*electronics*

MDPI

*Article*

# Decentralized Multi-Layered Architecture to Strengthen the Security in the Internet of Things Environment Using Blockchain Technology

**Ahmed Alhusayni [1,*], Vijey Thayananthan [2], Aiiad Albeshri [2] and Saleh Alghamdi [2]**

[1] Department of Computer Science, Umm Al-Qura University, Makkah 21421, Saudi Arabia
[2] Department of Computer Sdcience, FCIT, King Abdulaziz University, Jeddah 21589, Saudi Arabia; vthayanathan@kau.edu.sa (V.T.); aaalbeshri@kau.edu.sa (A.A.); salehg@outlook.sa (S.A.)
* Correspondence: aehusayni@uqu.edu.sa

**Abstract:** Smart devices are connected to IoT networks and the security risks are substantial. Using blockchain technology, which is decentralized and distributed, 5G-enabled IoT networks might be able to tackle security issues. In order to simplify the implementation and security of IoT networks, we propose a multi-level blockchain security model. As part of the multi-level architecture, the communication between levels is facilitated by clustering. IoT networks define unknown clusters with applications that utilize the evolutionary computation method coupled with anatomy simulation and genetic methodologies. Authentication and authorization are performed locally by the super node. The super node and relevant base stations can communicate using local private blockchain implementations. A blockchain improves security and enhances trustworthiness by providing network authentication and credibility assurance. The proposed model is developed using the open-source Hyperledger Fabric blockchain platform. Stations communicate securely using a global blockchain. Compared to the earlier reported clustering algorithms, simulations demonstrate the efficacy of the proposed algorithm. In comparison with the global blockchain, the lightweight blockchain is more suitable for balancing network throughput and latency.

**Keywords:** blockchain; dynamic consensus control algorithm; IoT; distributed data management; security



**Citation:** Alhusayni, A.; Thayananthan, V.; Albeshri, A.; Alghamdi, S. Decentralized Multi-Layered Architecture to Strengthen the Security in the Internet of Things Environment Using Blockchain Technology. *Electronics* **2023**, *12*, 4314. https://doi.org/10.3390/electronics12204314

Academic Editors: Myung-Sup Kim and Andrei Kelarev

Received: 31 August 2023
Revised: 4 October 2023
Accepted: 16 October 2023
Published: 18 October 2023



## 1. Introduction

Centralized networks can host ubiquitous interconnected objects using Internet of Things (IoT) platforms [1]. It is also possible to implement decentralized peer-to-peer solutions using blockchain technology [2], including smart homes and connected cars. However, both models have limitations regarding their ability to provide privacy and security due to limited resources, centralization management, and scalability, cost, and response time. The diversity of IoT network nodes is expected to result in different throughputs and rates [3]. Centralized networks control and improve the performance of a large number of IoT devices [4,5]. However, centralizing systems suffer from a number of disadvantages. A third party often has to manipulate the data collected by central cloud storage, which could lead to information leaks that could compromise the user's privacy [6]. As a result, many current centralized systems do not adequately protect the confidentiality and reliability of data. Because IoT gadgets have low-power wireless transmissions and recipients, they are able to only communicate over short distances. Taking advantage of multi-hop cellular networking (MCN) [7] can help accelerate the shortening of signal coverage in IoT networks.

The advent of IoT-enabled 5G networks introduces a multitude of complex challenges, encompassing the vast number of interconnected devices, the diversity of device types, the imperative for low communication latency, and the paramount issue of trust [8]. The

integration of device-to-device (D2D) and IoT platforms within the 5G framework necessitates a novel security model tailored to address their distinct requirements. These needs encompass scalability, minimal latency, energy efficiency, and robust secure communication protocols. Blockchain technology has long been recognized as a pivotal tool for fortifying security in various domains. In the context of IoT and 5G networks, blockchain holds the potential to usher in significant security enhancements. It does so by serving as a foundational pillar for ensuring the integrity and confidentiality of data exchanges among interconnected devices.

Additionally, blockchain can play a vital role in enabling massive machine-type communication (mMTC), a critical component of 5G networks. This functionality can substantially elevate IoT privacy and security within the broader 5G ecosystem. The importance of bolstering IoT security cannot be overstated, particularly within the realm of 5G-enabled networks. These networks are poised to underpin the connectivity of an unprecedented number of devices across diverse applications, spanning smart cities, healthcare, industrial automation, and more. The sheer scale and heterogeneity of these networks necessitate robust security measures to safeguard sensitive data, ensure reliable operation, and protect against malicious threats. Furthermore, the integration of 5G into critical infrastructure and mission-critical applications underscores the urgency of addressing security concerns. Failures in security could have far-reaching consequences, making it imperative to develop and implement advanced security models such as blockchain technology. In doing so, we can fortify the foundation of trust within the IoT landscape, ensuring the smooth and secure operation of 5G-enabled networks for the benefit of society as a whole.

This paper presents a multi-level architecture that would make it easier to implement IoT communication security, an innovative blockchain implementation model based on clustering. As a multi-level distributed blockchain network, this new model combines blockchain technology and clustering techniques to improve IoT security and reliability by effectively leveraging network clustering performance and capabilities. The performance metrics for network-based cost functions were used to develop an optimized clustering algorithm for IoT systems. Multi-hop cellular networks (MCNs) can help reduce network load, improve the scope, and reduce the power consumption in IoT networks. Compromised entities across multiple levels can be detected. Participants in the system verify each transaction using a consensus algorithm. The blockchain ledger is continuously updated as each participant maintains a copy of the blockchain. Therefore, the multi-level blockchain prevents compromised entities from participating in the system. This prevents the integrity of the blockchain from being compromised. One important aspect of the new architecture permits upgrades for the current centralized cloud service. This will enable extensive deployments. In addition, each cluster uses a lightweight authorization and authentication process to ensure secure network access.

*Research Contribution*

The key contributions of the proposed work are as follows:

- In this research, a hybrid local–global consensus protocol is proposed inside a blockchain model that is more reliable and provides a more secure structure to IoT devices.
- To develop a more refined graph-based clustering mechanism that clusters similar IoT devices in a better way than traditional clustering algorithms.
- The utilization of a hybrid consensus based on Pure Proof-of-Stake (Pure PoS) and Byzantine fault tolerance (BFT) at local level inside clusters. A hybrid consensus based on Proof of Power (PoP) and Delegated Proof of Stake (DPoS) significantly reduces the burden on the local leader node, allowing for a more even distribution of duties.
- In order to fully assess the efficacy of our proposed research, we compared the proposed technique by conducting numerous experiments. The empirical findings demonstrate that the performance of the proposed work surpasses the existing competing methods by a significant margin.

This paper has the following sections: Section 2 discusses IoT and blockchain security, followed by a literature review of IoT integration with blockchain. The multi-level framework and unique features are discussed in Section 3. Section 4 contains an implementation and validation method for our IoT blockchain framework. A description of the difficulties involved in implementing the suggested system model is found in Section 5. The last part of this paper concludes by highlighting future research directions.

## 2. Background

Contemporary IoT systems are marked by heightened connectivity, leading to an increased volume of data generated by interconnected devices. Consequently, the proliferation of data in IoT ecosystems gives rise to pressing concerns related to security and privacy. Due to their constrained memory capacities and limited computing capabilities, IoT devices not only grapple with significant security vulnerabilities, but also face challenges concerning data processing and communication, as highlighted in prior research [5].

### *2.1. IoT Authentication and Authorization*

The term "Internet of Things" refers to the connectivity of "smart" devices, including digital and mechanical machinery, goods, and people. These "smart" gadgets are able to exchange data via a network without the involvement of a human being. The typical Internet of Things system is depicted in Figure 1. Applications of the Internet of Things on a larger scale include, among other things, smart cities, smart homes, and smart healthcare systems. The typical IoT system is composed of: (i) IoT sensors and devices such as smart vehicles, smart electronics equipment, and smart home appliances. (ii) Networks, communication protocols, and 4G and 5G technologies. (iii) Communication and processing protocols (iv) Storage resources such as the cloud.

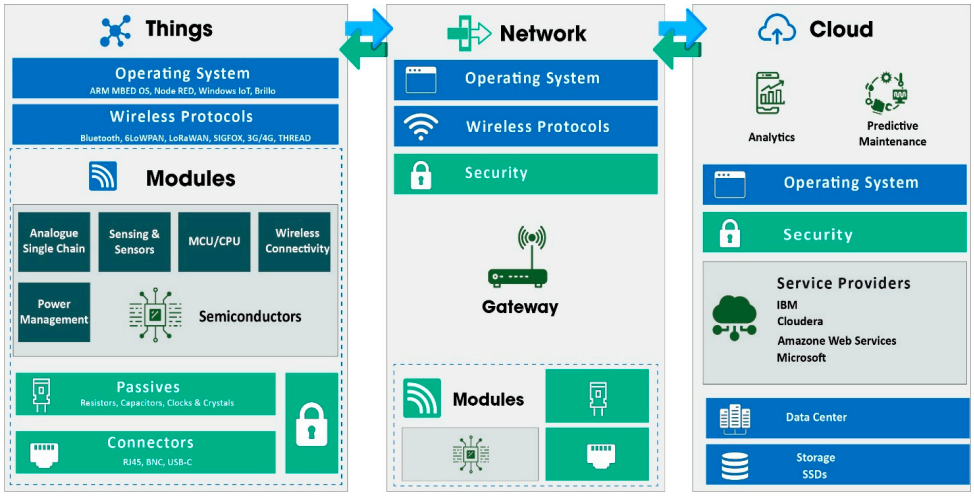


**Figure 1.** The IoT architecture and its distribution.

To access IoT applications, devices must be authenticated and authorized. In terms of network security, these measures are crucial [9]. A relevant authentication procedure is needed for establishing secure communication between IoT devices. An IoT network typically uses public key infrastructure to control the authentication and authorization of devices and nodes [10]. The high volume of requests greatly exacerbates the authority center's workload, resulting in considerable delays [11]. Several new mechanisms have been suggested to improve this situation. Ref. [12] proposes a method for authentication and privacy using IP-Sec with TLS. Nonetheless, due to its high computing requirements, such a mechanism is inefficient for connected devices with limited computational resources.

IoT researchers [13] found a way to provide an access management system based on blockchain technology. A Proof of Concept (PoC) algorithm is a consensus-based method

implemented instead of a centralized management server in the suggested approach. By utilizing Ethereum blockchain technology to verify the entity's identity [14], it presents IoT controlling access in a secure manner that addresses issues of delegating access rights. In a previous paper [15], blockchain structures (BCS) are proposed as IoT verification methods using layers, intersections, and self-organization. Security performance is assessed based on the efficiency of storage, responsiveness, and validity. Based on the blockchain, ref. [16] proposes an IoT security and authentication method. By using this method, single points of failure can be avoided.

### *2.2. The Blockchain and IoT Environment*

In 2008, a well-known crypto currency called Bitcoin developed and utilized blockchain technology for the first time [17]. It is a decentralized ledger technology with a peer-to-peer networking foundation. Figure 2 depicts the workings of a typical blockchain paradigm. In this approach, each node in the blockchain network updates its copy of the ledger. The Internet of Things (IoT) devices can be made more secure, private, and reliable by using blockchain technology for encrypted communication.

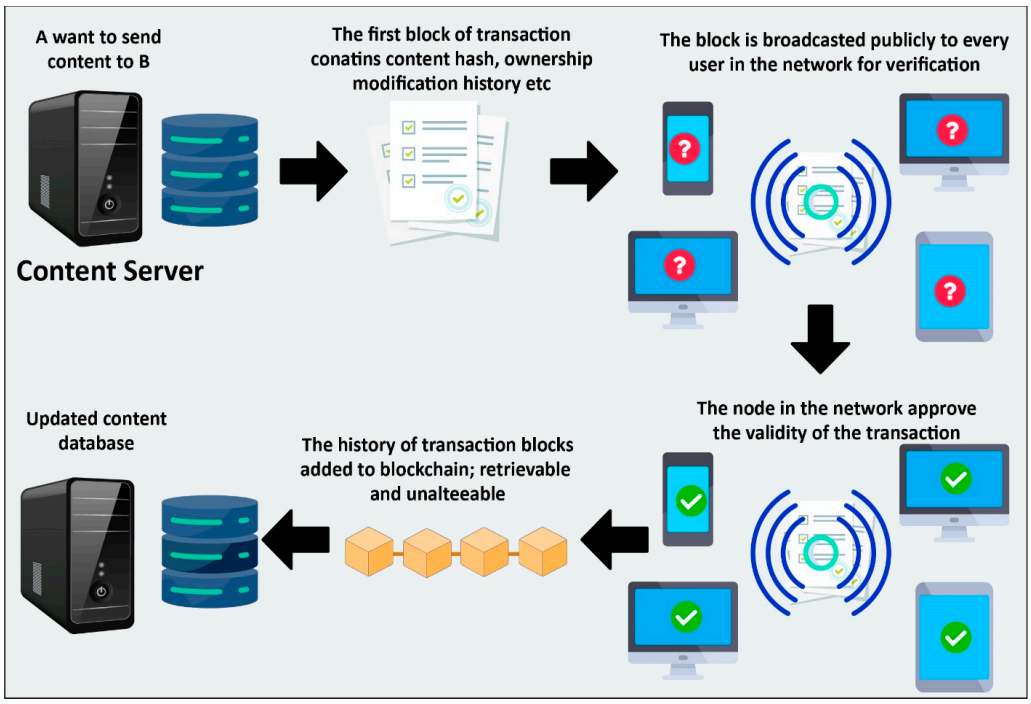


**Figure 2.** The working mechanism of a typical blockchain.

Conventional centralized systems rely on a single point of control and are hence open to attacks. On the other hand, blockchain is decentralized, meaning no organization has complete authority over the network. Lowering the single points of failure and potential attack routes can improve the security of IoT connectivity. Blockchain also offers an unchangeable, tamper-proof ledger in which data can be safely recorded. As seen in Figure 3, a chain of blocks that is impossible to tamper with without being noticed is created by connecting each data block to the one before it using cryptographic hashes. This guarantees the accuracy of the data transmitted between IoT devices.

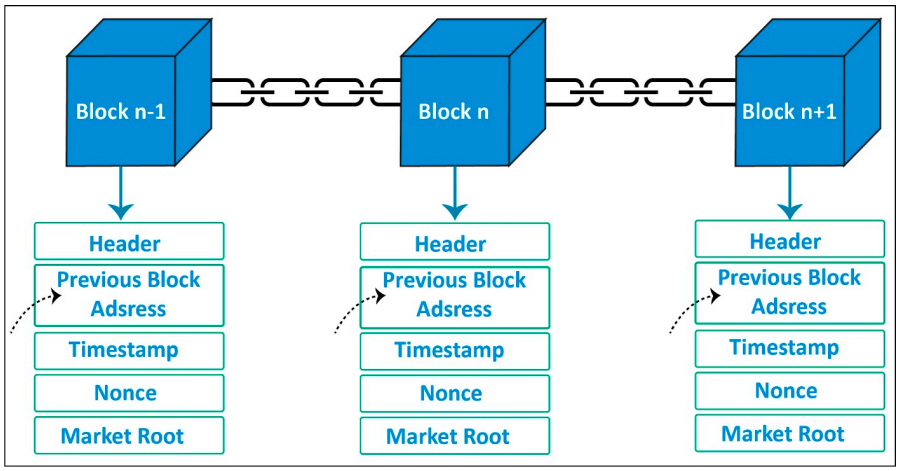


**Figure 3.** Data connectivity via chain of blocks inside blockchain.

Blockchain-based identity and authentication management allow for secure device authentication. Each IoT device can have a distinct digital identity that is kept on the blockchain and can be used to confirm the validity of the device and its data. The conditions of the agreement are explicitly contained in the smart contract's code, which is a self-executing contract. Smart contracts can be applied to the Internet of Things to automate processes based on predetermined criteria. To ensure secure and predictable behavior, a smart contract can specify, for instance, that a particular action carried out by an IoT device should only be conducted if certain criteria are met. Thanks to the secure data sharing, multiple parties can share data in a regulated, secure manner. The risk of data breaches and illegal access is decreased since IoT devices can share data directly with authorized parties without the use of middlemen.

### *2.3. Secure IoT Frameworks Based on Blockchain*

A new method of addressing privacy and security challenges associated with the IoT has been developed using blockchain; [18] presents several strategies for preserving privacy within blockchain-based IoT systems. Several strategies to implement differential privacy include encryption, anonymization, private contracts, and mixing.

Study [19] looks at blockchain and IoT applications and discusses how the technology can address security concerns. Figure 4 shows the secure IoT framework with blockchain implementation, as the IoT is challenged by insufficient standardization, the limited capacity of cloud servers, low manipulation potential, and costs [4]. As a way to facilitate IoT device privacy and security, lightweight scalable blockchain is described in [20]. By implementing a blockchain with robust computing performance, decentralization and privacy protection are achieved due to the implementation of an overlay network. IoT networks and blockchain should be integrated to address their challenges [21]. A redesigned consensus mechanism called Proof of Block and Trade is proposed. It aims to speed up the validation of trades and blocks by reducing computation time. An IoT device's memory requirements are reduced by developing a distributed ledger. The authors of [3] propose a blockchain-based model that uses lightweight scalable blockchain (LSB) to modify the consensus algorithm, reducing the deployment complexity of Proof of Work. Ref. [22] explains how blockchain-based frameworks can be utilized to address problems such as confidentiality, trust, resilience, and autonomy. Blockchain implementation can be assessed using an IoT and edge computing decision structure with the framework. Ref. [23] proposes a context-sensitive data allocation mechanism for blockchain-enabled IoT systems. For each data request, the authors compute the rating of allocation (RoA) score using a fuzzy logic mechanism. This paper investigates the efficiency of blockchain systems and fog architectures.

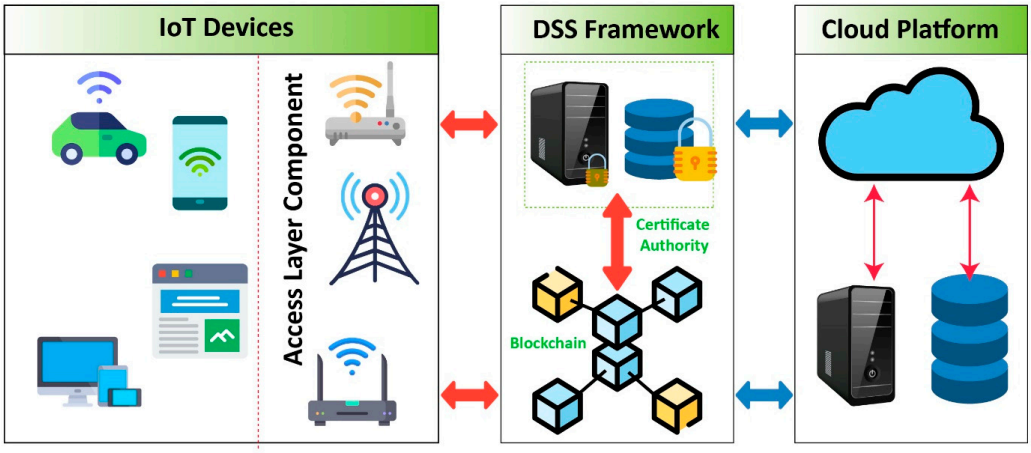


**Figure 4.** Secure IoT framework with blockchain implementation.

### *2.4. Blockchain Security Model for 5G-Enabled IoT Networks*

In [24], a blockchain-based solution for automated certificate revocation in 5G IoT networks is proposed. The system utilizes blockchain technology to ensure the security and privacy of IoT devices and data by providing a reliable and efficient certificate revocation mechanism. The proposed system uses smart contracts and consensus mechanisms to automate the certificate revocation process and maintain the system's integrity.

A blockchain-based remote data integrity checking scheme (RDIC) for IoT devices in 5G networks is proposed in [25]. The proposed scheme utilizes a blockchain to maintain the integrity of the data collected by IoT devices in the network. The system employs a challenge–response protocol and smart contracts to automate the data checking process and ensure the authenticity of the data. The proposed scheme addresses the security and privacy issues associated with data collection and sharing in IoT networks. Another paper proposes a blockchain-based data dissemination scheme for 5G-enabled softwarized UAV networks [26]. The proposed scheme utilizes blockchain technology to provide secure and reliable data dissemination between UAVs and other entities in the network. The system employs a consensus mechanism and smart contracts to automate the data dissemination process and maintain the integrity of the system. The proposed scheme is designed to address the security and privacy issues associated with data dissemination in UAV networks.

### *2.5. Permissioned Blockchain in IoT*

It is possible to achieve the benefits of a trust-free environment, which is also flexible, scalable, and confidential, without the need for centralized authority through the use of Hyperledger Fabric (HLF) [27]. Hyperledger Fabric is an open-source blockchain platform developed by the Linux Foundation. It provides a modular and highly flexible framework for building permissioned blockchain networks, making it suitable for various enterprise applications. Hyperledger Fabric offers features like confidentiality, scalability, and flexibility in terms of consensus algorithms and smart contract languages. It is designed to support consortium networks where multiple organizations collaborate while preserving data privacy and security. In the HLF framework, consensus algorithms are open architectures. This allows you to modify the configuration and increase performance. An authorization framework based on the HLF framework is proposed in [28] for an IoT network. There is some consideration of IoT-driven data collection and its standard features in [29]. In order to address the management issues of big data generated by the IoT, this research proposes the management of big data on a blockchain through a permissioned, decentralized trust management protocol (BlockBDM).

### 2.6. Level-Based IoT Blockchain

According to [17], a platform is proposed to make smart city communication more secure using blockchain. An IoT and blockchain especially suited for medical use have been proposed in paper [30]. With decentralized multi-layer IoT networks, the solution solves the computation and complexity challenges associated with blockchain implementation. To implement the smart city, a blockchain and SDN-based hybrid network architecture is proposed in [31]. A core network and edge network are proposed as parts of the proposed architecture to improve efficiencies. Both the strengths of centralized and distributed networks are inherited by this model. In [32], the authors present an enhanced privacy and data security framework based on blockchain technologies. Multi-layer management aims to improve response times and utilization. In this framework, mobile agents can perform a hash function, implement encryption, implement aggregation, and decrypt data. As a result, mobile agents are transferred from blockchains to IoTs to complete their tasks. An IoT blockchain framework based on a hierarchical two-tier system is proposed in [33] for the IoT car rental system that uses blockchain technology to enhance and measure its scalability. In [34], a cloud-based multi-layer architecture that utilizes blockchain is proposed to facilitate the monitoring and management of the Internet of Underwater Things (IoUT). Using selected residual energy super nodes, clusters and groups of sensor nodes are formed. The Bloom filter is used to track super nodes and nodes. In order to communicate, gateways deploy a standard secret key, which is distinct from the super node's secret key. As a result, the routed data are stored in the blockchain ledger.

In most literature reviews, solutions that address issues related to implementing blockchain technology in IoT systems, including identity management, low scalability, long transaction times, high mining computing resources, and device diversity, have not been proposed. In this article, we implement the lightweight Hyperledger blockchain framework to boost the capabilities of blockchain and the IoT.

From the above discussion, it has been concluded that a heterogeneous IoT network lifespan can be improved by implementing a multi-level architecture and a clustering model. Multi-level architecture can only be achieved with the clustering concept, i.e., the multi-level structure formed by cluster heads. The literature has extensively discussed device-to-device (D2D) networks. The energy consumption of these techniques is lower, and the throughput is higher. Our work proposes a self-clustering method for identifying cluster heads (CH). Each level of the multi-level architecture can perform different kinds of computing and hold different amounts of data. Consequently, each level has its own security strategies. Every design is built on top of the blockchain. In spite of this, blockchain implementations are adjusted for each level.

## 3. Methodology

We propose a cellular network model in order to offer an IoT security mechanism that is both reliable and trustworthy while leveraging cellular capabilities. A clustering algorithm and a consensus algorithm are used to represent the multi-level architecture [6]. In this paper, lightweight authentication and IoT authorization are supported by blockchain technology. In order to formulate such a multi-level network model, it is necessary to divide the whole cell-enabled IoT network into several levels. Level 1 includes a collection of clusters and IoT components. Level 2 consists of nodes and a controller, for instance super nodes (SN). Level 3 is composed of cellular base stations. Since the SNs are cellular devices, they can all connect to the 5G BSs, and thus support D2D. BSs are capable of implementing decentralized blockchain mechanisms at level 3 with appropriate servers and CPUs. Figure 5 illustrates the comprehensive model. It is worth noting that blockchain implementation [3] can lead to increased overhead, and efforts to minimize this should be considered.

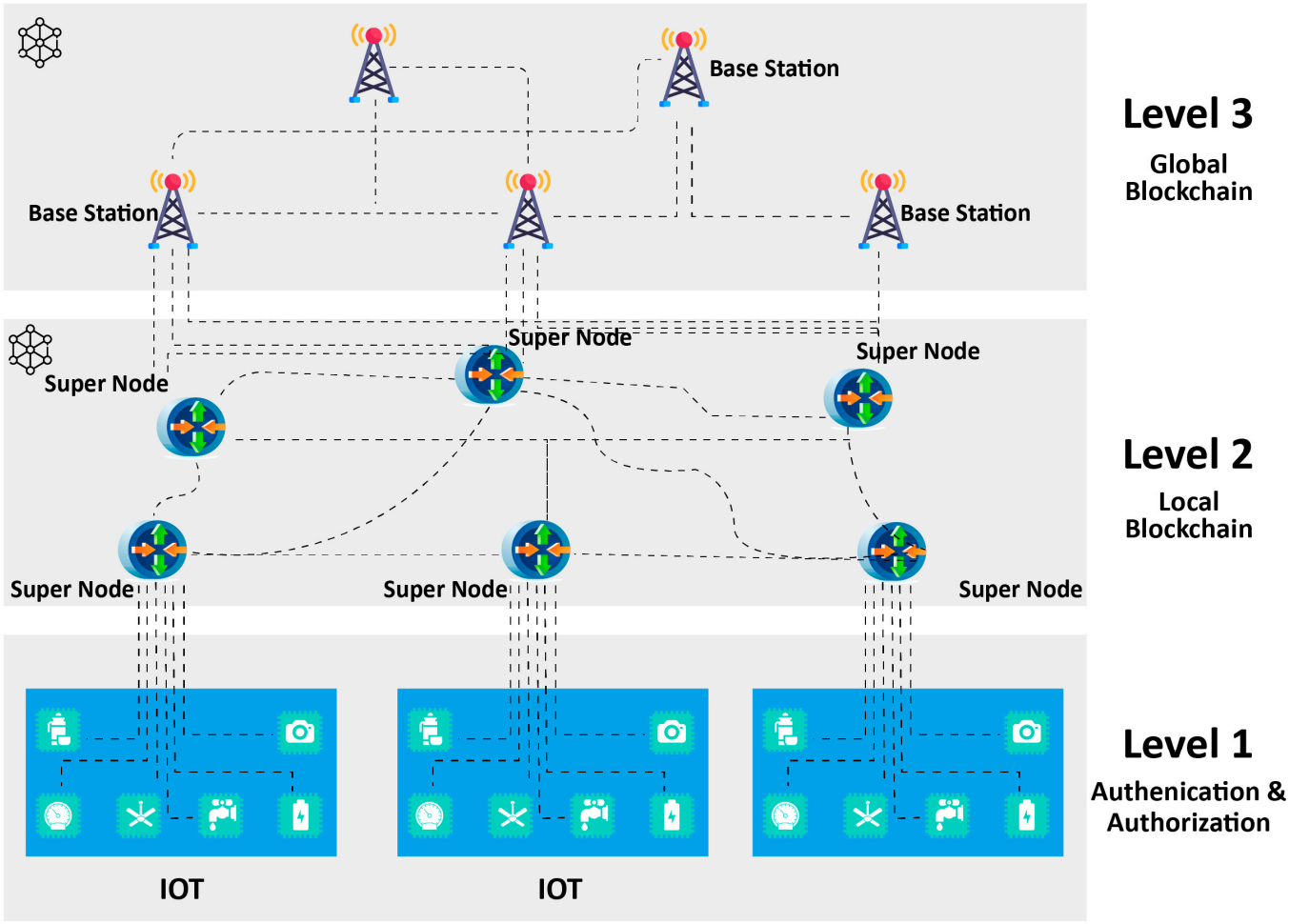


**Figure 5.** The Integrated multi-level (structure) model proposed for IoT and blockchain.

### *3.1. Layer-1: The Cluster Formation*

In this level of IoT, unsupervised hybrid clustering algorithms based on Kruskal's algorithm with the standard K-Means algorithm have been designed to divide an IoT network into multiple clusters. Initially, a comprehensive graph was created, with each vertex representing a single device in the Internet of Things (IoT) network. The weights are assigned to edges based on the Manhattan distance between the relevant devices. Equation (1) shows the Manhattan distance calculation. Where the absolute difference between the attribute vectors of each IoT device has been calculated and summed up. Following that, for each individual cluster, a weighted network containing the currently active nodes was generated. Then, for each weighted network formed in the previous phase, an iterative approach was used to construct a minimum spanning tree (MST) using Kruskal's algorithm.

$$D(A, B) = |A[1] - B[1]| + |A[2] - B[2]| + \ldots + |A[n] - B[n]| \quad (1)$$

where $D$ is the Manhattan distance, $A$ and $B$ are the attributes of two devices, and $n$ is the number of attributes.

Algorithm 1 shows Prim's algorithm used for the construction of a minimum spanning tree, in which a minimum spanning tree is initialized as T and a union set is initialized as UV. All the vertices are added in UV and a queue-based operation is applied to construct a minimum spanning tree.

**Algorithm 1:** Cluster formation using a Kruskal's algorithm-based MST

**MST-Kruskal (G, s)**
T← Ᵽ
UV← Ᵽ
**for each** *vertex v ε V*
***do*** UV← UV U {v}
**for each** (u, v) *ε E*
***do*** *ENQUEUE(Q,u,v,w)*
**while** | UV | > 1 ***do***
*(v, v)*←DQUEUE(Q)
***if*** u, v belongs to different sets US1, US2 *ε UV*
***then*** UV←UV-US1
UV←UV-US2
UV←UV U (US1 UUS2)
T←T U (u, v)
**Return** T

After the formation of clusters, there is a powerful device assigned to each cluster, known as the super node (SN). There are IoT authorization and authentication services built into each cluster of clusters to provide an optimum rate of security and privacy. Figure 6 shows the cluster formation and SN-based communication process.

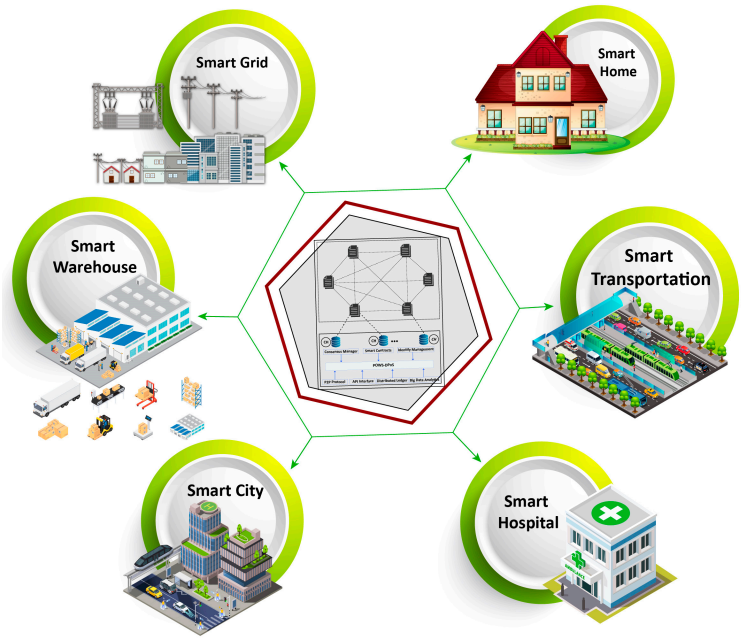


**Figure 6.** The cluster formation and SN-based communication.

The authentication procedure is initiated when a device from one cluster needs to communicate with a device from another cluster. The authentication procedure is the responsibility of the super nodes. This entails validating the authenticity of the requesting device and ensuring that it has the required permissions to access cluster resources. The super nodes determine the extent of access the requesting device should have within the target cluster following successful authentication. This authorization process may involve verifying user roles, permissions, and policies to ensure that the device only has access to the permitted resources. After authentication and authorization have been accomplished, the super nodes support secure communication between clusters by establishing encrypted communication channels and ensuring that data shared between clusters are protected from unauthorized access or alteration.

### *3.2. Layer 2: The Local Blockchain Consensus Protocol Formation*

SNs are connected to each other on the second level by their serving base stations (BSs). These super nodes process data and send them to the higher levels. In the second level, all nodes operate privately on a lightweight blockchain according to a defined consensus algorithm [3]. SN and BSs will verify blocks and generate new ones. Also, they communicate with non-consensus devices and broadcast blocks to each other. Using the blockchain protocol, lower and upper levels are accessible to trusted nodes. A platform called HLF is proposed for this level.

It is imperative to design a network model that addresses the resource-constrained and decentralized nature of IoT networks while considering secure SN communications. Blockchain mining takes up a lot of processing time and is computationally intensive. This makes it unsuitable for use in IoT systems. So, in order to facilitate decentralized, lightweight, and private data communication, we propose a hybrid consensus algorithm based on Proof of Work (PoW) and Pure PoS that overcomes the limitations of traditional PoS which demands significant computational power, leading to substantial energy and resource consumption. Algorithm 2 shows the working of the proposed PoS–Pure PoS. In order to cover the device limitations problem in IoT systems, a lightweight cryptography is also implemented.

**Algorithm 2:** Hybrid local consensus algorithm combining POW and PPoS

```
Function: hybrid-Local-Consensus(D, nonce)
        Broadcast (nonce, D)
        N(j) = HASH(NASH(PreBlockHead), nonce)
        While (HASH(PreBlockHead), nonce) > D)
              nonce = nonce + 1 N = N(i)
              Broadcast (N(c))
              N(T) = N = N(c)
        Endwhile
Return N(w), N(a)
End
```

A private permissioned blockchain platform called Hyperledger Fabric (HLF) [35,36] is also used to connect SNs and other networked elements in the proposed model. HLF uses a method of execution order validation. The execution of transactions using smart contracts is decoupled from the transaction order for scalability and modularity. In addition to the hybrid consensus protocol, this model has four essential components: base station, order clustering, IoT nodes and peers that further include endorsers and committers individuals, membership service providers, and channels as illustrated in Figure 7. A distributed ledger is maintained and transactions are executed by peers that may be either endorsers, committers, or both. The orders are responsible for transaction orders, proposing new blocks, and reaching the consensus. Usually, by default, every peer is a committer which maintains the ledger and receives a block from the ordering service. After the peers validate the transactions of a new block, they commit the changes to local ledgers and add them to the blockchain. Likewise, peers can endorse transactions as endorsers. Before sending the results back to the client, the endorser appends a cryptographic signature (called endorsement) to the results of the smart contract (ChainCode in HLF). According to predefined roles, SNs have the option to take on the role of endorser or committer.

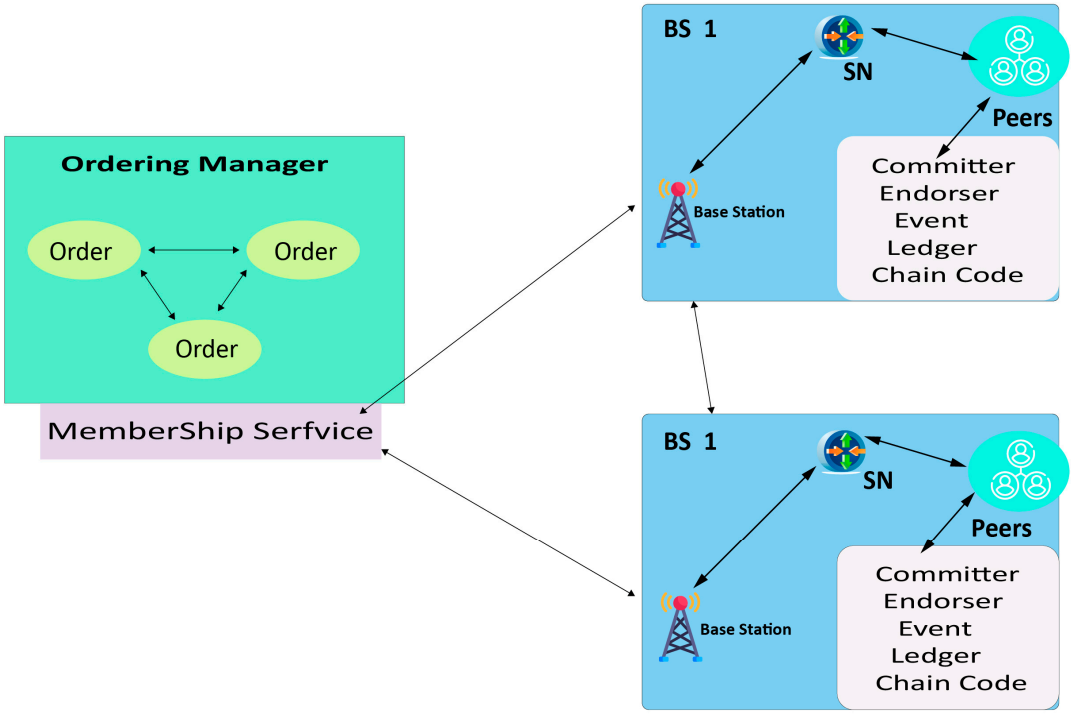


**Figure 7.** The cluster formation and SN-based communication.

In the Hyperledger network, MSP performs authentication services. To verify node identities, MSP performs identity validation. Organizations represent Hyperledger's logical entities. With the help of MSP, they manage all members of the network. Private channels facilitate the communication between the network elements. The committers validate and update the shared ledger. Smart contracts are used to define transactions [37]. Blockchain implementation takes place in BSs in the high-level layers. SNs and different nodes are connected to BSs as part of the IoT system. Using an ordering cluster, transactions and queue orders are handled using a peer-to-peer channel. Moreover, the ordering service creates transaction blocks then broadcasts the transactions. By utilizing the ordering service, ordering clusters receive transactions from IoT devices to create a block of transactions. Many variables determine whether IoT nodes should have an endorser or committer role in a blockchain network, such as the network configuration. Additionally, committer nodes add blocks to the blockchain ledger.

Putting in an endorsement request makes an IoT node an endorser. The endorser node approves and monitors the request. The smart contract is executed after the consistency check is completed. A specific read and write permission is granted to the endorser by responding to requests from an IoT node. The ordering service creates transaction blocks by ordering clusters. These blocks are distributed across all SNs. As part of this level, IoT node specifications and transactions are recorded to the blockchain ledger and a copy is pushed to all peers after validation.

### *3.3. Layer-3: The Global Blockchain Formation and Secure Communication*

Base station (BS) nodes are part of this level and act as the owners of organizations. Devices are managed, data are generated, and requests are processed as part of a cloud server by BSs. In this level, trusted nodes have computing power capabilities with a limited amount of power and processor. With the help of the global blockchain, better asymmetric cryptography mechanisms will be possible at this level. In order to meet these criteria, it has been determined that the implementation of elliptic curve cryptography (ECC) is one of the potential solutions that might work for this layer. We used the PoP and DPoS in this phase as a global level symmetry.

PoP can be seamlessly integrated with the DPoS consensus mechanism to establish a robust foundation for global blockchain formation. PoP introduces an innovative approach by incorporating participants' real-world influence and contributions into the consensus process. In the proposed hybrid model, participants showcase their expertise, reputation, or physical assets to validate transactions and create new blocks, thus bolstering the network's security and decentralization. Simultaneously, DPoS brings efficiency by enabling token holders to delegate their voting power to elected validators, who manage block production and network maintenance. This combination ensures that the blockchain's consensus is not solely reliant on computational power but also incorporates the tangible influence participants possess. This approach also mitigates the energy consumption concerns associated with PoP while maintaining high security and governance. By merging PoP with DPoS, the blockchain ecosystem can achieve a scalable and sustainable network that harnesses both computational and real-world prowess, fostering a new era of decentralized applications and services on a global scale. The proposed PoP–DPoS hybrid global consensus algorithm is shown in Algorithm 3. Here, Z represents node workload values, and N stands for the total number of nodes. Each node starts with an initial workload value of $ZV_{init}$ and node V is designated as the primary node. $ZV_{inilowt}$ and $ZV_{high}$ are threshold values.

**Algorithm 3:** POP–DPoS hybrid global consensus algorithm

**DPoS-POP (Z, $ZV_{init}$, $ZV_{low}$, $ZV_{high}$, *M*)**
T←$ZV_{low}$+($ZV_{init} - ZV_{inilowt}$)/2;
***For*** j←0 to M−1 do
    ***If*** Z[j] > $ZV_{high}$
        Z[j]←Random $\left(ZV_{init}, ZV_{high}\right)$
    ***Else if*** Z[j] ← $ZV_{init}$
        ***End if***
***End for***
***Return*** W;

In addition to the proposed global blockchain, this layer also consists of BSs capable of performing mining tasks independently of authentication servers. A distributed network at this level is composed of computationally powerful nodes. Thus, new security techniques and blockchain, such as Ethereum, are feasible. In this level, the elliptic curve cryptography (ECC) [38] was used as an ideal approach to asymmetric cryptography. Blockchain technology ensures data integrity while enhancing privacy and security. This level records the exchange of transactions between nodes. Super nodes, base stations, and computing edge nodes establish a global trust relationship service mechanism.

A blockchain's peer-to-peer nature enables BS nodes and other nodes to construct a globally distributed security framework. Through the use of certificates, the communication between SNs and computing edge nodes is implemented using blockchain-based communication. Smart contracts distribute certificates throughout this level to carry out trustful communication between nodes. SNs must sign the certificates. When two SNs collaborate to authorize their entities, the blockchain-based model helps enhance the distributed trust between them. In addition to enhancing trust, the blockchain-based model facilitates communication between entities or IoT nodes divided into separate clusters within the blockchain. With blockchain-based systems, smart contracts are executed in real-time, so there is no need to use fixed addresses and domain names in order to communicate. As proposed, the super node communicates with the edge device and executes a smart contract without requiring a fixed address or domain name.

## 4. Results

### *4.1. Network Self-Clustering*

At this stage of the process, network clustering is carried out using advanced metaheuristic algorithms, such as the genetic algorithm (GA) and ant colony optimization

(ACO), among others. Implementing these metaheuristic algorithms requires the establishment of a closely integrated relationship between computational practices and optimization techniques. This synergy between the two domains is essential for the successful application of these algorithms. One of the key advantages inherent to these metaheuristic methods, as indicated by research [39], lies in their ability to navigate past local optimal points effectively. This characteristic distinguishes them from conventional approaches, as it ensures that they do not get trapped in suboptimal solutions. Instead, these algorithms are inherently designed to explore and seek solutions across the entirety of the search space, leaving no stone unturned in their quest for optimal configurations.

Furthermore, the metaheuristic algorithms adopt a distributed control paradigm that extends its influence across all nodes within the network and among the various participants involved in the network. This decentralization of control empowers individuals within the network to engage in localized communication with one another. This capability fosters a dynamic and adaptive network structure, allowing for efficient coordination and decision making at the local level. As the environment surrounding the network changes, the system adapts accordingly. This dynamic responsiveness ensures that the system can swiftly react to shifts in its environment, whether they stem from alterations in data patterns or external factors. Consequently, the network system exhibits an elevated level of robustness and adaptability, capable of flexibly adjusting its configuration and behavior to align with the evolving environmental conditions. The holistic approach to network clustering and control, facilitated by these metaheuristic algorithms, underscores their significance in optimizing network performance and resilience.

### *4.2. Blockchain Implementation*

#### 4.2.1. Development Environment

To show the practicality and viability of the suggested blockchain system, we used two simulation models in two correspondingly leveled contexts. The level 2 implementation of the HLF blockchain includes IoT devices, SN nodes, APIs, and organizations. We compared Ethereum and HLF metrics implementation using a public blockchain simulator at level 3. In this simulation model at level 3, the blockchain applications are hosted on a workstation which acts as a server. The multi-level blockchain implementation environment, as shown in Figure 2, was designed to test the efficiency of the proposed blockchain architecture. It also shows the relationships between various IOT entities, including devices, servers, and the blockchain system. The IBM Watson was utilized to implement the IoTs, while the IBM IoT platform hosted the IoT's gateway. Ref. [40] was selected. The Constrained Application Protocol was used to communicate between IoT devices and Node-RED servers. A lightweight permissioned blockchain framework provided level 2 security, and a virtual environment was used to organize the IoT server.

To create a block of transactions that can be added to the blockchain ledger, peers must install and initiate smart contracts on their nodes. Both state changes and transactions are recorded in the ledger, which also stores versioning data and key-value pairs for the state data. The ledger records all changes to the state database in chronological order, with each block securely linked to the next using cryptography. The ordering node uses the PBFT algorithm to ensure the consistency of the ledger. HLF uses the execute–order–validate–commit transaction model.

As a blockchain server, a workstation was used as the level 3 simulation model. With this environment, we were able to measure the throughput and latency of Ethereum and Hyperledger networks. A virtual workload was generated, and the networks were configured under comparable settings. The experimental set up considered a distributed environment with two blockchain networks. Simulators used a workstation as a base station. One mining node was used in the Ethereum network for simplicity's sake. An analysis of the experiment is presented in Section 3.

#### 4.2.2. Modeling Transactions Using Smart Contracts

Using the Hyperledger Composer [41], developers could build and implement blockchain applications as well as smart contracts. The Hyperledger Composer was used to deploy the network using open development tools. Businesses could submit transactions pertaining to their networks in the case of business networks. An IoT participant is a device owner (SN or BS node) who has rights to manage their devices.

Assets are registerable as stored services, devices, properties, and goods in a network. It is possible to identify a device based on the ID, the type, the name, owner, the timestamp, the event, and the value. Simulation model nodes, including SN nodes, are different kinds of assets. A smart contract represents a logical process of transactions. As a result, cloud-based or off-chain storage systems were used to store the data, while blockchain-enabled checksums, pointers, and ownership were stored in the ledger. There were smart contracts that acted on assets and participants. In addition, a smart contract is able to specify miscellaneous conditions and rules for a transaction to perform multiple actions within the blockchain network, including reading, creating, updating, or deleting. Transaction process functions in smart contracts were used as a logical basis for the operations. An ad hoc query language was used in these smart contracts to extract data from the blockchain network. REST APIs were used to communicate between blockchain, IoT, and web applications through composer-rest-server.

### *4.3. Performance Evaluation*

Using blockchain applications, participants can submit transactions and keep track of them. The verification and ordering of submitted transactions generates a blockchain block. Several metrics have been identified as indicators of blockchain application performance by the Hyperledger Performance and Scale Working Group [42]:

- Transaction throughput: how many transactions are conducted during a specific time period.
- Transaction Latency: ledger entry time for a transaction.

To evaluate the model's performance, we benchmarked the system's results for latency and throughput versus parameters from the literature to demonstrate its efficiency. Hyperledger Caliper [42] was used to facilitate the configuration of the blockchain.

Based on the proposed model, SNs need a certain amount of time to verify blocks. There is a direct correlation between block size and both the network latency and node. When the new block validations begin to be detected on the node, latency is measured as the amount of time that it takes for the system to reach consensus.

Open, transfer, and query (transactions) were used to analyze the system. Our analysis covered Hyperledger Fabric and Ethereum. Three types of transactions were assessed for latency and throughput based on the simulation results shown in Table 1. This model allows some nodes (SNs) to participate in the new block validation. Multi-level models decrease average latency. The same table also includes the results of the Ethereum implementation. HLF appears superior to Ethereum due to its lightweight nature.

**Table 1.** Comparing Ethereum and Hyperledger performance metrics (HLF: Hyperledger Fabric, Eth: Ethereum).

| Blockchain | Send Rate | | Maximum Latency | | Minimum Latency | | Average Latency | | Throughput | |
|---|---|---|---|---|---|---|---|---|---|---|
| | HLF | Eth | HLF | Eth | HLF | Eth | HLF | Eth | HLF | Eth |
| Open | 19.3 | 23.8 | 0.29 | 6.56 | 0.02 | 1.89 | 0.15 | 4.37 | 19.91 | 11 |
| Query | 9 | 10.3 | 0.05 | 0.02 | 0.01 | 0.01 | 0.01 | 0.01 | 10 | 11.3 |
| Transfer | 9 | 10.8 | 0.29 | 6.34 | 0.04 | 1.66 | 0.16 | 4.44 | 10 | 7.8 |

It is equally important to consider the latency and throughput for IoT applications, despite the fact that security and privacy are crucial. The blockchain network needs to allocate resources accordingly to suit latency requirements. To further analyze the performance of the system under test, we conducted a series of benchmarking experiments at varying transaction sending rates. We generated 1000 transactions, each benchmark at 10–500 TPS, to test latency and throughput. This allowed us to evaluate the SUT's behavior under different loads. The results of each experiment are depicted in Figure 8, which shows the maximum, average, and lowest transaction delay figures from each trial. As the send rate approached 100 TPS, the maximum latency increased as the lowest latency hung less than 1 s. Figure 9 shows the results for the variable transmission rates for transaction throughput. Sending rates of up to 100 TPS were seen with a throughput of approximately 100 percent. After 150 TPS, SUT's throughput dropped significantly.

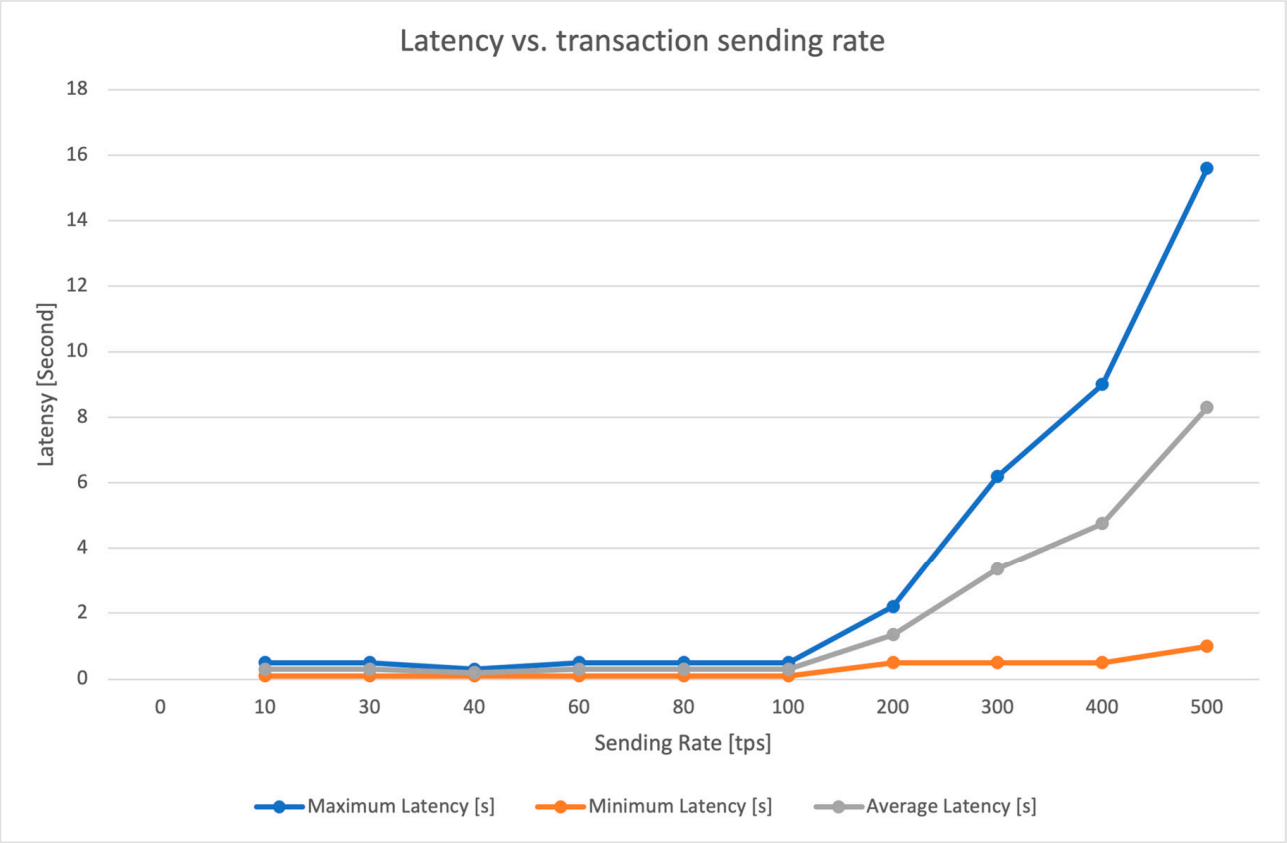


**Figure 8.** Latency vs. transaction.

It is not feasible to send at a rate of 100 TPS, because the current throughputs are somewhere between 95 and 100%. Even higher send rates of 100 and 300 TPS result in an insignificant reduction in throughput. As a result, we determined that our setup is capable of handling 100 TPS of sending. In the proposed model, multiple 5G-enabled IoT applications can be provisioned in real-time without imposing any latency. With an increase in input transactions, maximum latency grows to around 14 s. The reason for this is that peer nodes have been allocated containers with limited resources. Initially, peer nodes are not under a heavy load, so nearly constant latency is the minimum. Furthermore, the configuration of the blockchain has an impact on latency. There have been no instances of transactions being lost since all of the transactions have been successfully completed.

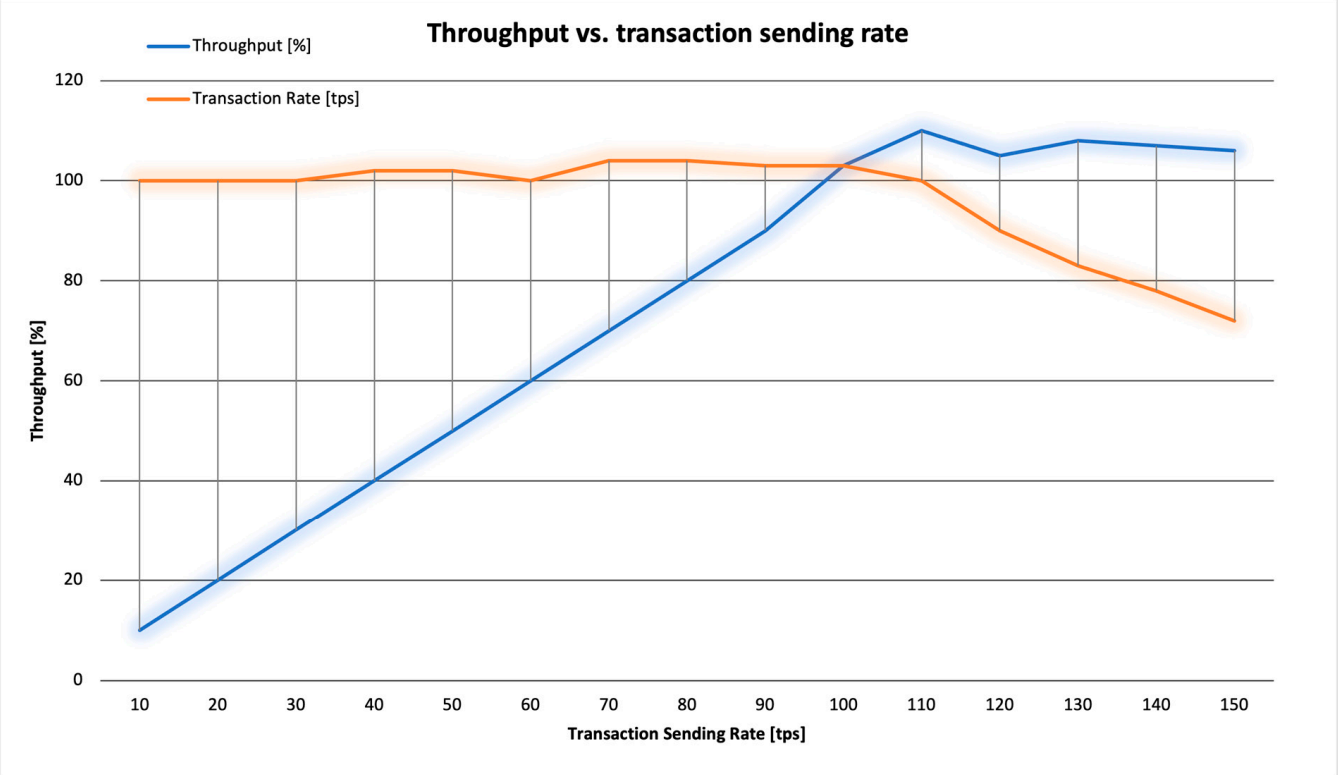


**Figure 9.** Throughput vs. transaction.

All of the transactions in this experiment were generated by a single client in the blockchain network. In line with our expectations, the blockchain network's performance is heavily influenced by the underlying hardware. HLF implements a revolutionary three-stage approach known as execute–order–validate that is dependent on previous transactions. Based on the results of our experimentations, the proposed blockchain-based IoT application based on HLF is able to perform 100 TPS with an average latency of 600 ms, approaching 100% throughput at the maximum of 100 TPS. It is not feasible to send at a rate of 100 TPS, because the current throughputs are somewhere between 95 and 100%. Even higher send rates of 100 and 300 TPS result in an insignificant reduction in throughput.

As a result, we determined that our setup is capable of handling 100 TPS of sending. In the proposed model, multiple 5G-enabled IoT applications can be provisioned in real-time without imposing any latency. With an increase in input transactions, maximum latency grows to around 14 s. The reason for this is that peer nodes have been allocated containers with limited resources. Initially, peer nodes are not under heavy load, so nearly constant latency is the minimum. Furthermore, the configuration of the blockchain has an impact on latency. There have been no instances of transactions being lost since all transactions have been successfully completed.

A comparison of metrics presented in Table 2 illustrates a clear advantage of the Hyperledger blockchain technology-based secured IoT multi-level model over previous literature reports.

**Table 2.** Comparison of security challenges in IoT blockchain applications.

| | Ref | Research | Consensus | Authentication | Privacy | Scalability | Flexibility | Type |
|---|---|---|---|---|---|---|---|---|
| 1 | [38] | Smart Cities, Smart Grid | PoW | × | × | √ | √ | Private |
| 2 | [43] | Smart Cities, Microgrids, Vehicle | PoW | × | √ | × | × | Consortium |
| 3 | [44] | Smart Cities, Microgrids | PoC | × | √ | × | × | Private |
| 4 | [45] | eHealth | PoW | × | √ | √ | × | Public |
| 5 | [46] | Industrial IoT | PoW | × | √ | × | √ | Private |
| 6 | [47] | Supply Chain, Smart Factory | PoS | × | × | × | √ | Consortium |
| 7 | [48] | Energy Harvesting networks, Industrial IoT | PoW | × | √ | × | √ | Consortium |
| 8 | [37] | eHealth | PoW | × | √ | × | √ | Public |
| 9 | [49] | eHealth, Mobile edge computing | PoC | × | × | √ | × | Permissioned |
| 10 | [50] | V2X, Cloud computing | PoS | √ | √ | × | × | Consortium |
| 11 | [51] | Vehicular Edge Computing | PoW | √ | × | × | √ | Consortium |
| 12 | [52] | IoT | PBFT and POS | √ | × | √ | √ | Consortium |
| 13 | | Proposed Multi-level | PBFT, PoC | √ | √ | √ | √ | Consortium |

### *4.4. Framework Privacy*

Within the framework of the blockchain system, one of its key functions involves the recording of contracts between various entities. In light of this, it becomes imperative to undertake a comprehensive assessment of privacy disclosure within the system. This is particularly relevant because the pseudonym of an entity is encapsulated within an IoT address, which serves as the means to encode the identity of an object on the blockchain. In this blockchain ecosystem, smart contracts play a pivotal role in the management of tasks and transactions. Unlike traditional systems that rely on domain names and physical addresses, smart contracts become the central element for governing interactions between entities. These contracts are self-executing and self-enforcing, ensuring a high degree of automation and reliability in the system. In order to bolster privacy and security, IoT networks are equipped with mechanisms to encrypt and record the IP address of each individual object. This encryption process serves the purpose of concealing the actual IP address associated with an object, thereby preserving its anonymity within the network. This measure is essential for safeguarding the privacy of objects and the data they generate or interact with within the blockchain ecosystem. Moreover, within the broader context of the blockchain, security is upheld by employing robust hash algorithms. These cryptographic algorithms are applied within the contractual context to ensure the integrity and authenticity of transactions and data. By using hash algorithms, the blockchain system can verify the validity of data, detect any unauthorized changes, and provide a high level of security and trust in the execution of smart contracts.

### *4.5. Heterogeneity and Flexibility*

In different scenarios, the proposed framework is able to accommodate different security configurations. In some cases, these are low-powered, high-risk, and broadcast IoT devices. Based on the power of cryptography techniques (strong and lightweight cryptography) and key lifetime features, there are a variety of security configuration options. An array of encryption and authentication protocols for session keys and cached session keys may have more than one owner. TCP and UDP stability are also important. By

allowing a node or entity the option of joining or leaving the system, it is possible to be flexible to some extent. As changes occur in the network, the blockchain records them.

### *4.6. Authentication*

Authentication consists of two stages: (1) the infrastructure level, which is responsible for local authentication, and (2) smart contracts, which confer rights to objects. Blockchains implemented in multiple segments record node requirements and rights. Essentially, the block summary consists of a brief description of the contract. It can be accessed whenever needed. This summary is non-repudiable, so that the interests of the subject are protected.

By grouping together the network tiers through a multi-level approach, the IoT network can be divided into several tiers. As well as local authentication services, the blockchain framework uses a globally distributed approach, while segregating external authority. The network would be significantly less impacted by an attack or failure of the local authentication service that only affects compromised nodes.

### *4.7. Scalability*

To attain scalability, the framework focuses on resolving two critical challenges: the handling of massive data traffic and the management of a large number of Internet of Things (IoT) devices. Scalability is accomplished through the adoption of a multi-level structure, enabling the implementation of multiple clusters. This multi-level approach is instrumental in expanding the capabilities of the framework. One of the core elements facilitating scalability is the utilization of a client–server model. In this model, sensor network (SN) nodes can establish secure and reliable communications with one another. This secure communication is vital for the efficient operation of the framework. The framework promotes secure communication primarily within individual clusters to further streamline operations and minimize unnecessary resource overhead. This means that SN nodes within a cluster securely communicate with one another. This intra-cluster communication reduces the potential for resource wastage and ensures efficient data transmission and processing. A crucial aspect of the security infrastructure within this framework involves the exchange of cryptographic keys. Before networked SN nodes can communicate within the blockchain framework, they must exchange cryptographic keys. This step significantly minimizes overhead even further, as it ensures that only authorized nodes can communicate securely.

## 5. Conclusions

IoT devices connected to multi-hop cellular networks are described in a multi-level security framework presented in this paper, which utilizes distributed technology applied to blockchain. In developing our model, we demonstrate that blockchain technology can be employed to secure cellular-enabled, decentralized IoT networks.. The manuscript discusses how the blockchain-based IoT system can enhance system authentication and authorization and provides a detailed description of system implementation. The model proposes deploying and verifying it on the open-source Hyperledger Fabric (HLF) blockchain. We leverage a multi-level architecture to improve security and the processing load while reducing the network load and latency. Utilizing the peer-to-peer nature of blockchain communication, our proposed implementation enhances communication efficiency between devices and aligns it with cellular systems, thereby enhancing integrity and security. This approach addresses various IoT security challenges, including privacy, identity confirmation, heterogeneity, flexibility, and scalability. Our algorithm underwent evaluation against four existing protocols. Through simulations, it has been demonstrated that this algorithm surpasses competing algorithms in several critical areas, such as throughput, network range, and distances. We conducted a performance evaluation of the proposed multi-level blockchain framework, revealing its effectiveness, particularly when compared to the global blockchain, Ethereum. Looking ahead, our future work entails the continued development, analysis, and real-world deployment of our framework for IoT devices. This

endeavor aims to comprehensively study and analyze its performance in practical settings, further establishing its utility and effectiveness in securing IoT networks.

**Author Contributions:** Conceptualization, writing—original draft, and methodology A.A. (Ahmed Alhusayni); software and validation, V.T.; investigation, A.A. (Aiiad Albeshri); resources, S.A. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research was funded by the Deanship of Scientific Research at Umm Al-Qura University, Grant Code: (23UQU4340121DSR01).

**Data Availability Statement:** Not Applicable.

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

## Abbreviations

Below a list of abbreviations used in this article:

| | |
|---|---|
| BS | Base Station |
| SN | Super Node |
| D2D | Device-to-Device |
| HLF | Hyperledger Fabric |
| IoT | Internet of Things |
| MSP | Membership Service Providers |
| PoC | Proof of Concept |
| PoW | Proof of Work |
| SUT | System Under the Test |
| TLS | Transport Layer Security |

## References

1. Mishra, S. Blockchain and Machine Learning-Based Hybrid IDS to Protect Smart Networks and Preserve Privacy. *Electronics* **2023**, *12*, 3524. [CrossRef]
2. Kshetri, N. Can Blockchain Strengthen the Internet of Things? *IT Prof.* **2017**, *19*, 68–72. [CrossRef]
3. Dorri, A.; Kanhere, S.S.; Jurdak, R.; Gauravaram, P. LSB: A Lightweight Scalable Blockchain for IoT Security and Anonymity. *J. Parallel Distrib. Comput.* **2019**, *134*, 180–197. [CrossRef]
4. Khan, M.A.; Salah, K. IoT Security: Review, Blockchain Solutions, and Open Challenges. *Future Gener. Comput. Syst.* **2018**, *82*, 395–411. [CrossRef]
5. Yang, Y.; Wu, L.; Yin, G.; Li, L.; Zhao, H. A Survey on Security and Privacy Issues in Internet-of-Things. *IEEE Internet Things J.* **2017**, *4*, 1250–1258. [CrossRef]
6. Mistry, I.; Tanwar, S.; Tyagi, S.; Kumar, N. Blockchain for 5G-Enabled IoT for Industrial Automation: A Systematic Review, Solutions, and Challenges. *Mech. Syst. Signal Process.* **2020**, *135*, 106382. [CrossRef]
7. Al-Fuqaha, A.; Guizani, M.; Mohammadi, M.; Aledhari, M.; Ayyash, M. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 2347–2376. [CrossRef]
8. Zhao, D.; Yan, Z.; Wang, M.; Zhang, P.; Song, B. Is 5G Handover Secure and Private? A Survey. *IEEE Internet Things J.* **2021**, *8*, 12855–12879. [CrossRef]
9. Felcia, H.J.; Sabeen, S. A Survey on IoT Security: Attacks, Challenges and Countermeasures. *Webology* **2022**, *19*, 3741–3763.
10. Liang, J.; Ma, M.; Yang, G.; Wang, H. Bac-Crl: Blockchain-Assisted Coded Caching Certificate Revocation List for Authentication in Vanets. *SSRN Electron. J.* **2022**, *218*, 103716. [CrossRef]
11. Maamar, Z.; Faci, N.; Ugljanin, E.; Baker, T.; Burégio, V. Towards a Cell-Inspired Approach for a Sustainable Internet-of-Things. *Internet Things* **2021**, *14*, 100400. [CrossRef]
12. Apthorpe, N.; Huang, D.Y.; Reisman, D.; Narayanan, A.; Feamster, N. Keeping the Smart Home Private with Smart(Er) IoT Traffic Shaping. *Proc. Priv. Enhancing Technol.* **2019**, *2019*, 128–148. [CrossRef]
13. Novo, O. Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT. *IEEE Internet Things J.* **2018**, *5*, 1184–1195. [CrossRef]
14. Pal, S.; Rabehaja, T.; Hill, A.; Hitchens, M.; Varadharajan, V. On the Integration of Blockchain to the Internet of Things for Enabling Access Right Delegation. *IEEE Internet Things J.* **2020**, *7*, 2630–2639. [CrossRef]
15. Qu, C.; Tao, M.; Zhang, J.; Hong, X.; Yuan, R. Blockchain Based Credibility Verification Method for IoT Entities. *Secur. Commun. Netw.* **2018**, *2018*, 7817614. [CrossRef]
16. Lau, C.H.; Yeung, K.H.; Yan, F.; Chan, S. Blockchain-based Authentication and Secure Communication in IoT Networks. *Secur. Priv.* **2023**, e319. [CrossRef]

17. Alnahari, M.S.; Ariaratnam, S.T. The Application of Blockchain Technology to Smart City Infrastructure. *Smart Cities* **2022**, *5*, 979–993. [CrossRef]
18. Hassan, M.U.; Rehmani, M.H.; Chen, J. Privacy Preservation in Blockchain Based IoT Systems: Integration Issues, Prospects, Challenges, and Future Research Directions. *Future Gener. Comput. Syst.* **2019**, *97*, 512–529. [CrossRef]
19. Dai, H.-N.; Zheng, Z.; Zhang, Y. Blockchain for Internet of Things: A Survey. *IEEE Internet Things J.* **2019**, *6*, 8076–8094. [CrossRef]
20. Al Hwaitat, A.K.; Almaiah, M.A.; Ali, A.; Al-Otaibi, S.; Shishakly, R.; Lutfi, A.; Alrawad, M. A New Blockchain-Based Authentication Framework for Secure IoT Networks. *Electronics* **2023**, *12*, 3618. [CrossRef]
21. Biswas, S.; Sharif, K.; Li, F.; Maharjan, S.; Mohanty, S.P.; Wang, Y. PoBT: A Lightweight Consensus Algorithm for Scalable IoT Business Blockchain. *IEEE Internet Things J.* **2020**, *7*, 2343–2355. [CrossRef]
22. Xu, X.; Zeng, Z.; Yang, S.; Shao, H. A Novel Blockchain Framework for Industrial IoT Edge Computing. *Sensors* **2020**, *20*, 2061. [CrossRef] [PubMed]
23. Yanez, W.; Mahmud, R.; Bahsoon, R.; Zhang, Y.; Buyya, R. Data Allocation Mechanism for Internet-of-Things Systems with Blockchain. *IEEE Internet Things J.* **2020**, *7*, 3509–3522. [CrossRef]
24. Hewa, T.; Bracken, A.; Ylianttila, M.; Liyanage, M. Blockchain-based Automated Certificate Revocation for 5G IoT. In Proceedings of the IEEE International Conference on Communications (ICC), Dublin, Ireland, 7–11 June 2020; pp. 1–7.
25. Wang, H.; He, D.; Yu, J.; Xiong, N.N.; Wu, B. RDIC: A Blockchain-Based Remote Data Integrity Checking Scheme for IoT in 5G Networks. *J. Parallel Distrib. Comput.* **2021**, *152*, 1–10. [CrossRef]
26. Gupta, R.; Patel, M.M.; Tanwar, S.; Kumar, N.; Zeadally, S. Blockchain-Based Data Dissemination Scheme for 5G-Enabled Softwarized UAV Networks. *IEEE Trans. Green Commun. Netw.* **2021**, *5*, 1712–1721. [CrossRef]
27. A Blockchain Platform for the Enterprise (Hyperledger Fabric). Available online: http://hyperledger-fabric.readthedocs.io/ (accessed on 15 September 2021).
28. Ayğin, N.; Karaköse, M. Genetic Algorithm-Based Optimization of Mass Customization Using Hyperledger Fabric Blockchain. *Turk. J. Sci. Technol.* **2022**, *17*, 451–460.
29. Zhaofeng, M.; Lingyun, W.; Xiaochang, W.; Zhen, W.; Weizhe, Z. Blockchain-Enabled Decentralized Trust Management and Secure Usage Control of IoT Big Data. *IEEE Internet Things J.* **2020**, *7*, 4000–4015. [CrossRef]
30. Alharbi, S.; Attiah, A.; Alghazzawi, D. Integrating Blockchain with Artificial Intelligence to Secure IoT Networks: Future Trends. *Sustainability* **2022**, *14*, 16002. [CrossRef]
31. Sharma, P.K.; Park, J.H. Blockchain Based Hybrid Network Architecture for the Smart City. *Future Gener. Comput. Syst.* **2018**, *86*, 650–655. [CrossRef]
32. Mbarek, B.; Jabeur, N.; Pitner, T.; Yasar, A.-U.-H. MBS: Multilevel Blockchain System for IoT. *Pers. Ubiquitous Comput.* **2019**, *25*, 247–254. [CrossRef]
33. Oktian, Y.E.; Lee, S.-G.; Lee, H.J. Hierarchical Multi-Blockchain Architecture for Scalable Internet of Things Environment. *Electronics* **2020**, *9*, 1050. [CrossRef]
34. Uddin, M.A.; Stranieri, A.; Gondal, I.; Balasurbramanian, V. A Lightweight Blockchain Based Framework for Underwater IoT. *Electronics* **2019**, *8*, 1552. [CrossRef]
35. Verdian, G. Quant Overledger Whitepaper. Release V0.1. 2018. Available online: https://chainwhy.com/upload/default/20181026/f5092d3f80d6aab53ce37b8f320dfe70.pdf (accessed on 31 August 2023).
36. Luo, H. ULS-PBFT: An Ultra-Low Storage Overhead PBFT Consensus for Blockchain. *Blockchain Res. Appl.* **2023**, 100155. [CrossRef]
37. 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]
38. Soman, P. Lightweight Elliptical Curve Cryptography (ECC) for Data Integrity and User Authentication in Smart Transportation IoT System. In Proceedings of the International Conference on Sustainable Communication Networks and Application, Erode, India, 30–31 July 2019; Springer: Cham, Switzerland, 2019.
39. García, J.; Crawford, B.; Soto, R.; Astorga, G. A Clustering Algorithm Applied to the Binarization of Swarm Intelligence Continuous Metaheuristics. *Swarm Evol. Comput.* **2019**, *44*, 646–664. [CrossRef]
40. Nykyri, M.; Kuisma, M.; Kärkkäinen, T.J.; Hallikas, J.; Jäppinen, J.; Korpinen, K.; Silventoinen, P. IoT demonstration platform for education and research. In Proceedings of the 2019 IEEE 17th International Conference on Industrial Informatics (INDIN), Helsinki, Finland, 22–25 July 2019; Volume 1.
41. Hyperledger Composer Documentation. 2018. Available online: https://hyperledger.github.io/composer/latest/introduction/introduction.html (accessed on 18 December 2021).
42. About Hyperledger Foundation. 2018, Volume 1. Available online: https://www.hyperledger.org/wp-content/uploads/2021/11/HL_Paper_HyperledgerOverview_102721.pdf (accessed on 18 December 2021).
43. 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, 22 July 2016.
44. Aitzhan, N.Z.; Svetinovic, D. Security and Privacy in Decentralized Energy Trading Through Multi-Signatures, Blockchain and Anonymous Messaging Streams. *IEEE Trans. Dependable Secur. Comput.* **2018**, *15*, 840–852. [CrossRef]

45. Wang, K.; Shao, Y.; Shu, L.; Zhu, C.; Zhang, Y. Mobile Big Data Fault-Tolerant Processing for Ehealth Networks. *IEEE Netw.* **2016**, *30*, 36–42. [CrossRef]
46. Wan, J.; Li, J.; Imran, M.; Li, D. Fazal-e-Amin A Blockchain-Based Solution for Enhancing Security and Privacy in Smart Factory. *IEEE Trans. Ind. Inform.* **2019**, *15*, 3652–3660. [CrossRef]
47. Lu, Q.; Xu, X. Adaptable Blockchain-Based Systems: A Case Study for Product Traceability. *IEEE Softw.* **2017**, *34*, 21–27. [CrossRef]
48. 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]
49. Rahman, M.D.A.; Hossain, M.S.; Loukas, G.; Hassanain, E.; Rahman, S.S.; Alhamid, M.F.; Guizani, M. Blockchain-Based Mobile Edge Computing Framework for Secure Therapy Applications. *IEEE Access* **2018**, *6*, 72469–72478. [CrossRef]
50. Liu, H.; Zhang, Y.; Yang, T. Blockchain-Enabled Security in Electric Vehicles Cloud and Edge Computing. *IEEE Netw.* **2018**, *32*, 78–83. [CrossRef]
51. Firdaus, M.; Rhee, K.-H. On Blockchain-Enhanced Secure Data Storage and Sharing in Vehicular Edge Computing Networks. *Appl. Sci.* **2021**, *11*, 414. [CrossRef]
52. Alghamdi, S.; Albeshri, A.; Alhusayni, A. Enabling a Secure IoT Environment Using a Blockchain-Based Local-Global Consensus Manager. *Electronics* **2023**, *12*, 3721. [CrossRef]