IoT

MDPI

Article

Enhancing IoT Data Security: Using the Blockchain to Boost Data Integrity and Privacy

Ali Eghmazi [1,*], Mohammadhossein Ataei [1], René Jr Landry [1] and Guy Chevrette [2]

[1] Département de Génie Électrique, École de Technologie Supérieure, 1100 Rue Notre Dame Ouest, Montreal, QC H3C 1K3, Canada; mohammad-hossein.ataei@lassena.etsmtl.ca (M.A.); renejr.landry@etsmtl.ca (R.J.L.)
[2] Corporate Office of iMETRIK Global Inc., Montreal, QC J4P 2K7, Canada; guy.chevrette@imetriklabs.com
* Correspondence: ali.eghmazi@lassena.etsmtl.ca

Abstract: The Internet of Things (IoT) is a technology that can connect billions of devices or "things" to other devices (machine to machine) or even to people via an existing infrastructure. IoT applications in real-world scenarios include smart cities, smart houses, connected appliances, shipping, monitoring, smart supply chain management, and smart grids. As the number of devices all over the world is increasing (in all aspects of daily life), huge amounts of data are being produced as a result. New issues are therefore arising from the use and development of current technologies, regarding new applications, regulation, cloud computing, security, and privacy. The blockchain has shown promise in terms of securing and preserving the privacy of users and data, in a decentralized manner. In particular, Hyperledger Fabric v2.x is a new generation of blockchain that is open source and offers versatility, modularity, and performance. In this paper, a blockchain as a service (BaaS) application based on Hyperledger Fabric is presented to address the security and privacy challenges associated with the IoT. A new architecture is introduced to enable this integration, and is developed and deployed, and its performance is analyzed in real-world scenarios. We also propose a new data structure with encryption based on public and private keys for enhanced security and privacy.

Keywords: blockchain; IoT; enhanced data security; data privacy; encryption; hyperledger fabric

Citation: Eghmazi, A.; Ataei, M.; Landry, R.J.; Chevrette, G. Enhancing IoT Data Security: Using the Blockchain to Boost Data Integrity and Privacy. *IoT* **2024**, *5*, 20–34. https://doi.org/10.3390/iot5010002

Academic Editor: Amiya Nayak

Received: 10 November 2023
Revised: 2 January 2024
Accepted: 4 January 2024
Published: 10 January 2024

1. Introduction

The Internet of Things (IoT) has gained significant recognition and popularity since its inception as a network model by Ashton and Gamble in 1999. Its widespread adoption has been driven by the vast number of interconnected nodes, networks, and protocols that offer convenience and efficiency in various industries. However, the growing scale and complexity of the IoT ecosystem have raised significant security concerns [1,2].

In the IoT, physical objects are connected to enable them to exchange data, which then require analysis. Sensors in devices collect and store data in the cloud for examination, which both offer possibilities and pose problems, such as the difficulty of data extraction from devices with restricted capabilities. Privacy problems with the IoT have also emerged, and industries with academics are striving to overcome them [3]. The number of IoT-connected devices is expected to reach an astonishing number above 75 billion in the coming years, and this has intensified the urgency of addressing the associated security challenges [4].

At the core of the IoT ecosystem are fundamental elements such as sensors, computing nodes, receivers, actuators, and devices [5]. The IoT framework consists of several layers, each of which serves a distinct purpose: the business layer, the application layer, the middle layer, the network layer, and the physical/sensor layer [6].

These interconnected components work together to collect, process, and exchange data, thus enabling the seamless functioning of IoT systems. However, modern linked IoT systems encounter difficulties in terms of efficiently allocating their limited energy resources

while maintaining a strong focus on privacy and security. Although centralized security solutions are commonly deployed, they may not fully meet the unique requirements of IoT systems, leaving them vulnerable to potential threats [7].

Massive IoT refers to the potential scenario where networks support billions of connected devices and applications that interact at extremely high data rates, facilitating a major technological revolution with the implementation of diverse and advanced systems such as telepresence, virtual-reality devices, swarms of drones, autonomous driving, and biosensors. This extensive network of IoT devices, while enabling innovative services in many domains, also raises significant security concerns due to the vulnerability of devices and the importance of the information they carry, making protection against cyber threats a crucial challenge [8].

To overcome these limitations, one emerging approach involves integrating the IoT with cognitive environments by leveraging cognitive technologies such as artificial intelligence and machine learning to enhance the capabilities of intelligent devices. Through the incorporation of cognitive capabilities, IoT devices can adapt to changing environments, optimize energy consumption, and offer advanced functionalities. Furthermore, this integration enables users to remotely monitor and interact with their IoT networks, resulting in improved efficiency and effectiveness [9].

Ensuring safety and privacy via trust management is crucial [10]. In addition, in industries where asset tracking is necessary, data immutability becomes a major concern [11], particularly in IoT applications that involve direct interactions with humans. Examples of such applications include medical implants, smart gadgets, and autonomous cars, to name a few. It is essential to establish trust in order to promote confidence in these systems and to protect the privacy and safety of the user [12]. However, IoT networks face various security and privacy risks, including distributed denial of service (DDoS) attacks, privacy breaches, false data injection, and data integrity issues [1]. Previous researchers have proposed a limited range of solutions due to the lack of trust and transparency in data processing, which highlights the need for innovative approaches [13].

Research scientists Stuart Haber and W. Scott Stornetta pioneered the development of blockchain technology in 1991 [14]. In 2008, Satoshi Nakamoto introduced Bitcoin, a decentralized virtual currency that resolved data privacy issues in economic transactions. The blockchain, a distributed ledger offering security and transparency, has gained in popularity and has begun to serve diverse industries worldwide. It stores distributed records over a number of nodes, which allows users to access and verify transactions. Key functionalities include routing, storage, wallet services, mining, and recovery [11,15].

Blockchain technology, which was initially introduced as a means to prevent double-spending in digital currencies, has evolved to find applications in diverse fields such as the IoT, logistics, and healthcare [16]. The inherent benefits of the blockchain, including the immutability of append-only chained data, a decentralized and non-changeable ledger, the absence of third-party involvement, transparency, and cryptographic security, make it a promising solution to address the IoT security challenges described above [17,18].

Among the various types of blockchain frameworks, such as public, permissioned, permissionless, and private, Hyperledger Fabric stands out as an enterprise-grade solution. Hyperledger Fabric is a private and permissioned blockchain that offers modularity, scalability, and a flexible permission model and is suitable for IoT deployments. Unlike public blockchains, permissioned blockchains such as Hyperledger Fabric restrict content publication to selected nodes, where access is controlled by a third party that manages user privileges [19,20]. This makes Hyperledger Fabric an ideal choice for meeting the specific security and privacy requirements of IoT applications.

The authors of [21] introduced two new concepts:

1. The storage of sensor data off the blockchain, keeping only the sensor ID and the transaction details on a local blockchain.
2. The use of "RESET" transactions that move local blockchain data to free up storage and store the hash on the global blockchain (GB) for data integrity.

These concepts can be used to connect local blockchains to the GB, which ensures data integrity and has its own chaincode and policies. Overall, they can improve scalability and efficiency in terms of data storage and transaction management.

The authors of [22] discussed a system configuration that included a root server, Hyperledger Fabric, and multiple users. They outlined the registration and verification process for users as agents and highlighted the roles of different certificate authorities. Their system allowed for the creation and management of multiple groups, with periodic monitoring and agent changes for stability and security purposes.

The article in [23] introduced a new architecture that used blockchain technology to enable interactivity among IoT devices. This architecture had four blocks, consisting of the sensors, the web service, the Ethereum blockchain (ETH), and the users and administrators. This system was shown to operate successfully under various conditions, and the secure and efficient use of the blockchain was showcased. However, its drawbacks included a reliance on a private ETH blockchain with low transaction processing capacity, the high cost of implementation in a public ETH blockchain, and a lack of encryption, privacy, and security on the device side.

In [24], the authors focused on the integration of IoT systems with a private blockchain deployed on an ad-hoc IoT network. The choice of a private blockchain was motivated by its advantages, which include a lower node count and reduced power and resource consumption. The study described the establishment of an Ethereum-based private blockchain on top of the network, with each IoT device utilizing the Ethereum execution client (Geth client) to form a full blockchain connection with other nodes. This research aimed to assess the performance of an integrated IoT-private blockchain system, with a specific focus on the connections between the IoT devices and the underlying network.

In another article [25], the authors examined the benefits of utilizing off-chain data storage and conducted a comparative analysis of the associated gas costs in Ethereum (ETH) for each transaction executed with a smart contract deployed on the Ethereum blockchain. They highlighted the importance of pre-processing in the fog layer and described the process of creating data chunks, which was governed by policies set by the administrator. Users could access these chunks through the blockchain, and smart contracts were utilized for validation purposes. However, several drawbacks were identified, such as the use of the ETH blockchain, leading to a low TPS rate, and the absence of a specific data structure for managing data chunks.

The goal of this research is to improve the security and efficiency of the Massive Internet of Things (MIoT) by developing a cohesive, four-layered IoT blockchain infrastructure. This method combines IoT devices with Hyperledger Fabric, a private and permissioned blockchain, to provide a secure, decentralized ledger for data transfers. the aim is to optimize data processing and secure storage inside this framework, solving issues like latency by using proper chaincode through hyperledger fabric and scalability by adding an off-chain data structure. To analyze the system's scalability, security, and efficiency, we use data validation through trials in diverse IoT domains. This strategy represents a big step forward in solving the collective difficulties of MIoT security and data management.

In the next section, we focus on the connection between IoT devices and the blockchain. We explore the best four-layered architecture for IoT deployment and resolve the problems associated with performance and storing IoT data on the blockchain. In Section 3, we present the findings of the integration between the blockchain and the IoT platform, elucidating its implications and consequences in the context. Section 4 presents an in-depth assessment of the features of the proposed platform, highlighting its advantages and beneficial outcomes. In the final section, we summarize the most important results and conclusions of this study.

2. Materials and Methods

We developed a comprehensive four-layer architecture with the specific aim of establishing connectivity between various IoT devices and end users. This architecture can

provide a robust and efficient framework for integrating IoT devices into everyday applications. In this simplified overview, we consider a wide range of such IoT devices, including sensors, cars, smart city infrastructure, and even sensors from aircraft.

Table 1 briefly outlines the four essential layers of an Internet of Things (IoT) architecture, ranging from physical IoT devices and sensors at the first layer, through network protocols, and data processing, up to end-user applications at the fourth layer. Each level plays a vital role in ensuring integration and functionality within the IoT ecosystem.

Table 1. Proposed four-layered architecture.

Layer	Examples
Fourth layer (application/ end-user layer)	Smart home applications, industrial control systems, healthcare applications, asset tracking and management systems
Third layer (middle layer)	Data storage, data management, data processing
Second layer (network layer)	WI-FI, Bluetooth, Zigbee, LoraWAN, cellular networks (3G, 4G, 5G)
First layer (physical layer/ IoT device)	Temperature sensors, humidity sensors, light sensors, air quality sensors, smart door locks, vehicles, aircraft

Figure 1 provides a comprehensive illustration of the four-layer architecture, detailing the various technologies utilized to ensure its complete functionality.

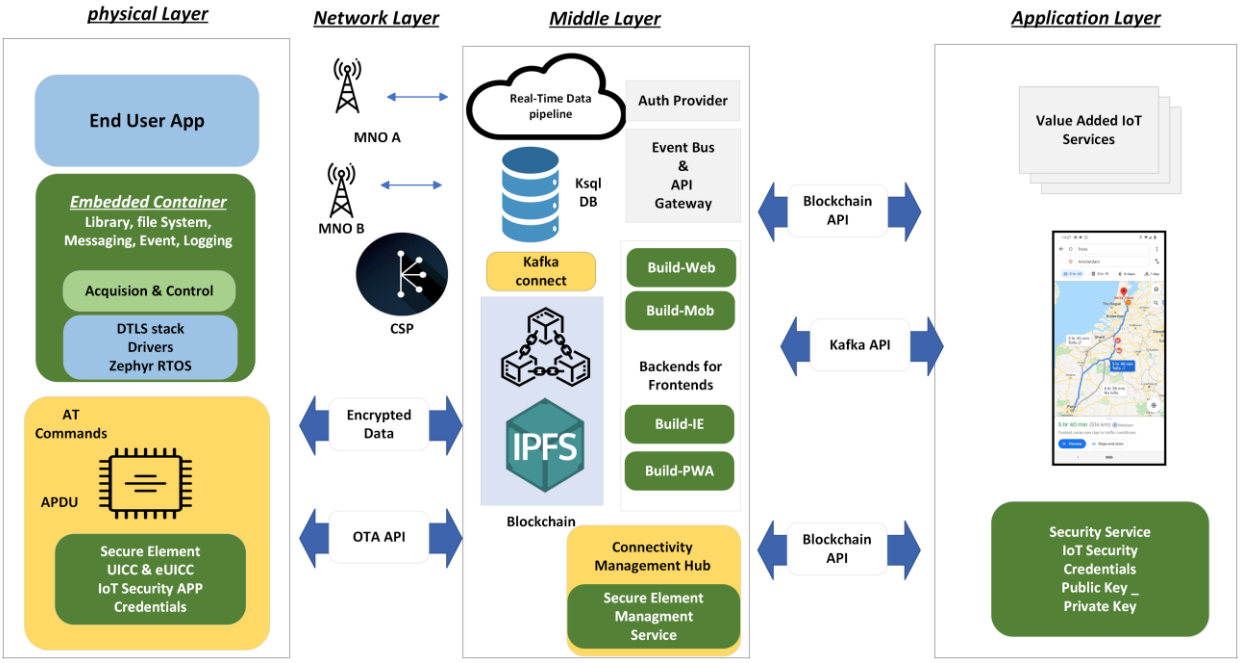

Figure 1. Structure of the proposed four-layered architecture.

2.1. First Layer (Physical Layer)

The physical layer in an IoT architecture involves a wide range of devices that enable the collection and sensing of data. In our specific implementation, we utilized the Laird connectivity device combined with Nordic RF Silicon, the BL654 model as the sensor. For the gateway functionality, we used the Pinnacle™ 100 DVK, devices from Laird Connectivity manufacturing company in Akron, OH, USA, which is equipped with a SIM card for connectivity.

To facilitate data transmission within the physical layer, we employed Bluetooth technology as the communication protocol. This allowed the sensors, represented by the BL654 model, to send their data efficiently to the Pinnacle™ 100 DVK.

Table 2 provides a comparative analysis of devices considered for gateway purposes. We selected the Pinnacle™ 100 DVK due to its low power consumption, inherent cellular connectivity, and additional features.

Table 2. Comparison of devices used as gateways [26–28].

Features	Raspberry Pi 4 Model B	Pinnacle™ 100 DVK	Arduino Uno
Power consumption	2.3 W (off)/3.3 W (idle)	Power Save Mode (PSM), eDRX, BLE–TX, low power consumption	N/A [1]
Processor	Broadcom BCM2711, ARM Cortex-A72 (64-bit)	Silicon Labs EFR32MG21, ARM Cortex-M4F (32-bit)	Microchip ATmega328P
Cellular connectivity	Not natively included	LTE-M/NB-IoT, release 13 GPP	N/A
Clock speed	1.5 GHz	64 MHz (Cortex-M4F)	16 MHz
RAM	Up to 8 GB	256 KB	2 KB
Storage	MicroSD card slot	1 MB internal flash	None (external storage required)
Performance	Higher processing power and capabilities	Optimized for low-power and IoT applications	Limited processing power and memory
Purpose	General-purpose computing and prototyping	IoT-specific applications and projects	General-purpose prototyping and embedded systems

[1] Not Available.

At this layer, we considered three specific types of sensors: humidity, pressure, and temperature; however, it is important to note that the versatility of IoT systems enables the integration of various other types of sensors depending on the specific requirements of the application. This flexibility allows for the incorporation of a diverse range of sensor technologies that can cater to a wide array of use cases and scenarios. Figure 2 The Pinnacle™ 100 is prominently featured on the left side, offering a sharp and detailed visual portrayal. Concurrently, the BL654 sensors are presented on the right side of the image.

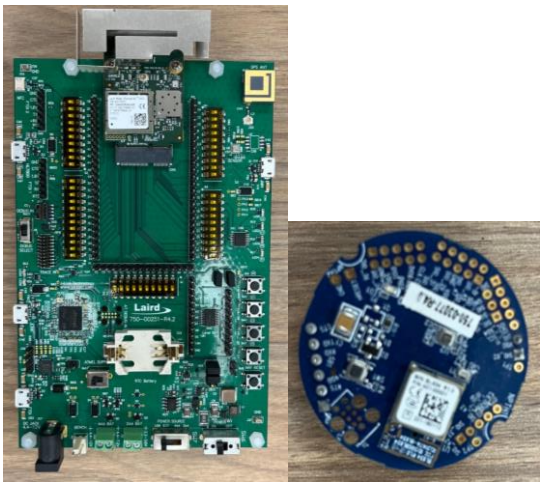

Figure 2. A Pinnacle™ 100 DVK on the left side and a BL654 sensor on the right side.

2.2. Second Layer (Network Layer)

The network layer plays a crucial role in facilitating the transfer of data from the first layer (IoT devices) to the third layer (middle layer). It serves as the communication bridge

between these layers, and various technologies can be employed to ensure efficient and reliable data transmission.

In our experimental setup presented in Figure 3, the second-generation Nutaq PicoLTE was used as a software-defined radio-network-in-a-box. This served as a versatile and powerful simulator, allowing us to create and emulate an LTE-based network environment for our IoT experiments, and facilitating the simulation and evaluation of the proposed IoT system. The Nutaq PicoLTE also allowed for the configuration and customization of various network parameters, such as signal strength, bandwidth, and interference, meaning that we could mimic real-world network conditions.

Figure 3. The PicoLTE setup with LTE antennas.

One notable aspect of our experiment was the use of LTE-M technology for data transmission from the IoT devices to the third layer, which served as the access network. This offered efficient and reliable connectivity for IoT devices, enabling them to transmit data over long distances while consuming minimal power. Table 3 shows a few characteristics and supporting features of the Nutaq PicoLTE.

Table 3. Distinctive features offered by the Nutaq PicoLTE.

	FDD/TDD Support	**Bandwidth Support (MHZ)**	**eDRX Support**	**PSM Support**	**IP Version**	**NB-IoT Support**
LTEENB	Yes	1.4, 3, 5, 10, 15, 20	Yes	No	IPv4/v6	NB1 UE
LTEMME	No	2	Yes	Yes	Ipv4/v6	NB-S1 UE
LTEUE	Yes	1.4, 3, 5, 10, 15, 20	Yes	Yes	Ipv4	NB 1 multi-tone

2.3. Third Layer (Middle Layer)

In the proposed architecture, the middle layer is responsible for handling and processing the data generated by the IoT devices. This layer will monitor and handle activities such as data storage, administration, and processing. Data storage enables the effective organization and retrieval of enormous volumes of IoT data, whereas data administration includes the management of data input, translation, and aggregation while ensuring data quality and dependability. Data processing entails leveraging technologies to execute activities such as analytics, machine learning, and real-time decision-making. The middle layer enables the smooth integration and use of IoT data for a variety of applications.

In this layer, it is proposed to use Kafka which would play a pivotal role as a powerful real-time data streaming pipeline for smooth data transfer to the blockchain. Kafka's capabilities were leveraged to ensure that the data generated by the IoT devices were efficiently collected and effortlessly transmitted to the blockchain network.

The blockchain, which resides in this layer along with the database, serves as a decentralized and secure ledger. It ensures the integrity and immutability of the data by storing hashed representations of the transmitted information. We employed an off-chain storage solution, with just the hash of this data maintained on the Hyperledger Fabric blockchain. This method dramatically decreases ledger size while retaining the blockchain network's efficiency and speed. We assure data integrity and speedy verification processes, since the on-chain hash may be used to authenticate the validity of the whole data stored off-chain. Using Hyperledger Fabric's features, such as private channels and chaincode, enables greater optimization and control over data management, resulting in a balanced and efficient system that adheres to security and decentralization principles.

In the specific implementation described here, the InterPlanetary File System (IPFS) was chosen as the database solution. IPFS offers a distributed and decentralized storage system that complements the characteristics of the blockchain. However, it is important to note that other proprietary databases such as MongoDB and MySQL could also be used within this layer, depending on the specific requirements and preferences.

Apache Kafka acts as a bridge, receiving data from devices and efficiently transmitting it through the pipeline to the database. We use a smart data transformation strategy to manage the massive data volumes generated by IoT sensors. We start by collecting raw data from sensors, which are typically vast in volume. This raw data is subsequently processed, resulting in a considerable reduction in bulk. Finally, we produce the collected data into usable insights, minimizing data quantity while maximizing value. This simplified technique assures efficient storage, rapid data access, and relevant results, successfully overcoming the issues of handling enormous data volumes.

Figure 4 provides a visual representation of the various data types being stored and illustrates the corresponding volume of data at each stage.

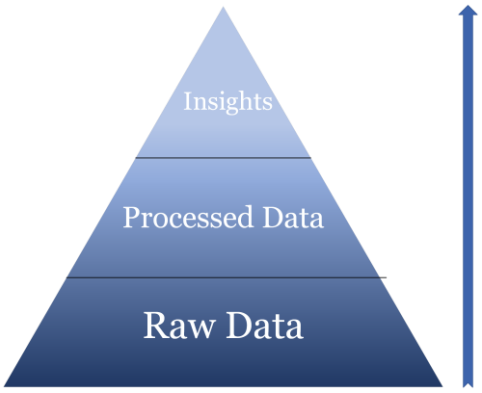

Figure 4. Types of data can be collected and stored.

2.4. Fourth Layer (Application Layer)

In the IoT architecture, the responsibility of the application layer includes data visualization and processing, as well as supporting firmware upgrades. In a smart device ecosystem, for example, the application layer may analyze sensor data, produce visual representations of the performance of devices, and provide a user interface for initiating firmware upgrades. Firmware upgrades guarantee that devices are equipped with the most recent features, security fixes, and performance enhancements. Users can easily upgrade firmware via the application interface, allowing for smooth device maintenance and feature enhancement. In the IoT ecosystem, the application layer therefore helps with both data visualization and firmware management.

User authentication is essential in this layer to enable communication with the blockchain with the proper data owner. A two-layer authentication mechanism was used in this case to ensure safe access. The first layer handles initial user authentication, which can securely store user profiles and information such as usernames, passwords, email addresses, etc.

The second layer relied on the blockchain's built-in authentication procedures. It has been specifically designed to interact with the blockchain. After the user's credentials have been verified by the first layer, the process advances to the second layer, which has the responsibility to handle any requests from the blockchain. The built-in authentication method included in our platform makes use of JSON Web Tokens (JWTs), which are produced securely utilizing a pair of public and private keys. These keys are created randomly, resulting in a secure and distinct key for each instance. The length of the phrase in our deployment varies from 13 to 17 words, providing enough complexity and security.

Each user is given a unique phrase to get their own keys, ensuring a safe and personalized experience. This method is critical to the operation of our crypto wallet. We took the effort to create our own wallet, which has been rigorously built to store and preserve these sensitive credentials, assuring the secure storage of user credentials. To authenticate the user's identity, both layers can execute authentication. The type of data shown to the user is governed by their unique requirements and access credentials.

This layer acts as the user interface for communicating with the blockchain, letting users submit and receive requests. The data are visualized on a web page to create a more user-friendly experience, fully secured, decentralized and immutable.

2.5. Data Flow in the Proposed Architecture

In this section, we will discuss the data flow through the deployed massive IoT platform.

Each user was assigned a unique public and private key, and RSA 2048-bit encryption which is a robust encryption standard that ensures the security of the key pairs used. For each public-private key pair, we used a JSON Web Token (JWT) with RSA-based encryption that can be verified by parties who have access to the public key, ensuring the authenticity of the token. The Hyperledger-Fabric Software Development Kit (SDK) was employed to validate the JWT to ascertain the integrity of the data.

We developed a specialized data flow procedure that consisted of multiple phases to assist in the secure and quick transfer of data from each sensor to the blockchain. The data from all sensors of each user were then converted into larger blocks containing many bits of information, such as the time of creation of the block, the processed data, and the IPFS Content IDentifier (CID) of previously inserted blocks to IPFS.

In the proposed scheme, each block is connected to the CID of the preceding block added to the IPFS, in order to guarantee the consistency and security of the data, and the first block (or 'genesis block') is given a CID of zero. This procedure helps to maintain the sequential order of the data and ensures that any changes or efforts to alter the data are readily discernible. Figure 5 illustrates how data blocks are interconnected in a chain, enhancing their immutability, and details the contents of each block.

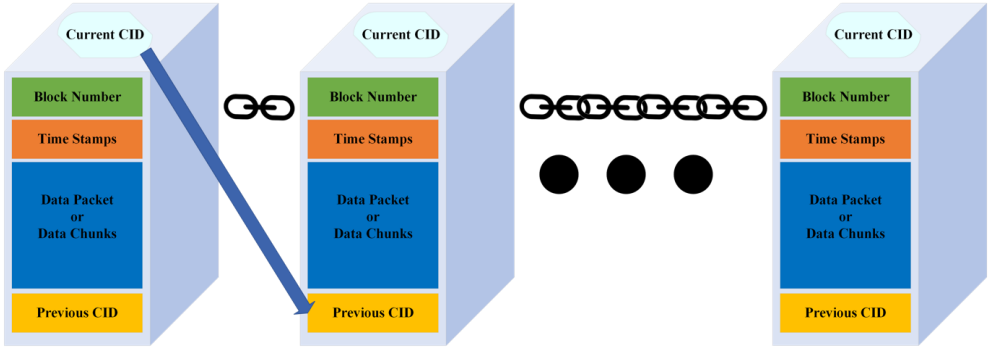

Figure 5. The data structure used for storage in IPFS.

This creates a unique information chain for each user. Users may have several gateways and sensors associated with these gateways, each with their own information chain. Notably, this chain is stored separately from the main blockchain on IPFS. The CID of each

block, on the other hand, is stored on the blockchain, connecting the two systems. Figure 6 shows every user maintains an individual chain, which is accountable for managing data originating from that specific user.

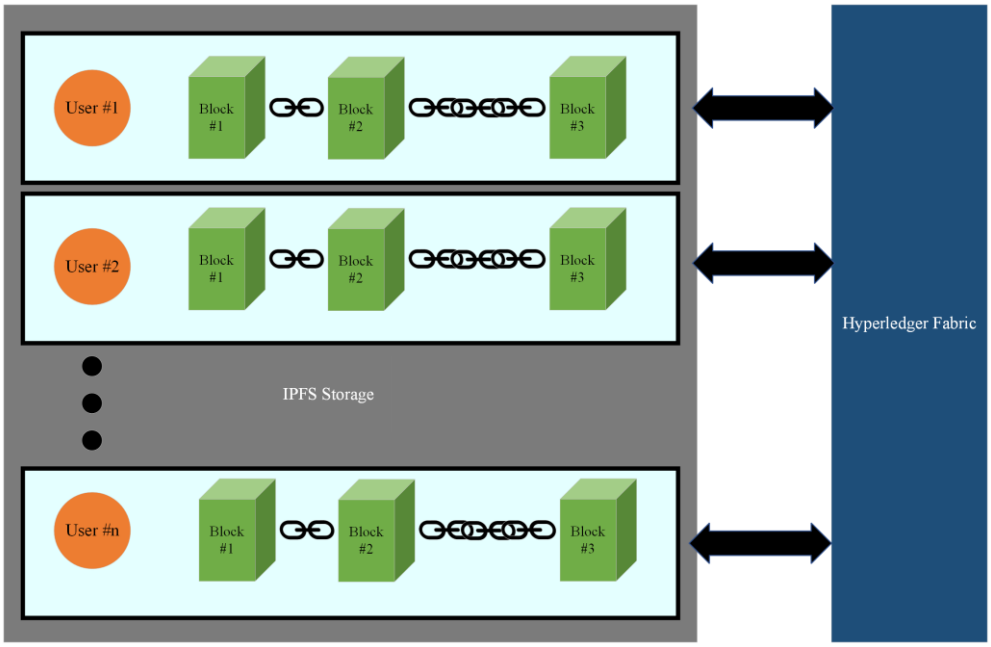

Figure 6. How data is chained and connected to the blockchain in IPFS.

Once the blocks have been produced and contain all the required information, they are sent to IPFS for storage. The data are then given a distinct CID with a length of 53 characters, which remains unaffected by the volume of the data. This CID acts as a permanent record of the data as it appeared at the time, allowing it to be readily traced and accessed. Here's a sample CID: Qmbt153PLWidJEv2PBMHDiLLBxQo3N14MbagEveQnK5EM5ZYv1. Each block of data possesses the capacity to incorporate readings from numerous sensors. The dimension of the data is directly proportional to the congestion observed within the network. Figure 7 depicts real-world scenarios. In this example, the quantity of collected data is 2.

```
parsedData                                                    HistoryPinnacle.js:38
▼ (5) ['Block-Number: 19', '2023-08-30, 4:20:00 p.m.', {…}, {…}, 'Previous-Hash: QmdGy5NFUjw6BBE722seaswYN9S93rTSU1U
  waeEBArPRM5'] i
    0: "Block-Number: 19"
    1: "2023-08-30, 4:20:00 p.m."
  ▶ 2: {sensorID: 'sensor2', value: {…}, name: '2023-08-30, 4:20:00 p.m.'}
  ▶ 3: {sensorID: 'sensor2', value: {…}, name: '2023-08-30, 4:20:00 p.m.'}
    4: "Previous-Hash: QmdGy5NFUjw6BBE722seaswYN9S93rTSU1UwaeEBArPRM5"
```

Figure 7. Example of data block in real-world scenarios.

Finally, the entire CID is transmitted to the blockchain, which allows for efficient and safe contact between devices. This data structure allows us to operate independently of the number of users; it scales efficiently, focusing solely on the users' count. We encrypt the data throughout the entire transfer using the provided public and private keys for each of the entries. This ensures the privacy of the data and allows us to verify its integrity.

Overall, this flexible data storage, which we may alter relying on the scenario and the congestion of the network, also the transmission mechanism provides a secure and fast transfer of data from sensors to the blockchain. This guarantees the security, anonymity, and accessibility of data, maintains the network's scalability, and helps us to handle large volumes of data or massive IoT devices.

3. Experiment, Results and Analysis

In this section, we present the results from the performance evaluation of the proposed Massive IoT architecture using our blockchain and chain code. To assess these aspects, we use Hyperledger Caliper (https://hyperledger.github.io/caliper/ accessed on 5 September 2023), a reliable benchmarking tool that was designed to measure the efficiency of blockchain implementations using a predefined set of use cases.

Hyperledger Fabric's performance is closely tied to the hardware utilized. Enhanced equipment typically yields improved outcomes. For the purposes of this experiment, we utilized a MacBook Pro featuring an M2 Pro chip, detailed by the following specifications:

- CPU: Apple M2 Pro chip (10-core).
- RAM: 16 GB unified memory.
- Storage: 512 GB.

Hyperledger Caliper operates through worker processes, each of which is responsible for generating the workload independently of the others. This design allows for efficient workload generation, even if a particular worker process reaches the capacity limit of its host machine. By employing multiple worker processes across various machines, we can further enhance Caliper's scalability and overall workload rate.

The architecture has been designed to be independent of the number of devices, focusing instead on the number of users. This means that each transaction is associated with a user, who may have multiple devices linked to their account.

Figures 8 and 9 show that the throughput ranges from 366.4 TPS to a peak of 798.3 TPS. As the TPS increases, there is a corresponding rise in the transaction failure rate, which reaches 7% when the number of workers is increased to 20 and the network is handling 20,000 transactions.

To address this challenge, we can leverage the advantages of the data structure proposed earlier. By regularly monitoring the performance over time, we can dynamically adjust and optimize the data size within our data structure. This approach aims to strike a balance between the throughput and transaction success rates, thereby ensuring more stable and efficient overall performance.

Figure 8. Transaction throughput (TPS) of hyperledger-fabric.

Figures 10–12 show the latency of Hyperledger Fabric, which is divided into minimum, average, and maximum values. Minimum latency displays the network's best efficiency, maximum latency determines imaginable congestion, and average latency provides a balanced perspective of general performance, administering in thorough Hyperledger Fabric performance examination and optimization.

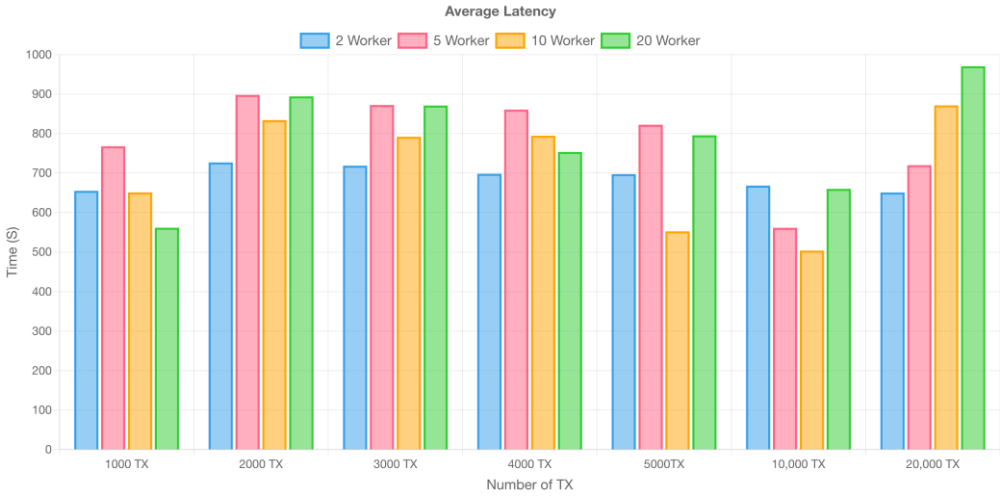

Figure 9. Inquiry performance of hyperledger-fabric.

Figures 13 and 14 show the resource utilization during a single round of transactions performed by Hyperledger Caliper. The graphs allow for critical insights into CPU and memory usage. These metrics offer a comprehensive view of how efficiently the system manages its resources during transactional activity.

As transaction volumes grow, we witness an increase in CPU and RAM usage, with the CPU undergoing a significant pinpoint. This pattern implies that higher transaction volumes set a powerful pressure on the CPU, potentially endangering system overload and performance issues. To ensure smooth operations, it is important to regularly monitor and optimize system resources, adopting a proactive approach to system maintenance. By doing so, we can actually manage CPU usage and maintain stable performance, even as transaction requests increase, potentially exploring scaling solutions to accommodate the increasing load gracefully.

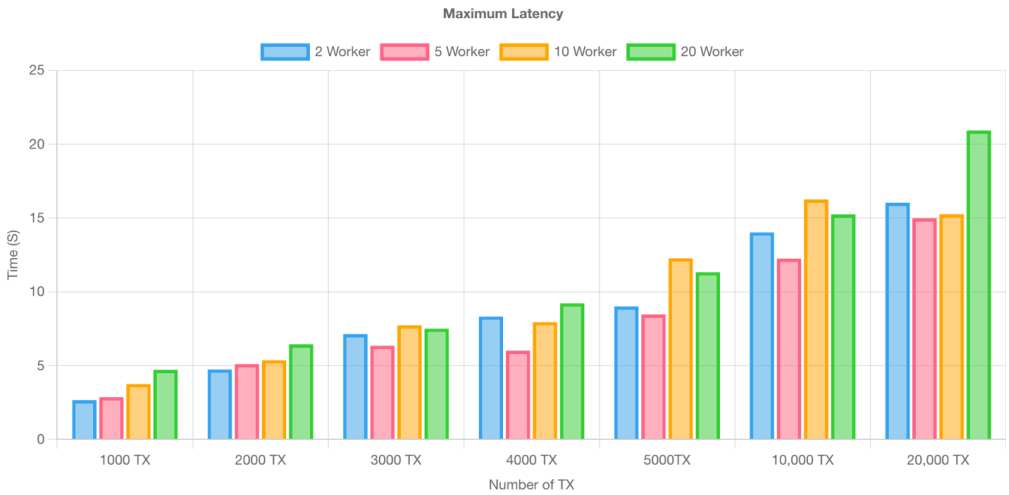

Figure 10. Maximum latency of transactions in hyperledger fabric.

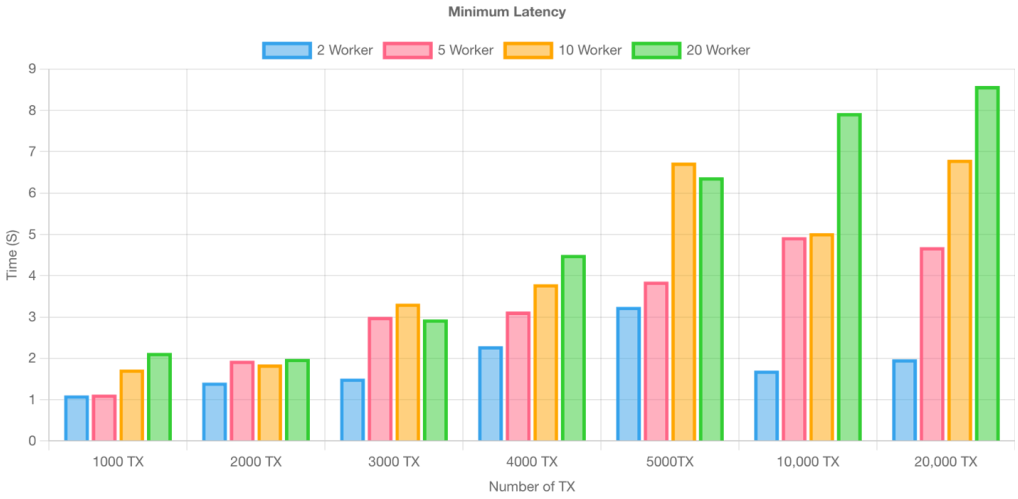

Figure 11. Minimum latency of transactions in hyperledger fabric.

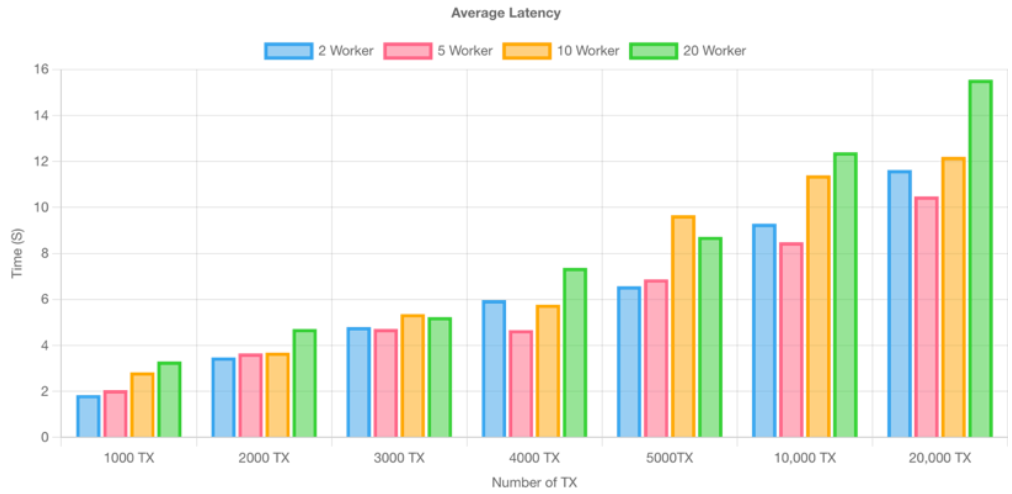

Figure 12. Average latency of transactions in hyperledger fabric.

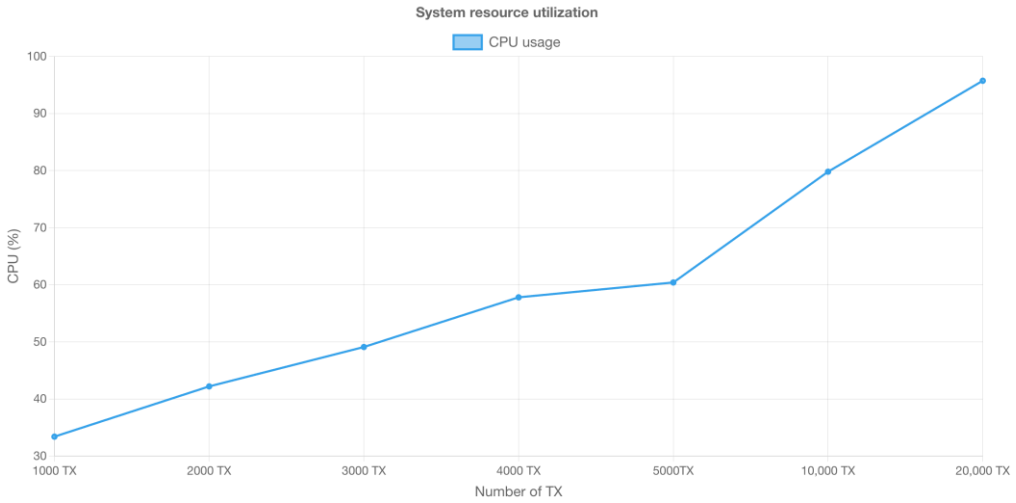

Figure 13. CPU usage.

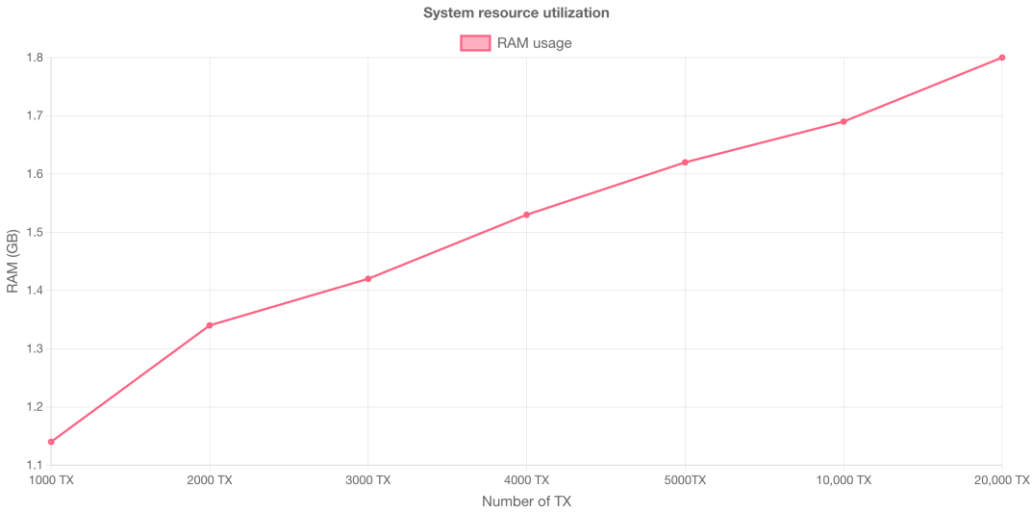

Figure 14. RAM usage.

4. Discussion

In this section, we will explore the numerous benefits and advantages of implementing our proposed architecture, which enable organizations to unlock a range of valuable outcomes and enhance their overall operations.

- **Security:** Robust security measures are implemented through multiple layers of authentication. The first layer handles user authentication, while a public and private key mechanism generates a JWT (JSON Web Token), thus fortifying the security of the blockchain. One of the most notable features of blockchain is its inherent security mechanism. Moreover, Hyperledger Fabric, as a private permissioned blockchain, can establish trust within the community utilizing the platform.
- **Integrity:** The blockchain serves as an immutable ledger, which can ensure data integrity. Once data are recorded on the blockchain, they become tamper-proof and are virtually impossible to alter or modify. By applying encryption throughout the entire process, we can ensure the integrity and privacy of the data.
- **Privacy:** User privacy is protected through data encryption. Only users with the corresponding private keys can decrypt and access the data, thus ensuring its confidentiality. Sensitive user data remains safeguarded from unauthorized access or viewing.
- **Access control:** Administrators have the authority to manage and access the analysis and insights derived from the data. Controlled access allows administrators to monitor and make informed decisions based on the analyzed data while preserving user privacy.
- **Scalability:** Hyperledger Fabric, our chosen framework, offers exceptional scalability with a high number of transactions per second. Our innovative data structure also enables efficient management of the platform's performance. The data block volume can be dynamically adjusted to adapt to changing requirements, thereby ensuring optimal scalability.
- **Data preservation:** By leveraging Kafka's built-in database functionality, the platform can retain data for as long as necessary. Even if there is a temporary increase in the latency of the blockchain, the data are preserved within Kafka's database until they can be securely sent to the blockchain. No data are lost or destroyed, thus ensuring comprehensive data retention and reliability.

5. Conclusions

This paper has presented a novel database-based blockchain using Hyperledger Fabric, with a four-layer architecture, which can effectively address data security and privacy concerns. The integration of Kafka as a streaming pipeline also gives enhanced overall

system performance, and the introduction of a new flexible data structure has been shown to be instrumental in improving the efficiency of the platform.

We have successfully linked an enormous amount of IoT devices with blockchain technology, creating a data structure that allows the platform to scale regardless of sensor count. Instead, scalability is directly related to the quantity of users. We have 20,000 registered users on the platform thus far. Despite current numbers indicating a high level of resource consumption, the platform retains solid security, ensuring good device management and monitoring. Our findings suggest that our solution, which employs advanced architectures and data formats, effectively addresses Hyperledger Fabric's scaling difficulties. This integration represents a significant advancement in the development of secure and scalable IoT blockchain networks, and it contributes to greater scholarly conversation on this subject.

In the next phase of this study, we will focus on building an algorithm that allows for easy performance verification and dynamic modifications to the volume of data that is saved and communicated between the database and the blockchain. This dynamic adaptability is essential for maintaining high performance and ensuring the long-term success of the system.

We predict that by applying this technique, we will be able to achieve even higher levels of efficiency, scalability, and reliability in database operations, thereby opening new opportunities for real use cases in a variety of sectors. Our findings have the potential to significantly enhance the field of blockchain-based databases and pave the way for future advances in safeguarding sensitive data and improving system performance.

Author Contributions: Conceptualization, A.E.; Methodology, A.E.; Software, A.E.; Validation, R.J.L. and G.C.; Investigation, A.E.; Resources, R.J.L.; Data curation, A.E. and M.A.; Writing—original draft, A.E.; Writing—review & editing, A.E., M.A. and R.J.L.; Visualization, A.E.; Supervision, R.J.L. and G.C.; Project administration, R.J.L. and G.C. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The data presented in this study are available on request from the corresponding author. The data are not publicly available due to confidentiality issues.

Conflicts of Interest: The funding sponsors had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, and in the decision to publish the results.

References

1. Verma, G.; Prakash, S. Emerging Security Threats, Countermeasures, Issues, and Future Aspects on the Internet of Things (IoT): A Systematic Literature Review. In *Advances in Interdisciplinary Engineering*; Kumar, N., Tibor, S., Sindhwani, R., Lee, J., Srivastava, P., Eds.; Lecture Notes in Mechanical Engineering; Springer: Singapore, 2021; pp. 59–66. [CrossRef]
2. Patnaik, R.; Padhy, N.; Raju, K.S. A Systematic Survey on IoT Security Issues, Vulnerability and Open Challenges. In *Intelligent System Design*; Satapathy, S.C., Bhateja, V., Janakiramaiah, B., Chen, Y.-W., Eds.; Advances in Intelligent Systems and Computing; Springer: Singapore, 2021; pp. 723–730. [CrossRef]
3. Roy, R.; Dheeba, J. Survey on Methodological Model of IoT in Digital Forensic. In Proceedings of the 2023 International Conference on Intelligent Systems, Advanced Computing and Communication (ISACC), Silchar, India, 3–4 February 2023; IEEE: Piscataway, NJ, USA, 2023; pp. 1–6. [CrossRef]
4. Suny, M.F.I.; Fahim, M.M.R.; Rahman, M.; Newaz, N.T.; Akhund, T.M.N.U. IoT Past, Present, and Future a Literary Survey. In *Proceedings of the Information and Communication Technology for Competitive Strategies (ICTCS 2020)*; Jaipur, India, 11–12 December 2020, Kaiser, M.S., Xie, J., Rathore, V.S., Eds.; Lecture Notes in Networks and Systems; Springer Nature: Singapore, 2021; pp. 393–402. [CrossRef]
5. Miraz, M.H.; Ali, M. Blockchain Enabled Enhanced IoT Ecosystem Security. In *Emerging Technologies in Computing*; Miraz, M.H., Excell, P., Ware, A., Soomro, S., Ali, M., Eds.; Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering; Springer International Publishing: Cham, Switzerland, 2018; pp. 38–46. [CrossRef]
6. Zhonghua, C.; Goyal, S.B. Blockchain-Based Framework to Handle Security and Privacy for IoT System. In Proceedings of the Third Doctoral Symposium on Computational Intelligence, Lucknow, India, 5 March 2022; Khanna, A., Gupta, D., Kansal, V., Fortino, G., Hassanien, A.E., Eds.; Lecture Notes in Networks and Systems. Springer Nature: Singapore, 2023; pp. 71–82. [CrossRef]

7. Anaam, E.; Hasan, M.K.; Ghazal, T.M.; Haw, S.-C.; Alzoubi, H.M.; Alshurideh, M.T. How Private Blockchain Technology Secure IoT Data Record. In Proceedings of the 2023 IEEE 2nd International Conference on AI in Cybersecurity (ICAIC), Houston, TX, USA, 7–9 February 2023; IEEE: Piscataway, NJ, USA, 2023; pp. 1–6. [CrossRef]
8. Alotaibi, A.; Barnawi, A. Securing massive IoT in 6G: Recent solutions, architectures, future directions. *Internet Things* **2023**, *22*, 100715. [CrossRef]
9. Alenizi, A.S.; Al-Karawi, K.A. Internet of Things (IoT) Adoption: Challenges and Barriers. In Proceedings of the Seventh International Congress on Information and Communication Technology, London, UK, 21–24 February 2022; Yang, X.-S., Sherratt, S., Dey, N., Joshi, A., Eds.; Lecture Notes in Networks and Systems. Springer Nature: Singapore, 2023; pp. 217–229. [CrossRef]
10. Dongre, N.; Atique, M.; Shaik, Z.A.; Raut, A.D. A Survey on Security Issues and Secure Frameworks in Internet of Things (IoT). In Proceedings of the 2022 4th International Conference on Smart Systems and Inventive Technology (ICSSIT), Tirunelveli, India, 20–22 January 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 173–181. [CrossRef]
11. Singh, C.; Chauhan, D. IoT–Blockchain Integration-Based Applications Challenges and Opportunities. In *Mobile Radio Communications and 5G Networks*; Marriwala, N., Tripathi, C.C., Kumar, D., Jain, S., Eds.; Lecture Notes in Networks and Systems; Springer: Singapore, 2021; pp. 87–116. [CrossRef]
12. Puschner, E.; Paar, C. Security Analysis of IoT Devices: From the system level to the logic level. *IEEE Solid-State Circuits Mag.* **2023**, *15*, 32–37. [CrossRef]
13. Xu, X.; Wang, X.; Li, Z.; Yu, H.; Sun, G.; Maharjan, S.; Zhang, Y. Mitigating Conflicting Transactions in Hyperledger Fabric-Permissioned Blockchain for Delay-Sensitive IoT Applications. *IEEE Internet Things J.* **2021**, *8*, 10596–10607. [CrossRef]
14. Zambre, P.; Panchal, M.; Chauhan, A. A Future to the Blockchain Technology and Its Concepts. In *ICT with Intelligent Applications*; Choudrie, J., Mahalle, P., Perumal, T., Joshi, A., Eds.; Smart Innovation, Systems and Technologies; Springer Nature: Singapore, 2023; pp. 111–122. [CrossRef]
15. Chaudhry, U.B.; Hydros, A.K.M. Zero-trust-based security model against data breaches in the banking sector: A blockchain consensus algorithm. *IET Blockchain* **2023**, *3*, 98–115. [CrossRef]
16. Nayancy; Dutta, S.; Chakraborty, S. IoT-Based Secure Communication to Enhance Blockchain Model. In Proceedings of the Fourth International Conference on Microelectronics, Computing and Communication Systems, Ranchi, India, 11–12 May 2019; Nath, V., Mandal, J.K., Eds.; Lecture Notes in Electrical Engineering. Springer: Singapore, 2021; pp. 255–264. [CrossRef]
17. Bettayeb, M.; Nasir, Q.; Talib, M.A. Hyperledger-Based Secure Firmware Update Delivery for IoT Devices. In Proceedings of the ArabWIC 2021: The 7th Annual International Conference on Arab Women in Computing in Conjunction with the 2nd Forum of Women in Research, Sharjah, United Arab Emirates, 25–26 August 2021; ACM: Sharjah, United Arab Emirates, 2021; pp. 1–5. [CrossRef]
18. Blasch, E.; Xu, R.; Chen, Y.; Chen, G.; Shen, D. Blockchain Methods for Trusted Avionics Systems. *arXiv* **2019**, arXiv:1910.10638.
19. Sarmah, S.S. Understanding Blockchain Technology. *Comput. Sci. Eng.* **2018**, *82*, 23–29.
20. Clementi, M.D.; Larrieu, N.; Lochin, E.; Kaafar, M.A.; Asghar, H. When Air Traffic Management Meets Blockchain Technology: A Blockchain-based concept for securing the sharing of Flight Data. In Proceedings of the 2019 IEEE/AIAA 38th Digital Avionics Systems Conference (DASC), San Diego, CA, USA, 8–12 September 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1–10. [CrossRef]
21. Oikonomou, F.P.; Ribeiro, J.; Mantas, G.; Bastos, J.M.C.S.; Rodriguez, J. A Hyperledger Fabric-based Blockchain Architecture to Secure IoT-based Health Monitoring Systems. In Proceedings of the 2021 IEEE International Mediterranean Conference on Communications and Networking (MeditCom), Athens, Greece, 7–10 September 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 186–190. [CrossRef]
22. Maeng, J.; Heo, Y.; Joe, I. Hyperledger Fabric-Based Lightweight Group Management (H-LGM) for IoT Devices. *IEEE Access* **2022**, *10*, 56401–56409. [CrossRef]
23. Al-Zoubi, A.; Saadeddin, T.; Dmour, M.; Adi, L. An Interactive IoT-Blockchain System for Big Data Management. In Proceedings of the 2022 4th IEEE Middle East and North Africa Communications Conference (MENACOMM), Amman, Jordan, 6–8 December 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 71–76. [CrossRef]
24. Su, Y.; Nguyen, K.; Sekiya, H. Latency Evaluation in Ad-hoc IoT-Blockchain Network. In Proceedings of the 2022 5th World Symposium on Communication Engineering (WSCE), Nagoya, Japan, 16–18 September 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 124–128. [CrossRef]
25. Dange, S.; Nitnaware, P. Secure Share: Optimal Blokchain Integration in IoT Systems. *J. Comput. Inf. Syst. Apr.* **2023**, *8*, 1–13. [CrossRef]
26. Coelho, P.; Bessa, C.; Landeck, J.; Silva, C. The Potential of Low-Power, Cost-Effective Single Board Computers for Manufacturing Scheduling. *Procedia Comput. Sci.* **2023**, *217*, 904–911. [CrossRef]
27. Pinnacle^{TM} 100 Cellular LTE-M/NB-IoT/Bluetooth 5 Modem. Laird Connectivity. Available online: https://www.lairdconnect.com/wireless-modules/cellular-solutions/pinnacle-100-cellular-lte-m-nb-iot-bluetooth-5-modem (accessed on 20 July 2023).
28. Arduino/Genuino Zero—Zephyr Project Documentation. Available online: https://developer.nordicsemi.com/nRF_Connect_SDK/doc/1.4.99-dev1/zephyr/boards/arm/arduino_zero/doc/index.html (accessed on 20 July 2023).