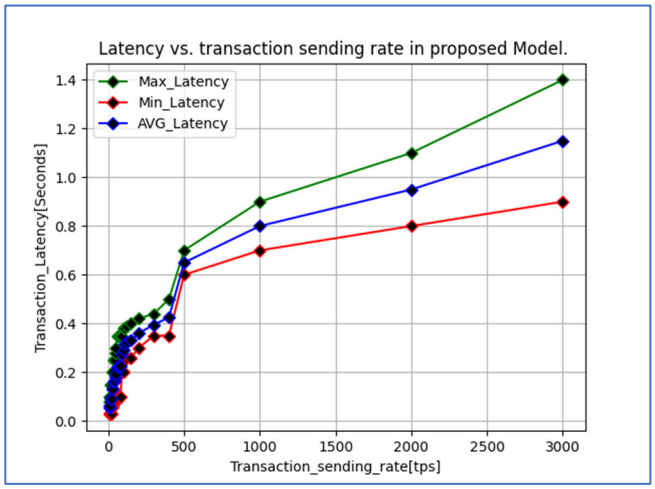

Figure 4. Transaction sending rate vs. latency.

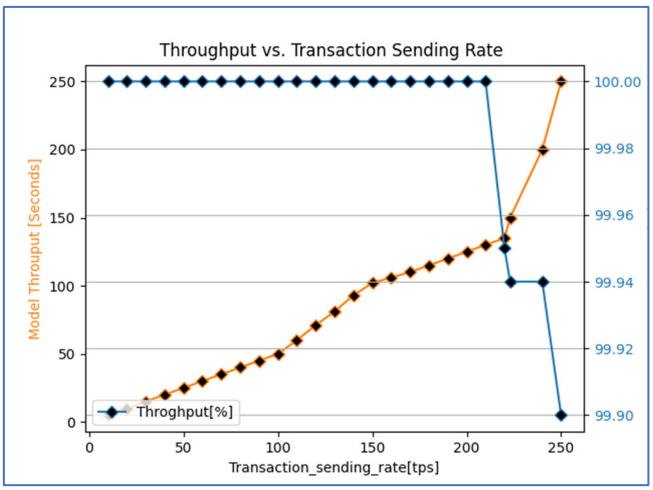

Figure 5. Transaction sending rate vs. throughput.

To clarify, each layer in the model is designed to handle specific types of data relevant to its function:

- Layer 1 (public blockchain): This layer primarily stores validated and immutable transaction data. The data here include finalized records of all validated transactions that have passed through Layer 2 (local blockchains). These transactions are critical for maintaining transparency, data integrity, and immutability across the system. The data typically contain transaction IDs, timestamps, hashes, and digital signatures, ensuring the authenticity and non-repudiation of the stored information.
- Layer 2 (local blockchain for IoT devices): The data in Layer 2 primarily involves high-frequency transaction information generated using IoT devices. This includes real-time device interactions, sensor readings, and device status updates. The data are processed and validated locally within IoT clusters, aggregated, and then submitted to Layer 1 for final storage. Key data types include transaction requests, device identifiers, aggregated sensor data, and event logs.
- Layer 3 (security and authentication): This layer handles the data related to user and device authentication, such as digital certificates, public and private keys, and transaction authorization information. The data in this layer ensure the secure communication and validation of actions between IoT devices and users, thereby preventing unauthorized access and ensuring data integrity across the system.

The experiment aimed to generate all transactions using a single user within the blockchain network. The results highlight that the performance of the blockchain system is heavily influenced by the underlying hardware infrastructure. The Hyperledger Fabric (HLF) framework employs a three-step architecture—execute, order, and validate—where each step depends on the successful completion of the preceding transactions. Finally, from the results, we found that the EMLBSM solves the latency problem in the MLBSM and ensures faster transaction speeds through clustering and parallel processing.

7. Conclusions

The proposed model Enhanced Multi-Layer Blockchain Security Model (EMLBSM) solves the important issues in the MLBSM, which resulted in improving latency through real-time transaction processing achieved through local blockchains, allowing for IoT devices to function with minimal delays. The blockchain system used in the experiment is Hyperledger for its suitability for enterprise-level applications and its unique features that make it an ideal choice for IoT and performance experiments and scalability features. In our system, we use five nodes distributed across multiple layers of the blockchain, including a consensus layer, a data layer, and a security layer, to improve latency and ensure secure transactions. The network bandwidth is set to 1 Gbps, which supports fast data transmission across the IoT network, enabling low-latency communication between nodes in the multilayer blockchain system. The workload consists of the following key components: (A) Data generation by IoT devices (e.g., temperature, humidity, location, and motion data), which are sent to the blockchain for validation and recording. (B) Data validation and consensus: Once the data are sent to the blockchain, the consensus layer validates the transactions. The security layer of the multilayer blockchain ensures that the data remain secure and tamper-proof, ensuring privacy and integrity. (C) Security measures: The workload also incorporates security protocols, including encryption and authentication, which are essential in an IoT environment. These security layers are enforced by the blockchain to ensure that data are protected throughout the transmission and validation process. The results indicate that the proposed model maintains a latency of less than one second when the transaction sending rate is below 2200 transactions per second (tps). A slight increase in latency, reaching approximately 1.2 s, is observed as the transaction sending rate rises to 3000 tps. In contrast, the MLBSM achieves sub-second latency only when the transaction sending rate is below or equal to 100 tps. However, as the transaction sending rate increases to 500 tps, the latency escalates substantially, reaching approximately 10 s. This demonstrates that the proposed model exhibits a more scalable performance, handling higher transaction rates with minimal latency compared to the MLBSM, which experiences a significant degradation in latency as the transaction rate exceeds 100 tps. The superior performance of the proposed model can be attributed to its more efficient handling of higher transaction loads, suggesting that it is better suited for environments with higher transaction throughput requirements. On the other hand, the results show that the proposed model maintains a throughput of 100% up to a transaction sending rate of 210 transactions per second (tps). A slight decrease in throughput to 99.9% is observed when the transaction sending rate increases to 250 tps. In contrast, the Machine Learning-Based Scheduling Model (MLBSM) sustains 100% throughput for transaction rates up to 100 tps, after which the throughput begins to decline, reaching approximately 70% at a transaction sending rate of 150 tps. This highlights the superior throughput efficiency of the proposed model, which is able to maintain high throughput at significantly higher transaction rates than the MLBSM, indicating better scalability and robustness under increasing transaction loads. In addition to scalability, accommodating large numbers of IoT devices and transactions using multiple local blockchains and the

ability to batch transactions significantly improves scalability. The PKI-based authentication and encryption that is used in the new model ensures secure communication and data integrity, providing a robust security framework for the entire IoT system to enhance security. To achieve transaction efficiency, the new model handles transactions locally within clusters of IoT devices and reduces the burden on the public blockchain, improving overall throughput and transaction efficiency. Finally, the new model works on reducing network congestion and improving system performance by sending only aggregated and validated data to the public blockchain, reducing network congestion.

Our future work will focus on solving the "Overhead for Local Blockchain Management" because, while local blockchains reduce congestion on the public blockchain, they introduce additional overhead in terms of managing multiple blockchain networks and ensuring consistency across them.

Author Contributions: Conceptualization, T.A.A.A.; Software, T.A.A.A.; Formal analysis, T.A.A.A.; Resources, T.A.A.A.; Writing—review & editing, T.A.A.A.; Supervision, B.M.E., H.A.H., K.S.H. and Q.K.; Funding acquisition, T.A.A.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Rebollar, F.; Ramos, M.A.; Marcial-Romero, J.R.; Hernández-Servín, J.A. Analysis of Multi-layer Information Flow in a Four-Layer Blockchain Model. In *Computer Science On-line Conference*; Springer: Berlin/Heidelberg, Germany, 2023; Volume 2, pp. 338–348.
2. Mukhlif, F.; Ithnin, N. Blockchain technology: Applications, security and privacy, big data, challenges and future directions. *Int. J. Crit. Comput. Based Syst.* **2024**, *11*, 216–233. [CrossRef]
3. Abdel Bary, T.A.A.A.; Elomda, B.M.; Hassan, H.A. Multiple Layer Public Blockchain Approach for Internet of Things (IoT) Systems. *IEEE Access* **2024**, *12*, 56431–56438. [CrossRef]
4. Abdel Bary, T.A.A.A.; Elomda, B.M.; Hassan, H.A. Blockchain: Architecture, Security and Consensus Algorithms. In *International Conference on Intelligent and Fuzzy Systems*; Springer Nature: Cham, Switzerland, 2023; pp. 738–753.
5. Wan, J.; Li, J.; Imran, M.; Li, D.; Amin, F.E. A blockchain-based solution for enhancing security and privacy in smart factory. *IEEE Trans. Ind. Informatics* **2019**, *15*, 3652–3660. [CrossRef]
6. Yang, X.; Li, Z.; Geng, Z.; Zhang, H. A Multi-Layer Blockchain Security Model for Internet of Things. *IEEE Access* **2020**, *8*, 2982975–2982985.
7. Wu, H.Y.; Li, L.J.; Paik, H.Y.; Kanhere, S.S. MEChain: A multi-layer blockchain structure with hierarchical consensus for secure EHR system. In Proceedings of the 2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Shenyang, China, 18–20 August 2021; pp. 976–987.
8. Cao, B.; Wang, Z.; Zhang, L.; Feng, D.; Peng, M.; Zhang, L.; Han, Z. Blockchain systems, technologies, and applications: A methodology perspective. *IEEE Commun. Surv. Tutor.* **2022**, *25*, 353–385. [CrossRef]
9. Kumar, P.A. A Multi-Layer Blockchain Model for Secure IoT Communications. *IEEE Access* **2023**, *11*, 1076543–1076555.
10. Biswas, K.; Muthukkumarasamy, V. Securing Smart Cities Using Blockchain Technology. In Proceedings of the 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), Sydney, Australia, 12–14 December 2016; pp. 1392–1393.
11. Kokoris-Kogias, L.; Gasser, L.; Khoffi, I.; Jovanovic, P.; Gailly, N.; Ford, B. Managing identities using blockchains and CoSi. In Proceedings of the 9th Workshop on Hot Topics in Privacy Enhancing Technologies (HotPETs 2016), Darmstadt, Germany, 19–22 May 2016.

12. Li, Z.; Kang, J.; Yu, R.; Ye, D.; Deng, Q.; Zhang, Y. Consortium blockchain for secure energy trading in industrial internet of things. *IEEE Trans. Ind. Inform.* **2017**, *14*, 3690–3700. [CrossRef]
13. Esposito, C.; De Santis, A.; Tortora, G.; Chang, H.; Choo, K.-K.R. Blockchain: A panacea for healthcare cloud-based data security and privacy? *IEEE Cloud Comput.* **2018**, *5*, 31–37. [CrossRef]
14. Pajooh, H.H.; Rashid, M.; Alam, F.; Demidenko, S. Multi-Layer Blockchain-Based Security Architecture for Internet of Things. *Sensors* **2021**, *21*, 772. [CrossRef]
15. Wu, J.; Sie, M.F.; Harding, S.A.; Lin, C.L.; Wang, S.T.; Liao, S.W. Multi-layer aggregate verification for IoT blockchain. In Proceedings of the 2021 3rd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), Paris, France, 27–30 September 2021; pp. 43–44.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.