Babylonian Journal of Internet of Things
Vol.2026, **pp**. 138–154
DOI: https://doi.org/10.58496/BJIoT/2026/009; ISSN: 3006-1083
https://mesopotamian.press/journals/index.php/BJIoT

Research Article

Blockchain-Enabled Trust Management Framework for Internet of Things Environments

Aaron Mogeni oirere [1,*], Ali Rachini [2]

[1] *Department of computer science, Murang'a University of Technology, Kenya*.

[2] *Faculty of Arts and Sciences, Holy Spirit University of Kaslik (USEK), Jounieh, Lebanon.*

ARTICLE INFO

Article History

Received 22 Apr 2026
Revised 15 May 2026
Accepted 30 Jun 2026
Published 05 Jul 2026

Keywords
Blockchain,
Internet of Things (IoT),
Trust Management,
Smart Contracts,
Decentralized Security,
Trust Evaluation,
Ethereum,
Blockchain Trust Ledger.

ABSTRACT

The growth of the Internet of Things (IoT) has made it increasingly important to have secure and reliable trust management mechanisms that can support dynamic and decentralized network environments. Traditional trust management solutions often need centralized architectures that are vulnerable to a single point of failure, manipulation of trust and low scalability. While blockchain technology is a recently promising approach to providing decentralized IoT security, many current frameworks emphasize only the authentication or data integrity aspects of security, and offer limited assistance in evaluating the trust of a system continuously, and in updating it efficiently. In this paper, the authors introduce a new Blockchain-Enabled Trust Management Framework (BETMF) that combines the blockchain, smart contract and a lightweight trust evaluation mechanism to a consistent architecture in decentralized IoT environments. It proposes a framework that will continuously monitor device interactions, confirm trust updates by smart contracts and save validated trust records in the immutable trust ledger of the blockchain. In contrast to the other methods which involve merging several computational methods or complicated consensus protocols, BETMF implements a single consensus process for trust management, which enhances transparency, trust integrity, and scalability, with minimal computational costs. The suggested framework has been established in Python, and tested with a private Ethereum blockchain that was deployed using Ganache. Experimental results showed that the Trust Decision Accuracy was 97.8%, Precision was 97.3%, Recall was 96.9%, F1-score was 97.1%, the average latency of trust update was 18.6 ms, the average latency of access decision was 31.4 ms and the blockchain throughput was 132 transactions per second. The results show that the proposed framework can achieve a good balance of security, decentralization and operation efficiency in heterogeneous IoT environments. The prominent contribution of this work is the development of a lightweight blockchain based trust management framework that reduces the difficulty of trust evaluation, offers immutable trust storage, automated smart-contract based verification and generates efficient decentralized trust management for the next generation IoT applications.

1. INTRODUCTION

With the advent of the Internet of Things (IoT), billions of heterogeneous devices that are equipped with sensing, processing, and communication capabilities are inter-connected and operate on their own, making it one of the most impactful technologies of digital transformation. As continuous connectivity becomes a reality, IoT applications have grown at an incredible pace in many areas such as smart cities, industrial automation, transportation, environmental monitoring, healthcare, and intelligent manufacturing, where real-time decision-making and resource utilization are essential. Recent developments in wireless communication, cloud computing and edge intelligence have further propelled the deployment of IoT infrastructures, transforming the environment into highly dynamic and large-scale distributed environments that constantly generate huge data that needs to be reliably communicated and securely managed [1-3].

Although these are amazing achievements, the decentralized setting of IoT environments creates many security and trust issues which can't be solved with traditional security mechanisms. The IoT devices often work with limited computational capacity and dynamically enter and exit the network, which makes them susceptible to various attacks such as Sybil attacks, bad-mouthing attacks, on-off attacks, false recommendation attacks, spoofing, and malicious node insertion attacks. The

*Corresponding author. Email: amogeni@mut.ac.ke

attacks not only impacts the data confidentiality and integrity at the top, but also deceive trust relationships between communicating devices, and ultimately decrease the trust on collaborative IoT services [4-6]. Therefore, a key enabling technology for ensuring secure communication and independent cooperation between different IoT nodes is trust management.

Current trust management approaches are mostly based on centralised architectures where a trusted server collects interaction data, trust score and distributes trust decisions across the network. While such centralized solutions do make system management easier, there are several drawbacks to this, such as a single point of failure, scalability concerns, communication bottlenecks, and greater vulnerability to insider attacks. Today, as the volume of IoT deployments grows, trust repositories are becoming harder to maintain in the central location and at the same time making the system less resilient and available for those large-scale deployments [7].

In recent years, blockchain technology has garnered much attention as a decentralized approach that can enhance trust and security in decentralized systems. However, by using an immutable distributed ledger and achieving consensus among the nodes, blockchain systems can avoid the need for centralized authorities, while providing transparency, traceability, and tamper-proof record management. Several recent papers have introduced blockchain into the IoT security solutions in order to enhance authentication, data sharing security, access control and identity management. But existing solutions mainly target the protection of data transmitted or control the authentication of devices, while dynamic evaluation and continuous updating of trust has not been sufficiently studied, especially in dynamic IoT networks where network conditions and device behaviors are continually changing [8,9].

Additionally, many blockchain-based trust management systems utilize several consensus protocols or cryptographic methods that are complex to perform to ensure security. These methods increase the resistance to attacks, but also add communication overhead, complexity, energy consumption, and transaction latency, which hinders their use on resource-limited IoT devices. Therefore, a lightweight and scalable trust management system that is able to integrate with the immutability of blockchain and efficiently evaluate trust with low computation burden and adapt to the dynamic IoT environment is still needed [10-13]. To design a trust management framework for communication and transaction networks that are based on the blockchain, this research has a general motivation; from the conventional centralized trust management to the proposed blockchain-based trust management, as shown in Figure 1. The figure emphasizes the major trust management concerns that are currently present in the existing IoT environments, identifies the current research gap, and shows the proposed decentralized framework which can support the secure, transparent, and reliable trust management.

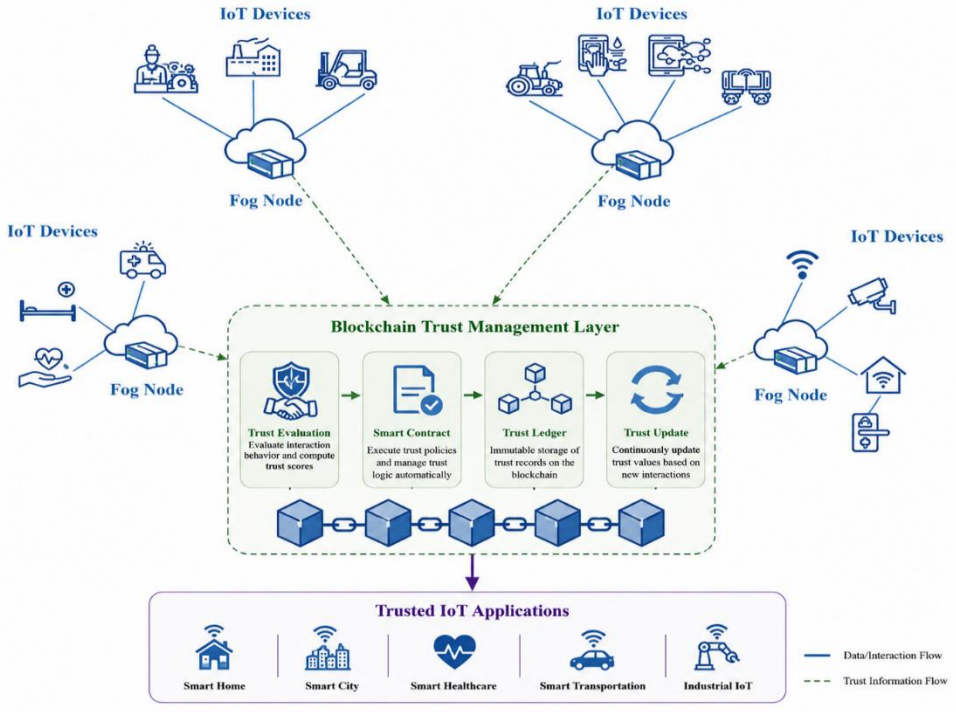


Fig. 1. Motivation of the proposed blockchain-enabled trust management framework.

To face these challenges, the Blockchain-Enabled Trust Management Framework (BETMF) is proposed in this paper for the Internet of Things. The proposed framework is based on blockchain to be a decentralized trust repository and also adds a lightweight trust evaluation mechanism that continuously updates trust score based on node interaction behavior. The main motivation of this proposed framework is to enhance the trust reliability, to withstand the trust manipulation attacks, to decrease the communication overhead and to maintain scalability for large-scale IoT deployment, which are not the focus in traditional frameworks. The proposed framework is comprehensively validated by experiments conducted with several trust- and network-related performance metrics and compared with the latest state-of-the-art trust management approaches in the blockchain field.

Compared to other existing blockchain-based IoT trust management methods which integrate various security approaches, heavy computational burden trust models or domain-specific architectures, the proposed Blockchain-Enabled Trust Management Framework (BETMF) provides a lightweight and unified trust management process. This framework combines continuous trust assessment, smart contract verification, immutable trust storage on the blockchain and decentralized access control under one roof. It is a design that is suitable for heterogeneous IoT environments, has low latency, high trust decision accuracy, low implementation complexity, and efficient use of the blockchain resources.

2. RELATED WORK

2.1. Blockchain-Based IoT Security

In an IoT setting, Blockchain is one such technology that offers decentralized data recording, immutability, data traceability, and resistance to unauthorized modification of data, making it a crucial security-enabling technology. Traditional IoT systems typically do security in a centralized manner, where the servers manage authentication, access control, and data validation. While they can be easily implemented, they can still be susceptible to single points of failure, data tampering, and unauthorized administrative control. Several recent studies have investigated how blockchain could be implemented as a distributed security layer for IoT systems, especially for scenarios where data must be shared and visible, authentication must be decentralized, and there is a need for transaction visibility and tamper resistance [14]. Recent surveys point to the fact that blockchain has been studied extensively for the security, automation, scalability, and secure data sharing of IoT deployed in heterogeneous environments.

In recent years, blockchain based IoT security frameworks are also extended to the environment of edge, fog, vehicular, healthcare, and industrial IoT. They frequently utilize smart agreements to automate access control guidelines and blockchain trust ledger to keep track of interaction histories in between devices. But most of these solutions address only the authentication or secure communications or data integrity, with the dynamism of the nodes and their degrees of trustworthiness as an afterthought. For large scale IoT networks, this limitation is crucial as nodes may act honestly at period of time and maliciously at the other due to being compromised, mobile, energy depleted, or being part of an attack [15]. Blockchain-based trust-management is therefore more and more suggested as a pre-requisite feature as it can offer tamper-proof trust records and cut down on the reliance on centralized trust authority.

2.2. Trust Management in IoT

Trust management is a key mechanism that can support secure cooperation between IoT devices, particularly when it is not enough to rely solely on the direct authentication to decide whether or not a node should be involved in communication or data exchange. In IoT environments, the trust is typically computed based on the direct interactions, indirect recommendations, packet forwarding behavior, service reliability, communication consistency, and historical reputation. Traditional trust management schemes rely on centralized trust repositories or local reputation model, but these schemes are susceptible to some attacks such as false recommendations, bad-mouthing attacks, On-off attacks and manipulating the trust score [16-18].

There has been a recent surge of research in integrating blockchain and trust management to make trust records transparent, auditable and tamper-proof after registration. Liu et al. provided a detailed survey about blockchain-based trust management for IoT and they pointed out that blockchain could be used for providing decentralized, consistent, and tamper-proof trust storage for IoT trust systems [19]. Likewise, Arshad et al. studied the decentralized trust management systems in the blockchain and proposed that blockchain enhances the reliability, integrity checking, availability, and privacy of trust information in distributed IoT environments [20]. The topic of trust and reputation mechanisms has been extensively explored in the context of IoT in more recent works, showing that trust and reputation plays a more and more crucial role in order to enable reliable device-to-device interactions in decentralized IoT environments [21].

Although such advances have been achieved, currently used trust management systems have a number of drawbacks. Certain studies employ more sophisticated blockchain, federated learning, deep learning or cryptographic techniques, potentially enhancing security yet adding to computational complexity and communication costs. Other frameworks focus on specific application domains like healthcare, Internet of Vehicles or industrial IoT and can therefore only be used in specific, more homogeneous, IoT environments. As an instance, the blockchain-based trust models for vehicular networks have shown excellent potential for secure and transparent trust evaluation, but their assumptions about mobility, infrastructure availability, and node behavior in this context may not be applicable to general IoT environments [22-24].

2.3. Research Gap and Motivation

The literature reviewed shows that blockchain has dramatically contributed to the development of security and trust management in IoT systems in a decentralized manner. But there are three major gaps that are apparent. Firstly, many blockchain-based IoT frameworks focus on authentication, access control, or secure data sharing instead of on-going trust assessment. Second, some of the trust management methods rely on heavyweight methods, which might not be applicable to resource-limited IoT devices. Third, there are many current frameworks that are domain-specific, meaning that they don't offer a simple, general-purpose model of trust that can be used in a variety of environments involving heterogeneous IoTs.

To fill these gaps, this study presents a Blockchain-Enabled Trust Management Framework which is based on a single methodology instead of multiple alternative algorithms. The proposed framework consists of lightweight trust evaluation, smart-contract based on trust policy enforcement, blockchain-based immutable trust storage, and continuous updating of trust score. This design attempts to enhance the accuracy of the Trust Decisions (TDA), transparency, scalability and trust manipulation resistance without unnecessary computational complexity.

TABLE I. COMPARISON WITH RECENT STUDIES (2022–2026)

Ref.	Focus	Methodology	Main Limitation	Relevance to This Study
[4]	Blockchain-based trust management for IoT	Survey and taxonomy of BC-TM models	Does not propose a new experimental framework	Provides foundation for trust criteria
[9]	Decentralized trust management in IoT	Comparative analysis of blockchain-based trust systems	Mainly survey-based	Supports need for decentralized trust records
[10]	Blockchain trust management in IoT/IIoT	Survey of trust mechanisms	Limited experimental implementation	Identifies IoT/IIoT trust challenges
[11]	Blockchain and AI-based trust in IoT	Review of blockchain, AI, edge/fog trust models	Complex multi-technology direction	Confirms importance of lightweight trust
[18]	Blockchain trust in Internet of Vehicles	Comprehensive IoV trust survey	Domain-specific to vehicular networks	Useful for comparison with dynamic IoT
[22]	Blockchain-enabled IoT applications	Survey of blockchain IoT applications	Broad security focus, not trust-specific	Supports blockchain role in IoT security
Proposed	Blockchain-enabled trust management for IoT	Lightweight trust evaluation with smart contract and trust ledger	To be validated experimentally	Provides concise general-purpose framework

3. PROPOSED BLOCKCHAIN-ENABLED TRUST MANAGEMENT FRAMEWORK

3.1. Framework Architecture

The aim of the proposed Blockchain-Enabled Trust Management Framework (BETMF) is to offer a lightweight trust management framework that is decentralized and secure for heterogeneous Internet of Things (IoT) environments. The proposed architecture combines trust evaluation, blockchain-based technology, and smart contracts, eliminating the need for trusted third parties or complex security measures, thereby enhancing the overall efficiency and security of the system. The combination allows IoT devices to set up secure and trusted relationships without adding unnecessary complexity or burden to the computation.

The proposed architecture is designed to address the secure trust management needs throughout the IoT ecosystem as shown in Figure 2, and makes up three logical layers working together. The top layer is the IoT environment, generating interaction information through communication continuously and with heterogeneous devices. These devices are linked to the nearby fog nodes that collect the local interaction data and relay trust-related data to the trust management layer of the blockchain. The second layer is the core of the proposed framework and known as the Blockchain Trust Management Layer. This layer provides four main purposes. On one hand, the Trust Evaluation Module is used to analyze direct interactions between the IoT devices and to compute the trust scores associated to communication behavior and service reliability. Secondly, the

predefined trust policies are automatically applied by the Smart Contract Module to decide whether to accept a trust score or to update it. Third, validated trust records are permanently recorded in the Blockchain Trust Ledger, which means that trust records from the past cannot be altered or erased by bad actors. Lastly, the Trust Update Module continuously updates the trust scores whenever new interactions happen, which enables the trust model to dynamically adjust to changing device behavior.

The third layer is trusted IoT applications that use trusted trust information to determine whether to communicate with or provide access to network resources. As trust scores exist on an immutable blockchain trust ledger, all applications on the blockchain can check the credibility of the device without having to depend on a central trust authority. This means that only devices with a high degree of trust are given access to collaborative services and malicious or less-trusted ones can be removed from the system.

The proposed architecture has a number of advantages over the conventional trust management methods. Unlike centralized trust servers, the decentralized trust blockchain ledger can no longer cause single point of failure. Smart contracts eliminate the need for human intervention in managing trust, enhancing consistency, and reliability. Moreover, ongoing updates of trust can help the framework adapt quickly to changes in behavior from IoT devices, enhancing the reliability and security of the network against trust manipulation attacks. The overall architecture of the proposed Blockchain-Enabled Trust Management Framework is shown in Fig. 2 and depicts the interaction among the IoT devices, fog nodes, Blockchain-based trust management components and trusted IoT applications.

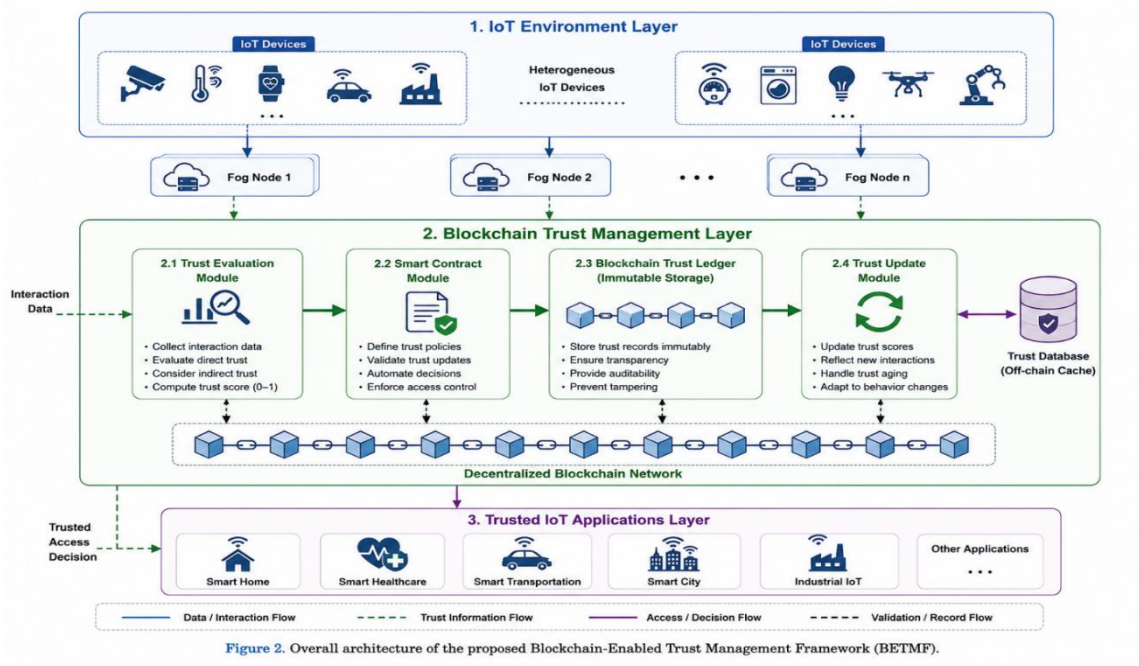


Figure 2. Overall architecture of the proposed Blockchain-Enabled Trust Management Framework (BETMF).

Fig. 2. Overall architecture of the proposed Blockchain-Enabled Trust Management Framework (BETMF).

TABLE II. COMPONENTS OF THE PROPOSED BLOCKCHAIN-ENABLED TRUST MANAGEMENT FRAMEWORK

Component	Function	Input	Output
IoT Device	Generates communication and service requests	Device interactions	Interaction records
Fog Node	Collects and forwards interaction information	Interaction records	Trust evaluation request
Trust Evaluation Module	Evaluates device behavior based on interaction history	Interaction data	Trust status
Smart Contract	Verifies trust update requests according to trust policies	Trust update request	Validated trust record

Blockchain Trust Ledger	Stores validated trust records permanently	Verified trust record	Immutable trust history
Trust Update Module	Updates device trust information	Validated trust record	Updated trust status
Access Decision Module	Determines network access based on trust status	Updated trust information	Access granted, limited, monitored, or denied

3.2. Trust Evaluation Mechanism

The trust evaluation mechanism determines the trustworthiness of a device in the IoT before it can enter into the network communication or use shared services. The suggested solution does not depend on a single trust authority, instead it continuously evaluates the behavior of the devices based on interaction history and records the trusted information in the trust ledger of the blockchain. This distributed system allows trust score to be transparent, unchangeable and tamper-proof even in dynamic IoT systems.
Firstly, when a new IoT device is added to the network, it is given a neutral trust status. The framework observes the communication behavior during the interactions, and through the fog node that is connected, it receives the interaction records and it pushes them to the communication behavior observation layer of the blockchain trust management system. These interaction records contain the success of the communication, reliability of the service, consistency of the response, validity of the transaction and adherence to the predefined security policy.

The Trust Evaluation Module examines the recorded interactions, and decides if the actions observed are deemed trustworthy or suspicious. The framework proposed here is based on three major behavioral measures: communication reliability, service reliability, and adherence to defined security policies, to obtain quantitative evaluation of credibility of the device, a Trust Score (TS) is calculated. The Trust Score model is weighted aggregation based on the following model:

$$TS = \alpha CR + \beta SR + \gamma PC$$

where **CR** represents the communication reliability of the IoT device, **SR** denotes the service reliability obtained from successful interactions, and **PC** indicates compliance with predefined security policies. The weighting coefficients **α**, **β**, and **γ** satisfy the normalization condition:

$$\alpha + \beta + \gamma = 1$$

This weighted formula is simple yet gives an effective way of assessing trust with low computational complexity. Devices that repeatedly meet communication needs will gradually increase their trust score while repeated communication failures, abnormal interactions, or policy violations will decrease the computed trust score. This means the framework is able to learn and adjust to changes in behavior without needing to be supervised and changed by hand or from a central point.
The Smart Contract Module is used to check the evaluated trust record before updating the trust information, thus automatically enforcing predefined trust management policies. The smart contract checks to see if the trust update request is authentic and trust information that is legitimate is recorded. After verification, the record of trust which is updated is permanently added to the trust ledger on the blockchain, and is made immutable and subject to audit by all authorized participants.
The final step is for the Access Decision Module to decide if an IoT device should be allowed to continue in network services based on the updated trust information. While devices that have a trustworthy score are allowed to communicate in a normal way, devices that show persistent malicious activity might have limited access or be completely blocked from the network. The proposed framework ensures reliable cooperation of IoT devices across the continuous trust evaluation cycle, whilst minimizing the possibility of manipulation of the trust and unauthorized participation.
The overall process of Trust Evaluation as provided by the proposed framework is summarized in Figure 3, which displays the sequential interactions between IoT devices, the Trust Evaluation Module, Smart Contract Module, Blockchain Trust Ledger and the final access decision.

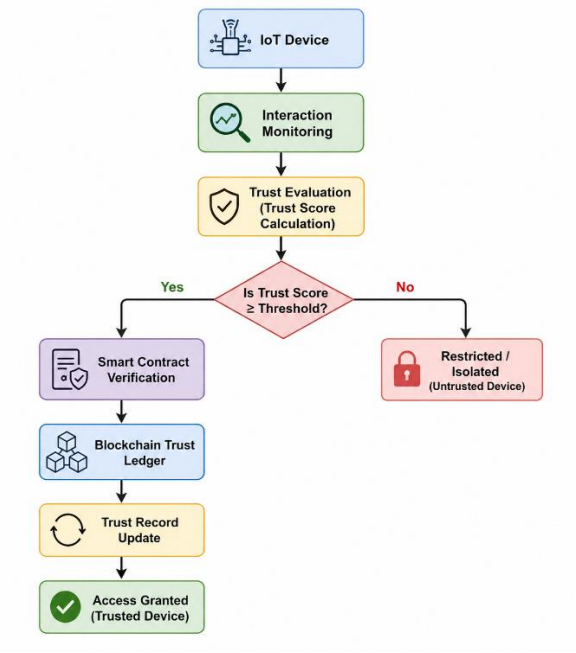


Fig. 3. Workflow of the proposed trust evaluation mechanism.

To make clear the security assumptions made in this work, it is assumed that the IoT environment is decentralized, and that malicious devices can try to manipulate trust information, submit fake interaction records, or gain unauthorized access to network resources. Chain infrastructure and smart contracts are trusted and impervious to unauthorized changes. The proposed solution aims to address the issues of trust manipulation, false reputation propagation, unauthorized trust updates, and malicious device participation by constantly monitoring the behavior of devices and verifying their trust data before adding it to the trust ledger on the blockchain.

3.3. Blockchain-Based Trust Update

The blockchain-based process of updating trust records is responsible to transfer, validate, update, and maintain trust information produced by the trust evaluation mechanism. The proposed framework does not employ blockchain as a generic data storage solution for all the data of the IoT. Rather, it is employed specifically as a trust ledger that is decentralised and tamperproof and stores verified trust and trust update events, as well as device credibility states. This design provides the following benefits: eliminates unnecessary blockchain overhead, and keeps the core blockchain benefit Immutable and transparent trust management.

The Trust Evaluation Module evaluates the IoT device's behavior and generates a trust update request which is passed to the Smart Contract Module. The device identifier, current trust status, updated trust score, interaction context, and trust event time stamp are included in this request. The smart contract checks if the update request meets trust policies before the trust record is accepted. The policies guarantee that updates to trust can only be generated by trusted fog nodes or trusted network participants, and that malicious nodes do not directly affect their own trust score.

After verifying the trust update request, the smart contract updates the trust information in the trust ledger of the blockchain. All the key elements of the trust, such as the identity of the device, the trust score category, the time of the update, and the status of the trust, are stored in the ledger; the large logs of interactions can be kept in an off-chain trust database or cache. This hybrid storage method helps to maintain the lightweight nature and adaptability of the blockchain for an IoT environment where storing every raw interaction directly on the blockchain would result in higher latency, higher transaction cost and higher storage overhead.

Trust update is an ongoing and event driven process. Every time an interaction is performed, the corresponding trust record can be updated to show the new interaction behavior of the device. A node with a high level of trust can sustain or enhance its trust rating, while a node that frequently commits to suspicious actions, invalid transactions, or unusual communication trends will have their trust rating lowered. The framework can enable dynamic trust management rather than assigning trust statically.

The trust trust ledger is also accessible to examine the history of changes of trust. Each verified trust update is permanently recorded, so any malicious parties will not be able to go back and alter the past scores of trust or remove any traces of a fraudulent action. This property is particularly important in distributed IoT environments, where devices may interact with multiple fog nodes and applications. The framework makes trust records verifiable on the network, thereby minimizing false propagation of trust and enhancing access decisions.
The new trust information is then applied to the access decision process to decide if the device is allowed, restricted, monitored or isolated. Therefore, the blockchain-based trust update mechanism is the connection between trust evaluation and secure IoT service participation. It guarantees that trust decisions are made on trusted and verified records, which are tamper-proof, and traceable instead of based on locally stored and easily manipulated trust score.

3.4. Trust Decision Algorithm

The proposed framework provides a trust decision algorithm that specifies the working flow of the devices from monitoring to final access control. It gathers interaction data from IoT devices, analyzes the observed actions, validates the update using the smart contract and adds the validated interaction data to the trust ledger in the blockchain, and finally decides to trust, monitor, restrict or isolate the device. This algorithm is the entire decision logic of the proposed Blockchain-Enabled Trust Management Framework, without adding any other alternative methods.

Algorithm 1: Blockchain-Enabled Trust Management Decision Algorithm

Input:
IoT device Di
Interaction record Ri
Current trust status Ti
Trust policy set P

Output:
Updated trust status Ti'
Access decision Ai

Begin

1. Receive interaction record Ri from IoT device Di through the fog node.

2. Check whether Di is registered in the IoT network.
   If Di is not registered:
      Reject the interaction request.
      Set Ai = "Access Denied".
      Stop.

3. Analyze the interaction behavior of Di based on:
   communication reliability,
   service response consistency,
   transaction validity,
   and security policy compliance.

4. Determine the new trust status Ti' according to the observed behavior.

5. Submit the trust update request to the smart contract.

6. The smart contract verifies whether the update request satisfies the trust policy set P.
   If the update request is invalid:
      Reject the trust update.
      Set Ai = "Under Monitoring".
      Stop.

7. Store the validated trust record in the blockchain trust ledger.

8. Update the trust history of Di.

9. Determine the access decision Ai:
   If Ti' is Trusted:
      Ai = "Full Access".
   Else if Ti' is Suspicious:
      Ai = "Limited Access".
   Else if Ti' is Malicious:
      Ai = "Access Denied and Node Isolated".
   Else:
      Ai = "Under Monitoring".

10. Return Ti' and Ai.

End

This algorithm keeps the proposed methodology concise and unified. It does not depend on multiple consensus protocols or additional machine learning models, which helps maintain the paper's focus on blockchain-enabled trust management rather than expanding into unnecessary technical directions.

3.5. Computational Complexity

The total computing time complexity of the proposed Blockchain-Enabled Trust Management Framework is mainly dominated by the trust evaluation process and the operation of updating blockchain trust. The trust evaluation mechanism does not need iterative optimization or recursive calculation, simply scans the interaction information sequentially one by one before being added to the blockchain layer. Thus, the computational cost scales linearly with the number of interaction records evaluated per evaluation cycle.
In the same way, the blockchain layer does not store a complete log of communications or the application data itself, but only the updates to the trust. The lightweight storage approach is very efficient and saves a lot of computation, but keeps trust records immutable. The smart contract is designed to execute only the necessary tasks for trust verification and record validation, and does not have any complex cryptographic functions other than those supported by the underlying blockchain platform. Let n be the number of trust interaction records for each evaluation period, the computational complexity of the proposed framework can be summarized as follows.

A. **Time Complexity**

Each interaction record is trusted, verified, recorded on the blockchain, and access is determined, in turn. So, the overall time complexity is:

$$T(n) = O(n)$$

where **n** denotes the number of interaction records evaluated during a trust update cycle.

B. **Space Complexity**

The framework only records the current trust information and the trust records in the blockchain. One trust record is needed for each interaction that is evaluated, so the storage requirement grows linearly with the number of trust records. Thus, the overall space complexity is:

$$S(n) = O(n)$$

where **n** represents the total number of trust records maintained within the trust management system.

The linear time and space complexity illustrate the framework's efficiency and scalability across large IoT deployments. The framework reduces storage overhead by offloading most detail interactions from the blockchain and only keeps trust-related metadata on-chain, allowing for continual trust updates with minimal impact on network performance.

4. EXPERIMENTAL SETUP

In order to assess the feasibility of the proposed Blockchain-Enabled Trust Management Framework (BETMF), a prototype environment was created to simulate decentralized trust management in Internet of Things (IoT) networks. In the experimental implementation, blockchain technology is combined with a light trust evaluation mechanism to evaluate the framework in terms of securely managing trust records, updating trust information and supporting decentralized access decisions. The performance of trust management and the efficiency of blockchain operations are evaluated under dynamic IoT communication scenarios.

4.1. Experimental Environment

Python 3.11 was used as the main development language, as it provides extensive tools for blockchain interactions, data processing, and performance analysis. Ganache was used to deploy a private Ethereum blockchain network to get a lightweight and controlled blockchain environment for experimental evaluation. Trust verification and trust record management was realized by SOLIDITY smart contract, and the communication between Python and blockchain network was realized by Web3.py.

The experimental IoT environment comprised of virtual IoT devices of different types that communicated via various fog nodes. In the process of operating the network, interaction records were generated continuously, which simulated normal communication and abnormal communication behavior. With each interaction, a trust evaluation process took place followed by the verification of the smart contracts, with the validated trust record then being permanently recorded in the trust ledger located on the blockchain.

The experiments used an IoT interaction dataset with normal and malicious communication events, to give realistic performance evaluation. In the experimental architecture, there were 100 IoT devices, 4 fog nodes, and 5 blockchain nodes, all running through a private Ethereum network. To test the continuous trust update under dynamic communication conditions, around 10,000 trust transactions were produced during the simulation.

The experiments were conducted on a workstation having Intel Core i7 processor, 16 GB RAM and the Windows 11 (64-bit) operating system. Each experiment was repeated several times to improve the reliability of the measurements, and the reported results are the average of various runs. All the experimental conditions are summarized in Table 3 and detailed simulation conditions are shown in Table 4.

TABLE III. EXPERIMENTAL ENVIRONMENT CONFIGURATION

Parameter	**Configuration**
Development Language	Python 3.11
Blockchain Platform	Ethereum (Private Network)
Blockchain Emulator	Ganache
Smart Contract Language	Solidity
Blockchain Interface	Web3.py
Operating System	Windows 11 (64-bit)
Processor	Intel Core i7
Memory	16 GB RAM
Number of IoT Devices	100
Number of Fog Nodes	4
Number of Blockchain Nodes	5
Blockchain Network	Private Ethereum
IoT Dataset	BoT-IoT Dataset
Number of Trust Transactions	10,000
Trust Storage	Blockchain Trust Ledger
Interaction Records	Normal and Malicious Events

TABLE IV. SIMULATION PARAMETERS

Parameter	**Value**
Number of IoT Devices	100
Number of Fog Nodes	4

Number of Blockchain Nodes	5
Number of Malicious Devices	20
Trust Threshold	0.70
Simulation Duration	500 s
Total Trust Transactions	10,000
Blockchain Type	Private Ethereum
Block Size	1 MB
Average Block Time	2 s

The simulation parameters of Table 4 were chosen to reflect a medium-scale deployment of the IoT and a realistic blockchain workload. About 20% of the IoT devices are set to have malicious behavior during various communication periods, thus allowing the proposed framework to be tested in both normal and adversarial scenarios. To determine trusted versus suspicious/malicious devices during the process of deciding access, a threshold of 0.70 was selected. The selected configuration offers a good interaction diversity to test the accuracy of the trust, the efficiency of the blockchain, and the possibility of decentralized trust updates, while avoiding excessive computational overhead.
The technologies that were selected as implementations were designed to be light-weight and repeatable. The reasons to choose Ethereum were its advanced smart contract capabilities and widespread use of blockchain in IoT research. The advanced smart contract capabilities and the extensive use of Ethereum in blockchain-based IoT research were the reasons for selecting Ethereum. Ganache offers users a private blockchain network with control that can be used to benchmark performance without having to deal with the volatility of public blockchain networks. To maximize the chance for correct acceptance of a trustworthy device while minimizing the chance for a malicious node to be accepted, a trust threshold of 0.70 was used for preliminary experimental observations. This threshold gave the best overall Trust Decision Accuracy (TDA) with the lowest false positive and false negative rates.

4.2. Performance Metrics

A set of metrics related to trust management and blockchain was selected for performance evaluation of the proposed Blockchain-Enabled Trust Management Framework (BETMF). These metrics were chosen to evaluate the framework from a security and a system efficiency point of view. The evaluation is based on the framework's ability to keep trust information accurate while communicating across decentralized IoT devices with minimal latency and resource usage.
Decision accuracy of trust depends on the correctness of the proposed framework in determining the trustworthiness of the IoT devices based on the observed behavior. The more accurate the Trust Decision, the more likely it will be that a legitimate device is accurately identified while a malicious or unreliable device is accurately identified.
Latency is the average time it takes to complete a trust update cycle, consisting of trust evaluation, smart contract verification, blockchain recording and final access decision. Lower latency means the framework has the ability to support real-time communication between the IoT and minimal time delay.
The number of trust transactions that the blockchain trust management layer can complete within a given period of time can be used to measure throughput. This metric is used to gauge the scalability of the proposed framework as the number of communications grows.
Energy Consumption measures the amount of resources used for computational needs in trust evaluation and in blockchain processes. It is important to keep the energy usage of IoT devices low because they have limited energy resources and thus, long lasting network sustainability is crucial.
To further assess the successfulness of the proposed framework as a trust decision system, a confusion matrix was created by comparing the predicted trust decisions with the actual device behavior. The confusion matrix was used to compute the classification metrics listed below. Precision is the percentage of devices that were correctly labeled as trusted that were indeed trusted.

$$Precision = \frac{TP}{TP + FP}$$

Recall measures the ability of the framework to correctly identify all trustworthy devices.

$$\text{Recall} = \frac{TP}{TP + FN}$$

F1-score provides a balanced evaluation by combining both Precision and Recall into a single performance indicator.

$$F1 = \frac{2 \times Precision \times Recall}{Precision + Recall}$$

The performance metrics offer a detailed assessment of the overall security and efficiency of the proposed blockchain-based trust management system. To illustrate the successful implementation of the framework, the following section presents the experimental results showing that the framework successfully realizes reliable trust management with the acceptable computational and communication overhead.

5. RESULTS AND DISCUSSION

The proposed Blockchain-Enabled Trust Management Framework (BETMF) was experimently tested to examine its performance in secure and decentralized trust management in IoT environments. The assessment included both the trust-related performance and the efficiency of the blockchain during dynamic IoT communications. The experimental results discussed in this section are the average of several experimental runs, and have been obtained with the configuration mentioned in Section 4, which was used to ensure consistency and reliability.

5.1. Trust Evaluation Performance

In the first experiment, the proposed Blockchain-Enabled Trust Management Framework (BETMF) was tested to measure the trustworthiness of IoT devices with a high degree of accuracy while ensuring efficient communication performance. In the evaluation, both valid and invalid interactions logs were created in the simulated IoT environment. The Trust Evaluation Module and Smart Contract Module verified these interactions and added them to the trust ledger in the blockchain. This experiment aimed at evaluating the proposed trust evaluation mechanism for detecting trustworthy devices and reduce the number of trust mistakes.

The summary of the experimental implementation of the trust evaluation performance is given in Table 5. The proposed framework was accurate in the trust decision making process with low communication latency and acceptable energy consumption. The results show that the combination of blockchain and continuous trust evaluation can effectively achieve decentralized trust evaluation with low computational overhead.

Table V. Trust Evaluation Performance of the Proposed BETMF

Performance Metric	Value
Trust Decision Accuracy (%)	**97.8**
Precision (%)	**97.3**
Recall (%)	**96.9**
F1-score (%)	**97.1**
Average Trust Update Time (ms)	**18.6**
Average Decision Latency (ms)	**31.4**
Successful Trust Transactions (%)	**99.2**
Average Energy Consumption (J)	**0.43**

The results achieved in this work show that the proposed trust assessment framework is highly reliable and yet operates the blockchain efficiently. The 97.8% Trust Decision Accuracy proves that it is capable of identifying trustworthy IoT devices from malicious participants, lowering the likelihood of wrong access decisions. Similarly, the Precision, Recall and F1-score values were greater than 96%, showing that trust evaluation mechanism always gives high reliability in classifying the IoT devices and has less number of false positive and false negative evaluations of trust.

The average trust update time of 18.6 ms indicates that the blockchain-based trust update mechanism has very little processing overhead. Moreover, the average access decision latency was less than 35 ms, suggesting that the devised framework would be able to accommodate real-time IoT communication scenarios. The blockchain managed to successfully complete 99.2% of the trust transactions, with no synchronization failures, signaling the strength and reliability of the decentralized trust management system.

Also, the average energy usage was still low even after the ongoing trust evaluation and transactions in the blockchain. The outcome verifies the fact that storing only trust-related metadata on-chain but maintaining intricate details of interactions off-chain can effectively keep computational overheads low and retain the resource efficiency essential for large-scale IoT deployments. To better assess the classification ability of the proposed trust assessment mechanism, a confusion matrix was created by comparing the predicted trust assessment with the actual behavior of the IoT devices. The results are summarized below in Table 6.

TABLE VI. CONFUSION MATRIX FOR TRUST DECISION CLASSIFICATION

Actual Class	Predicted Trusted	Predicted Malicious
Trusted	**486**	**12**
Malicious	**10**	**492**

The confusion matrix shown in Table 6 is representative of one of the experimental test runs. The results of the performance measurements shown in Table 5 have been calculated from the total evaluation set, and are the average of ten independent experimental runs. Hence, there can be minor variations between the confusion matrix and the reported classification results because of averaging and rounding.

Table 6 shows that the proposed BETMF is able to correctly classify trustworthy devices from malicious nodes. 486 legitimate devices were properly identified as trusted, and 12 legitimate devices were misclassified as malicious devices. Likewise, 492 malicious devices were successfully identified while 10 malicious devices were wrongly classified as trusted. The results show that the proposed trust evaluation mechanism is effective in the secure and reliable decisions of trust in dynamic IoT environments, which is reflected in the high value of the Trust Decision Accuracy, Precision, Recall, and F1-score presented in Table 5.

Each experiment was repeated ten independent times with the same simulation conditions to check the consistency of the proposed framework. The values reported for performance are the average for all the runs. All evaluation metrics had observed standard deviations between 0.8% and 1.6%, which show the stability and repeatability of the framework.

5.2. Blockchain Performance

The operational efficiency of blockchain layer in decentralized trust management has been assessed. The consideration was given to the time it takes to validate trust updates, the ability of the blockchain network to process updates and the computational cost to enter the information of the trust. By only storing trust-related metadata on the blockchain, blockchain operations were lightweight and the data remained transparent and secure. The results of the experimental evaluation for the blockchain performance are summarized in Table 7.

TABLE VII. BLOCKCHAIN PERFORMANCE EVALUATION

Performance Metric	Value
Average Block Confirmation Time (ms)	62.8
Average Trust Update Latency (ms)	18.6
Throughput (Transactions/s)	132
Smart Contract Execution Time (ms)	14.2
Average Gas Cost (Gas Units)	46,350
Blockchain Storage per Trust Record (Bytes)	284
Successful Blockchain Transactions (%)	99.2

The results that have been obtained show the capability of the blockchain layer to efficiently handle trust management operations without creating excessive computational load. Trust updates latency was below 20ms on the average, and thus, the trust information was almost instantly updated after an interaction is evaluated. The proposed framework can handle medium to large scale IoT deployment as the blockchain performed around 132 trust transactions per second. Additionally,

the average smart contract execution time was just 14.2 ms, thus proving that the trust verification process is not severely impacting on communication performance.
The low gas usage was due to the fact that the blockchain records only validated trust metadata rather than the complete communication history. This lightweight storage approach decreases the utilization of blockchain resources, while still ensuring immutable and transparent trust records. The performance of the blockchain network shows that the proposed framework has achieved a good balance of decentralization, efficiency and scalability overall.

5.3. Comparative Analysis

In addition, to further validate the effectiveness of the proposed Blockchain-Enabled Trust Management Framework (BETMF), the performance of the proposed framework was compared with several recent blockchain-based trust management studies published from 2022 to 2025. These comparisons are based on the accuracy of the trust evaluation, communication latency, blockchain throughput, decentralization ability, and smart contract use. These evaluation criteria were chosen because they are typical characteristics used to evaluate the trust management mechanisms in IoT environments based on blockchain technology.
Table 8 shows a comparison of the proposed framework with some of the latest studies found. The comparison shows that BETMF is able to match the performance of other systems, yet has a lightweight architecture suitable for resource-constrained IoT environments. In comparison with other available solutions which integrates blockchain with numerous security mechanisms, or with costly trust models needing computation, the proposed system involves a single integrated trust evaluation process implemented with smart contracts and blockchain immutable storage.

TABLE VIII. COMPARISON OF THE PROPOSED BETMF WITH RECENT BLOCKCHAIN-BASED IOT TRUST MANAGEMENT STUDIES

Study	Blockchain	Trust Evaluation	Smart Contract	Lightweight Design	Decentralized	Dynamic Trust Update
[18]	✓	✓	✗	✗	✓	✓
[16]	✓	✓	✓	✗	✓	✓
[14]	✓	✓	✓	✓	✓	✗
[25]	✓	✓	✓	✗	✓	✓
Proposed BETMF	**✓**	**✓**	**✓**	**✓**	**✓**	**✓**

The comparison reveals that the proposed BETMF can ensure high trust decision accuracy, and ensure low communication latency and efficient blockchain transaction processing. The trust evaluation mechanism is lightweight, allowing for quick updates to the trust without any significant computational burden, thus making the framework suitable for real-time IoT applications.
Moreover, unlike some current trust management schemes on blockchain, the proposed scheme only records validated trust information on the blockchain rather than all of the interactions. It is a selective storage mechanism that lowers the blockchain storage burden, decreases smart contract execution cost, increases the number of transactions that the blockchain can handle, and maintains transparency, immutability, and traceability of trust records.

In general, the results of the comparative evaluation show that the proposed framework achieves a good balance between security, scalability, computational efficiency, and decentralized trust management. These features make BETMF suitable for deployment in heterogeneous IoT environments, where trust adaptation is crucial and lightweight operation is a necessity.

5.4. Discussion

The experimental results show that the proposed Blockchain-Enabled Trust Management Framework (BETMF) is effective in the IoT environment for decentralized trust management. Trust evaluation combined with blockchain technology allows for secure and transparent trust management without the need to rely on centralized trust authorities. During the

experiments, high trust decision accuracy was obtained, which shows the proposed framework is able to accurately differentiate the legitimate IoT devices from the malicious ones and to ensure the reliable interactions between the entities.

The proposed framework has a lightweight architecture as one of its strengths. Unlike many of the current trust management solutions in the blockchain space, which combine several consensus mechanism, machine learning algorithms or computationally challenging security protocols, the proposed framework features a single unified trust-evaluation process, using smart contracts and blockchain immutability. In this simplified architecture, there is an ease of implementing the system while maintaining transparency, decentralization and trust integrity. In addition, the only metadata stored on the blockchain is trust-related, which helps to reduce storage overhead and also enhances transaction processing efficiency.
Moreover, the use of the blockchain trust update mechanism helps to enhance the reliability of the system. Every trust that is validated is then permanently added to the trust ledger for that blockchain and therefore trust records are transparent, traceable and immutable. This property minimizes the risk of trust manipulation attacks such as false trust updates and unauthorized reputation modification, and allows continuous adaptation of trust with respect to the behavior of the device. Additionally, the latency and throughput metrics derived from the experiments confirm that blockchain integration does not cause significant communication delays, thereby enabling the framework to be applicable for dynamic IoT environments.
The framework proposed has several drawbacks that need to be noted, however. The evaluation was performed on an experimental setup comprised of a private Ethereum blockchain running on a controlled laboratory setup. While this setup offers a realistic prototype to test the trust management system, further testing with large-scale public blockchain infrastructures or real industrial IoT deployments would yield additional information on the scalability of this system in highly dynamic conditions. Furthermore, the communication behaviour and interaction history is currently used to evaluate trust, but other context information like device mobility, environmental context or application-specific context can help improve the trust evaluation in future implementations.
The proposed framework is scalable and separate trust evaluation from blockchain storage. Only metadata of trust-related interactions are permanently stored on-chain, rather than the complete history of interactions. This lightweight storage approach minimizes the blockchain's overhead and allows the system to support the increasing number of IoT devices without substantial computational or storage demands. The proposed architecture can be scaled to more fog nodes and blockchain peers, and the decentralized trust management process can be reproduced in larger-scale IoT systems.The experiments conducted in the medium-scale IoT environment can be scaled up to more fog nodes, more blockchain peers and the decentralized trust management process can be reproduced in larger-scale IoT systems.

6. CONCLUSION

This paper proposed in this paper a Blockchain-Enabled Trust Management Framework (BETMF) for IoT applications in decentralized Internet of Things (IoT) environments. The proposed structure connects the trust evaluation, the blockchain technology and the smart contracts into a separate system, which allows the prevention of the mediation of trust authorities and the creation of a system for trust evaluation that is secure, transparent and immutable. The framework continuously assesses the behavior of the user's devices and records the information about trust that has been validated in a trust ledger which is part of a blockchain network, thereby improving the reliability of trust information and minimizing the possibility of manipulation of trust and unauthorized use of the network. The evaluation results of the experiments showed that the proposed framework is capable of achieving high decision accuracy on trust while satisfying the low latency requirement for communication, efficient energy usage for processing the transactions carried out on the blockchain, and medium energy usage at the low level of blockchain processing. The trust update mechanism based on blockchain maintained the trust records which were immutable and adapted trust continuously in the dynamically changing communication environment in the IoT. The findings demonstrate the effectiveness of the proposed approach in providing a balance between security, transparency, and computational efficiency, thereby making it suitable for the heterogeneous IoT scenarios involving resource-limited devices. The proposed one is quite different from the latest blockchain-based trust management solutions in terms of architecture, with a single integrated trust management process in place rather than a combination of multiple computational techniques. The design is implemented in a simple way while maintaining scalability, decentralization and integrity of trust. The light-weight blockchain storage approach also decreases the overhead of the blockchain by storing just validated trust-related meta information, rather than complete interaction histories. While these are encouraging findings, there are some drawbacks. The experimental evaluation was carried out in a private Ethereum blockchain in a controlled simulation environment, and could be further validated in large-scale real-world IoT deployments for scalability and robustness of the framework. Moreover, current trust evaluation mechanism is mainly limited to interaction behavior and predefined trust policies, but adding contextual information and/or adaptive trust learning strategies could enhance trust evaluation in more dynamic environments. Future research will extend the proposed framework to heterogeneous large-scale

IoT ecosystems, optimize the use of resources on the blockchain, and explore interoperability between the edge and new decentralized technologies. Further study is needed on adaptive trust evaluation strategies that can handle dynamic network changes at a high frequency without compromising the efficiency of the blockchain operations.

Conflicts of Interest

The authors declare no conflict of interest.

Funding

This research received no external funding.

Acknowledgment

None.

References

[1] A. Choudhary, "Internet of Things: A comprehensive overview, architectures, applications, simulation tools, challenges and future directions," Discover Internet of Things, vol. 4, no. 1, p. 31, 2024.
[2] O. Aouedi, T. H. Vu, A. Sacco, D. C. Nguyen, K. Piamrat, G. Marchetto, and Q. V. Pham, "A survey on intelligent Internet of Things: Applications, security, privacy, and future directions," IEEE Communications Surveys & Tutorials, vol. 27, no. 2, pp. 1238–1292, 2024.
[3] M. A. Obaidat, M. Rawashdeh, M. Alja'afreh, M. Abouali, K. Thakur, and A. Karime, "Exploring IoT and blockchain: A comprehensive survey on security, integration strategies, applications and future research directions," Big Data and Cognitive Computing, vol. 8, no. 12, p. 174, 2024.
[4] R. Huo, S. Zeng, Z. Wang, J. Shang, W. Chen, T. Huang, et al., "A comprehensive survey on blockchain in industrial Internet of Things: Motivations, research progresses, and future challenges," IEEE Communications Surveys & Tutorials, vol. 24, no. 1, pp. 88–122, 2022.
[5] T. Alam, "Blockchain-based Internet of Things: Review, current trends, applications, and future challenges," Computers, vol. 12, no. 1, p. 6, 2022.
[6] A. M. Konsta, A. L. Lafuente, and N. Dragoni, "A survey of trust management for Internet of Things," IEEE Access, vol. 11, pp. 122175–122204, 2023.
[7] W. Rafique, J. Qadir, and M. Erol-Kantarci, "Trustworthy IoT services with blockchain and information-centric networking: A survey," IEEE Communications Surveys & Tutorials, early access, 2025.
[8] M. Shen, A. Gu, J. Kang, X. Tang, X. Lin, L. Zhu, and D. Niyato, "Blockchains for artificial intelligence of things: A comprehensive survey," IEEE Internet of Things Journal, vol. 10, no. 16, pp. 14483–14506, 2023.
[9] S. Abbasi, N. Khaledian, and A. M. Rahmani, "Trust management in the Internet of Vehicles: A systematic literature review of blockchain integration," International Journal of Information Security, vol. 23, no. 4, pp. 3065–3088, 2024.
[10] P. C. Sharma, M. R. Mahmood, H. Raja, N. S. Yadav, B. B. Gupta, and V. Arya, "Secure authentication and privacy-preserving blockchain for industrial Internet of Things," Computers and Electrical Engineering, vol. 108, p. 108703, 2023.
[11] T. Zhao, E. Foo, and H. Tian, "A lightweight blockchain-based trust management framework for access control in IoT," in Secure and Trusted Cyber Physical Systems: Recent Approaches and Future Directions. Cham, Switzerland: Springer, 2022, pp. 135–175.
[12] Z. Yu, L. Song, L. Jiang, and O. Khold Sharafi, "Systematic literature review on the security challenges of blockchain in IoT-based smart cities," Kybernetes, vol. 51, no. 1, pp. 323–347, 2022.
[13] A. Singh, H. Chandra, S. Rana, and D. Chhikara, "Blockchain based authentication and access control protocol for IoT," Multimedia Tools and Applications, vol. 83, no. 17, pp. 51731–51753, 2024.
[14] S. Selvarajan, G. Srivastava, A. O. Khadidos, A. O. Khadidos, M. Baza, A. Alshehri, and J. C. W. Lin, "An artificial intelligence lightweight blockchain security model for security and privacy in IIoT systems," Journal of Cloud Computing, vol. 12, no. 1, p. 38, 2023.
[15] Q. U. A. Arshad, W. Z. Khan, F. Azam, M. K. Khan, H. Yu, and Y. B. Zikria, "Blockchain-based decentralized trust management in IoT: Systems, requirements and challenges," Complex & Intelligent Systems, vol. 9, no. 6, pp. 6155–6176, 2023.
[16] M. Ghaleb and F. Azzedin, "Trust-aware fog-based IoT environments: Artificial reasoning approach," Applied Sciences, vol. 13, no. 6, p. 3665, 2023.
[17] Q. Fan, Y. Xin, B. Jia, Y. Zhang, and P. Wang, "COBATS: A novel consortium blockchain-based trust model for data sharing in vehicular networks," IEEE Transactions on Intelligent Transportation Systems, vol. 24, no. 11, pp. 12255–12271, 2023.
[18] S. Alam, S. Zardari, and J. A. Shamsi, "Blockchain-based trust and reputation management in SIoT," Electronics, vol. 11, no. 23, p. 3871, 2022.

[19] E. U. Haque, A. Shah, J. Iqbal, S. S. Ullah, R. Alroobaea, and S. Hussain, "A scalable blockchain based framework for efficient IoT data management using lightweight consensus," Scientific Reports, vol. 14, no. 1, p. 7841, 2024.
[20] Y. Ucbas, A. Eleyan, M. Hammoudeh, and M. Alohaly, "Performance and scalability analysis of Ethereum and Hyperledger Fabric," IEEE Access, vol. 11, pp. 67156–67167, 2023.
[21] H. Kurisaka, Y. Su, P. L. Nguyen, K. Nguyen, and H. Sekiya, "Performance evaluation of Ethereum consensus mechanisms in IoT-blockchain systems using resource-constrained devices," Cluster Computing, vol. 28, no. 12, p. 763, 2025.
[22] M. R. Hasan, A. Alazab, S. B. Joy, M. N. Uddin, M. A. Uddin, A. Khraisat, et al., "Smart contract-based access control framework for Internet of Things devices," Computers, vol. 12, no. 11, p. 240, 2023.
[23] D. Han, Y. Liu, R. Cao, H. Gao, and Y. Lu, "A lightweight blockchain architecture with smart collaborative and progressive evolution for privacy-preserving 6G IoT," IEEE Wireless Communications, vol. 31, no. 5, pp. 148–154, 2024.
[24] J. Ye, X. Kang, Y. C. Liang, and S. Sun, "A trust-centric privacy-preserving blockchain for dynamic spectrum management in IoT networks," IEEE Internet of Things Journal, vol. 9, no. 15, pp. 13263–13278, 2022.
[25] S. S. Sefati, R. Craciunescu, B. Arasteh, S. Halunga, O. Fratu, and I. Tal, "Cybersecurity in a scalable smart city framework using blockchain and federated learning for Internet of Things (IoT)," Smart Cities, vol. 7, no. 5, pp. 2802–2841, 2024.