information

Article

IoTBChain: Adopting Blockchain Technology to Increase PLC Resilience in an IoT Environment

Philipp Schmid, Alisa Schaffhäuser and Rasha Kashef *

Department of Electrical, Computer, and Biomedical Engineering, Toronto Metropolitan University, Toronto, ON M5B 2K3, Canada
* Correspondence: rkashef@torontomu.ca

Abstract: The networks on a centralized cloud architecture that interconnect Internet of Things (IoT) gadgets are not limited by national or jurisdictional borders. To ensure the secure sharing of sensitive user data among IoT gadgets, it is imperative to maintain security, resilience and trustless authentication. As a result, blockchain technology has become a viable option to provide such noteworthy characteristics. Blockchain technology is foundational for resolving many IoT security and privacy issues. Blockchain's safe decentralization can solve the IoT ecosystem's security, authentication and maintenance constraints. However, blockchain, like any innovation, has drawbacks, mainly when used in crucial IoT systems such as programmable logic controller (PLC) networks. This paper addresses the most recent security and privacy issues relating to the IoT, including the perception, network and application layers of the IoT's tiered architecture. The key focus is to review the existing IoT security and privacy concerns and how blockchain might be used to deal with these problems. This paper proposes a novel approach focusing on IoT capabilities and PLC device security. The new model will incorporate a proof-of-work-based blockchain into the (PLC) IoT ecosystem. This blockchain enables the transmission of binary data and the data logging of the (PLC) networks' signals. This novel technique uses fewer resources than other sophisticated methods in that PLC devices communicate data while maintaining a high transmission, encryption and decoding speed. In addition to ensuring repeatability, our new model addresses the memory and tracing problems that different PLC manufacturers encounter.

Keywords: blockchain; IoT; PLC; hashing; man-in-the-middle attack

Citation: Schmid, P.; Schaffhäuser, A.; Kashef, R. IoTBChain: Adopting Blockchain Technology to Increase PLC Resilience in an IoT Environment. *Information* **2023**, *14*, 437. https://doi.org/10.3390/info14080437

Academic Editors: Soumya Banerjee and Samia Bouzefrane

Received: 26 February 2023
Revised: 24 July 2023
Accepted: 27 July 2023
Published: 2 August 2023

1. Introduction

The Internet of Things (IoT) is a network that has found large-scale use in several applications that forego human interference. Given the significant improvements in wireless sensor networks (WSN), it provides a common operating picture (COP) through links between humans and machines or between machines [1]. The rising number of IoT smart objects linked to the Internet will communicate vast amounts of information to make people's lives more convenient [2,3]. These intelligent items include straightforward wearables like Fitbit smartwatches for evaluating fitness data to more complex infrastructures like self-driving cars for automatic vehicle intelligent transportation systems and microgrids for distributed generation systems [4,5]. The microgrid system is an example of a cyber-physical system combining all dispersed energy sources to supply electricity to a specific region. However, as existing microgrid IoT systems rely on conventional SCADA systems, combining the physical and digital worlds will considerably widen the system vulnerabilities [6]. For example, cyberattacks may threaten SCADA systems that would take down the whole physical realm. Additionally, the drone market is rapidly developing toward automating crucial tasks like emergency management and firefighting. These technologies are needed to ensure safety and dependability and will grow along with the dependency of individuals and communities on them. From a privacy and safety standpoint, IoT is a

technology that is most vulnerable to new cyberattacks, where compromised IoT devices might significantly negatively affect the physical world and leak data. The most notable IoT assaults were Stuxnet [7] and the Mirai DDoS attack [8], which showed how a single IoT device might impact the whole IoT system. Providing safe and reliable communication routes will help protect the vital data that scattered IoT devices gather and share. With the development of blockchains, a new strategy to control dispersed operations in the IoT environment has emerged. The main driving force behind the IoT's adoption of blockchain is to do away with centralized control and to automate a secured real-time data transmission between IoT devices. Blockchain converts the present centrally managed operating model to a decentralized one by deploying widespread, public ledgers to permit anonymized operations [9]. Furthermore, blockchain gives users control over their private information, allowing them to disclose it only to those they desire to and only in preapproved situations [10]. Since alteration or data modification necessitates commencing a new block, all transactions made on the blockchain network can be tracked, making the public ledger a convenient means to authenticate footprints and artifacts. Similar to any innovation, blockchain has drawbacks, mainly when used in crucial IoT systems such as programmable logic controller (PLC) networks. Prior research has focused on conventional security measures such as encryption and authentication protocols. While these approaches provide protection, they may not adequately address IoT networks' evolving and complex security challenges. Additionally, these methods often rely on centralized systems, which can introduce single points of failure and vulnerability to cyber-attacks. Other studies have investigated using traditional centralized databases for data storage and management in IoT systems. However, these approaches may face scalability issues and can be prone to data manipulation and unauthorized access. Centralized databases also raise concerns regarding trust and data ownership. In contrast, the new model proposed in this paper leverages blockchain technology to overcome the limitations of previous studies. The model provides enhanced security, authentication and data logging capabilities by incorporating a proof-of-work-based blockchain into the PLC IoT ecosystem. The decentralized nature of the blockchain ensures resilience and eliminates single points of failure. Moreover, the new model's efficient resource utilization and high-speed data transmission address the limitations of conventional methods. The main contributions of this paper can be summarized as follows: (1) establishing a firm basis by utilizing the literature to understand existing IoT security and privacy vulnerabilities and how these concerns influence the various levels of an IoT system's design; (2) examining and offering solutions for the security and privacy problems that exist in IoT devices; (3) finding restrictions and open security risks a blockchain-based IoT network might face; (4) implementing a suitable, effective and safe blockchain in a PLC IoT environment; (5) providing recommendations and a path forward by offering a blockchain-based IoT model that demonstrates how blockchain technology can be incorporated into a PLC IoT framework to increase the robustness of the PLC in the IoT environment.

The remainder of the paper is structured as follows. In Sections 2 and 3, a background on IoT security and privacy and blockchain is presented, respectively. We review the literature on the most current blockchain-based techniques used to increase IoT security in Section 4, which also covers the development of blockchain technology and highlights its security and privacy aspects that are ideal for IoT systems. A novel approach using blockchain in IoT systems regarding security and privacy is presented in Section 5. Section 6 describes the performance evaluation, outlining the simulation options and evaluation methods. Section 7 summarizes the proposed method's simulation results and the protocol implementation. The paper is wrapped up and concluded in Section 8.

2. A Background on IoT Security and Privacy

In this section, we first provide an overview of the IoT architecture and issues related to IoT security and privacy.

2.1. IoT Architecture

The Internet of Things (IoT) is a platform of millions of networked smart objects with sensors, actuators, software and a network connection. These devices collect and exchange data with various organizations, including businesses, governments and people. Three distinguishing characteristics—restricted computation, limited capacity and constrained processing—are used to classify these devices. The dramatic increase in IoT device usage is mainly the result of several factors: the falling cost of processors and the widespread accessibility of wireless connectivity. Although no defined and widely accepted IoT structure exists, multilayered models are usually used. A 4- or 5-layer IoT design has been suggested by some researchers. Typically, this model consists of the sensing, network, processing and application layers. These layers are explained as follows in [11]. Sensors gather essential data from the physical environment at the perception layer. Actuators that could affect the physical universe and cause modifications sans human interaction might also be present. Actuators oversee the gathering of data from items and reliably send the data back for additional operations. Sensors would send the collected data via an uplink or a wireless connection. At the network layer, data from the perception layer is consistently sent across wired and wireless networks to the processing layer, the subsequent layer. Network access gateways conduct data transfer in this tier using a variety of communication protocols. Through the aid of cloud computing, edge computing and data centers, increased analytics, quick data processing and massive data storage can be carried out on the processing layer, also known as the middleware layer. Both data and information are integrated into the application layer, where they then provide target devices' data in the context of apps in a user-friendly manner. These programs were created to meet specific customer or business requirements. They engage with people and provide them with solutions to certain issues. These programs can communicate with other programs. IoT has a broad application range that is constantly increasing. IoT is increasingly employed in various industries where it is used to regulate, analyze and improve our everyday lives due to the rapid development of the technology that enables it. Any item in our life has the potential to become a smart sensor. IoT devices can be utilized at the municipal level to track citizen transportation or recycling habits, or they could be used on a personal level to live healthier lifestyles or lower personal power expenses. IoT has been employed in transportation, industry, healthcare and smart grids.

2.2. IoT Issues in Security and Privacy

Every IoT system must adhere to some fundamental security standards [12]. Confidentiality, integrity, availability and authentication are such needs. The following definitions apply to such security aspects:

- **Confidentiality**: Only authorized individuals can view and retrieve personal data. Confidentiality is violated when confidential data is accessible due to a data leak.
- **Data integrity** guarantees that unauthorized entities have not altered or tampered with data. Among the many assaults that might jeopardize integrity, a man-in-the-middle attack is an example in which the data transmitted by one party to another could be intercepted and even altered by a "man-in-the-middle."
- **Availability** guarantees that data are always available to those who require it. Attacks such as denial-of-service (DoS) attacks impede availability and prevent authorized individuals from obtaining information.
- **Authentication** is the process of confirming the legitimacy of the entities demanding access to data. Achieving these goals is crucial for any system. Multiple variables, such as weak passwords or password reuse that facilitate password-breaking operations by hackers, might undermine authentication. Because of this, protocols, like the FIDO protocol [13], that offer passwordless authentication are becoming increasingly common. Using such elements in an IoT system presents several difficulties [12].

Maintaining the security of IoT system components should be accomplished with little impact on their operation, such that the IoT system components' storage, processing and

computing capacities are constrained. The security procedures that could be applied are constrained by their limiting capabilities. Any security procedures implemented must be scaled to protect a vast number of targets of numerous assaults. The possibility for security risks grows along with the quantity and diversity of IoT components, compromising the security need of every layer in the IoT architecture. Several hazards to IoT systems and their supporting technologies are found in the perception layer [12]. The perception layer relies significantly on innovations like RFID, Bluetooth and Zigbee. The perception layer is exposed to several assaults due to the employment of these systems [14]; some cases are:

- *Node Capture* describes a hacked node that causes the release of sensitive data. The hacker compromises the IoT system by adding a fake node, which allows for intrusive code attacks and compromises the system.
- A *denial-of-service (DoS) attack* could consume all available capacity and render the operations unavailable.
- A few assaults that may be encountered on the next layer, the network layer, are [12]:
    - *Jamming attack:* By blocking the communication link, a jamming attack greatly slows down the nodes' ability to communicate. A continuous jamming attack is an illustration of a jamming attack. A *continuous jamming assault* prevents legitimate nodes from using the communication link by emitting a radio signal.
    - *Reactive jamming attacks* are more challenging to identify than continuous jamming attacks because the assault is dormant until it detects interaction on the communication link, after which it begins releasing the radio signal.
    - In a *selective forwarding attack*, the attacking nodes will disable the network's routing pathways by refusing to send some, all or portions of the packages.
    - *A sinkhole/wormhole attack* consists of a malicious node answering routing queries, forcing communication to pass via a malicious node. The wormhole attack consists of a tunnel connecting two nodes while disregarding intermediary nodes.
    - In a *Sybil attack*, a malicious node will impersonate several nodes to gain control over network spaces or impair the operation of the IoT system by copying their identities. Denial of service might be brought on by a rogue node, replicating the identity of some other node.
    - The data's confidentiality is compromised by a *traffic analysis attack*, which records and examines data chunks.
    - In a *"Man in the Middle"* attack, an attacker or a malicious node listens in on exchanged information between two nodes. The attacker must intercept all pertinent communications sent and received by the two victims. This enables the malicious node or attacker to insert modified messages or data undetected. "Man in the middle" attacks only succeed if the malicious node successfully impersonates the endpoint by meeting the recipients' or protocol's expectations, as it aims to circumvent authentication.

The security vulnerabilities in the processor layer are [12]:

- Unauthorized access by attackers to sensitive data. By accessing data as they are being delivered to their destination, malicious insiders might violate confidentiality and privacy.
- Insecure software service: Malware-infected software services are provided via the processing layer. An IoT system's security features are in danger due to this. Third parties offer services with an unknown risk profile with an uncertain risk level in the processing layer. Lastly, the primary hazards [13,14] at the application level in which the consumers' demands are addressed are:
- A social engineering attack involves mentally coercing people into divulging sensitive data or unwittingly carrying out destructive deeds. For instance, phishing scams.
- Software attacks are assaults that strike software, such as backdoors and buffer overflows.

3. Blockchain-Based Systemt

Blockchains are a novel approach to decentralized data storage and processing using distributed, securely shared ledgers across all stakeholders to preserve information without outside authorities [15]. Blockchains enable nodes or partakers to use decentralized peer-to-peer (P2P) data sharing, ensuring exchange traceability and data integrity simultaneously. Prominent industrial actors have predicted that blockchain will be a transformative force. As a result, they are actively extending the range of goods they provide to take advantage of it and offer further effective support. To deal with the primary enhancements blockchain augments to enhance IoT security and privacy, we will outline the adoption of this technology in relation to the current IoT concept in this section. The development of blockchains remarkably coincided with the popularity of cryptocurrencies such as Bitcoin [16]. It functions essentially as a distributed, unchangeable ledger that is decentralized and captures P2P network interactions. Elliptic curve encryption (ECC) and SHA-256 hashing safely transfer chain data to preserve data integrity and authenticity [17]. Every block consists of all activities and the hashes of the prior and following blocks. As a result, a block that has already been transmitted cannot be edited and added to the blockchain network. As such, blockchain is immutable and resistant to manipulation. This immutability creates a network of trustworthy participants in which mistakes or weaknesses may be easily traced to ensure the safety of participants' information and assets. A consensus method that manages to put and connect data into new blocks in the blockchain network is used to validate transactions throughout the network.

3.1. Types of Blockchains

Depending on how nodes may connect to the network, the rights every node is given, and the consortium used to confirm operations, there are several blockchain types and architectures [18–20]. There are three types of blockchains: proof of work (PoW), proof of stake (PoS) and proof of authority (PoA). With PoW (Figure 1), a participant in a network must undertake physical efforts. The participant, the miner, provides computing power to solve a cryptographic puzzle. The solution is needed to convert and link information from pending transactions and the previous block into a new block.

Figure 1. The proof of work (PoW) [20].

Mathematically, the PoW algorithm can be expressed as:

$$\text{Hash}(B + N) = H. \quad (1)$$

where,

- B: block data (e.g., binary input and output signals of the PLC)
- N: nonce (a random value)
- H: hash value (with Z leading zeros).

As shown in Figure 2, the PoS validation process is designed to reduce power and resource intensity. Instead of a computing competition, a network actor is chosen in turn, according to the random weight principle, to process the due transaction and create a new block. Confidence in the actor's credibility is formed by depositing a deposit—called a stake. In PoS, network actors (validators) are chosen to process transactions and create

new blocks based on the random weight principle. Each validator must deposit a certain amount of cryptocurrency (stake) as collateral to participate in block validation.

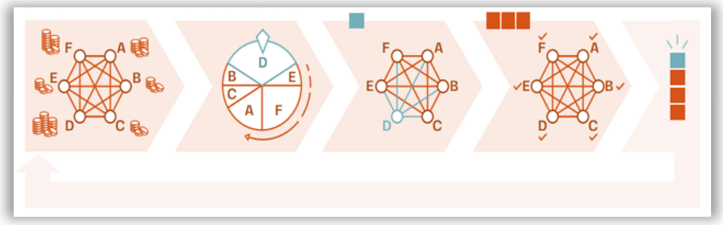

Figure 2. The proof of stake (PoS) [20].

Let us represent the stake deposited by a validator as "S_i" for validator i. The probability of a validator being chosen to create the next block is directly proportional to their stake in the network. Let us represent the probability of validator i being selected as "P(i)". It can be calculated as follows:

$$P(i) = S\_i/\Sigma(S\_all) \quad (2)$$

where,

- S_i: stake deposited by validator i
- Σ(S_all): total stake deposited by all validators.

With the PoA illustrated in Figure 3, only a certain number of actors, the so-called "authorities," have the right to validate blocks. However, usage of the blockchain is freely accessible. The identity of these "authorities" is known to the network and trust in the network is based on their reputation. Each "authority" alternately proposes a block. The remaining "authority" majority must confirm the correctness. This mechanism also significantly reduces energy and computation consumption. The last two blockchain variants enable "smart contracts, "an interesting aspect for various industries. The PoA mechanism significantly reduces energy and computation consumption compared to traditional proof of work (PoW) consensus. Let us represent the energy consumption reduction ratio as "R_energy" and the computation consumption reduction ratio as "R_computation".

$$R\_energy = (\text{Energy Consumption PoW} - \text{Energy Consumption PoA})/\text{Energy Consumption PoW} \quad (3)$$

$$R\_computation = (\text{Computation Consumption PoW} - \text{Computation Consumption PoA})/\text{Computation Consumption PoW} \quad (4)$$

Smart contracts are concluded in an energy-efficient and resource-saving manner through the so-called "second-layer mechanism." This is an algorithmic contract with predefined conditions. When these are met, actions are automatically triggered, so smart contracts form the basic framework for machine-to-machine contract execution.

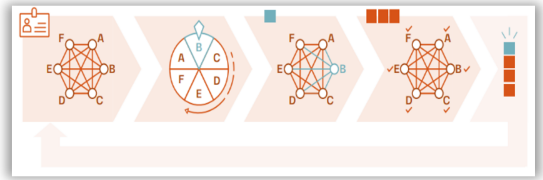

Figure 3. Proof of authority (PoA) [20].

3.2. Blockchain Architectures

3.2.1. Public Blockchain

An open-source platform known as a public blockchain enables anybody to connect to the network anonymously and without any requirements. Every node has complete powers

to verify, read and write on the network (i.e., Bitcoins) [18]. To connect to the networks and obtain a duplicate of the ledger, nodes or miners must acquire the genesis block, the network's initial block [19]. Due to the redundancy, data integrity is guaranteed and information tampering is prevented. By a consensus method that ensures the consistency of blocks across the whole blockchain network, miners verify transactions before submitting them as a new block in the network. Enemies must command 51% of the network's mining power to seize the public blockchain. Furthermore, cryptographic key pairs—public and private—are utilized to protect operations. This hashed public key serves as the address for the miner or node, whereas the private key is used to sign transactions [21]. Particularly concerning the initial use case—cryptocurrencies—public blockchain has specific security threats and weaknesses [22,23].

3.2.2. Private Blockchain

A decentralized network called a permissioned or private blockchain enables the exchange of information between specified nodes in a particular system. Prior permissions must be provided to every new node before it may take part and submit new blocks to the network. One of the well-known private blockchain platforms, Hyperledger [24], uses PFBT [25] to ensure valid transactions and uphold transparency. When writing capabilities are exclusively allowed to specifically approved nodes, private blockchains move away from decentralization and into centralization [26]. A private blockchain controls the network's operating nodes and how a node is linked. To obtain data more quickly, nodes must keep up a particular number of links to be regarded as operational [23]. Nevertheless, the centralized feature of private blockchain makes it difficult to spot nodes that could purposefully obstruct communications or send false data. Organizations must carefully examine the degree of potential threats when choosing where to host their utilities to preserve service dispersion, clients' anonymity and data confidentiality.

3.2.3. Consortium Blockchain

A consortium blockchain is a partly or semiprivate blockchain in which several companies or participants oversee validating transactions and submitting blocks. Every block is verified utilizing a multisignature system, which requires the authorization and signature of every operating node. Participants may, at any moment, remove credentials and assign nodes to read or write on the network [27]. Although it offers identical performance and transaction data protection advantages like a private blockchain, no single entity controls the network. The consortium blockchain is, therefore, more resistant to data falsification and transaction alteration [28].

3.3. Blockchain Security and Privacy Characteristics

Most IoT systems are predicted to transform significantly thanks to blockchain technology that employs smart contracts to secure IoT devices. Blockchains can improve IoT systems, particularly those requiring distributed, safe and reliable information exchange across all stakeholders. Blockchain's decentralized structure might help IoT systems avoid serious centralized security problems like single points of failure and ensure the responsiveness of IoT services. Additionally, it provides dependable control, administration and monitoring for every stage of an IoT device's life cycle, including manufacturing, distribution, installation, ownership and reinstallation. The decentralized and distributed ledger [28] also provides redundant data, where each node must have a database backup, making the data unchangeable and trustworthy. Furthermore, exchanges are verified in a trust-free network where nodes are anonymous, and their identification can be safely maintained.

The IoT gadget may be tracked at each stage of the product life, beginning with the producer, distributor and customer. The holder may vary throughout an IoT device's lifespan, necessitating a practical and secure identity management system. The producer, GPS coordinates, serial number, model and other IoT-device-related characteristics necessitate safe and reliable management [29]. Blockchain can potentially reduce these issues

throughout the entire lifespan of IoT devices. Using a decentralized and distributed ledger (Figure 4), it can handle linked IoT devices' complicated properties and interconnections and recognize and verify identities.

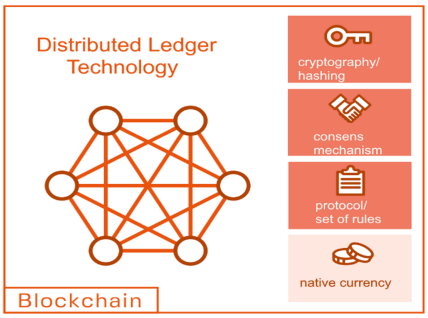

Figure 4. Distributed ledger technology [20].

Blockchain uses 160-bit address space as a hashed public key generated by the ECDSA (Elliptic Curve Digital Signature Algorithm). Using blockchain, many addresses regarded as safe and one-of-a-kind to assign to IoT devices are produced and allocated. Hence, contrasted to different addressing schemes like IPv6, which gives 128-bit address space, blockchain can be a scalable solution for the Internet of Things. The original sender cryptographically authenticates data communicated among all IoT devices to assure data security and authenticity thanks to the address individuality of the blockchain delivers. To ensure data consistency and dependability, exchanges in the network are also irreversible and trackable. A useful aspect of blockchain is the ability to hard code constraints that establish privileges and access restrictions among network nodes, such as smart contracts. Smart contracts can offer decentralized authentication logic for efficiently authenticating IoT devices, which is not as complicated and hard-coded into regulations. While specifying the terms and restrictions whereby some nodes can obtain certain data, it also ensures data security. Smart contracts can provide guidelines for IoT software updates or patches, ownership changes or the creation of new keypairs.

4. Literature Review

The development of the Bitcoin blockchain network has significantly transformed the distributed ledger technology landscape. With its high cryptographic security and immutability level, blockchain offers compelling advantages for secure data sharing among heterogeneous Internet of Things (IoT) devices while ensuring data accuracy [30]. While several blockchain platforms are available, many are still reliant on centralized cloud networks. To truly understand how the IoT can benefit from the core security characteristics of blockchain, it is essential to explore the significant security distinctions between the cloud and blockchain. One key distinction between blockchain and the cloud lies in their centralization or intermediate dependency levels. Cloud-based services are typically provided through centralized management by a reputable third party. However, this centralization introduces vulnerabilities, as it creates single points of failure that can compromise access, security and the protection of user data. Cloud service providers must be trusted to prevent data tampering, as they can potentially violate customer privacy and alter data without permission [30]. On the other hand, blockchain operates on a decentralized model. In a blockchain network, each participating node must copy and maintain the ledger that preserves the network state. This decentralized nature ensures that nodes with corrupted replicas of the ledger are denied access without causing disruptions to the overall operations of the blockchain. By distributing the ledger among multiple nodes, blockchain enhances security and resilience [30]. However, the growth of blockchains, particularly in IoT contexts where data are collected from many sensors, presents a challenge. The sheer size of blockchains can strain IoT devices' limited storage and processing capacity, potentially affecting their ability to act as full nodes for verifying transactions. Furthermore,

the cloud is susceptible to unwanted data exchange with third parties, which can violate users' privacy. In contrast, blockchain technology addresses this concern by incorporating role-based access control into smart contracts. By hard coding access control rules into the blockchain, users are empowered to regulate who can access their data. Additionally, data encryption plays a crucial role in safeguarding customer information. Data are encrypted to protect customer privacy before adding a new block to the blockchain network. Since only individuals with the appropriate private key can decode the encrypted data, all nodes can store and maintain data without compromising secrecy [31]. The literature on blockchain and IoT security highlights the potential of blockchain technology to address the security challenges of IoT systems. Researchers have proposed various approaches to leverage blockchain for enhancing IoT security. Recent approaches to increase IoT security through blockchain are discussed next.

4.1. Software Update Approach

The secure and timely update of IoT systems is crucial to address the inherent vulnerabilities and flaws present in these systems. Given that most IoT devices are not secure by default, regular updates are necessary to fix bugs, patch security vulnerabilities and improve overall system performance. However, ensuring the confidentiality of involved individuals during the update process is equally important. In this context, the software update approach leveraging blockchain technology emerges as a promising solution. Researchers have proposed innovative methods to facilitate secure blockchain software updates for IoT devices. One such approach, as presented by authors in [32], involves the utilization of a redesigned block format and the BitTorrent network for firmware exchange. The BitTorrent network, known for its decentralized and efficient file-sharing capabilities, provides a robust foundation for securely distributing firmware updates to many IoT devices. The authors integrated a specific node into the blockchain network to enhance the security of the software update process [33]. This dedicated node verifies the legitimacy and availability of software updates, ensuring that only authorized updates are downloaded and applied.

By incorporating blockchain technology, the software update approach adds a layer of security, making it more resilient to potential attacks and unauthorized modifications. By leveraging the transparency and immutability of blockchain, the system provides a reliable and tamper-resistant platform for secure firmware updates. The software update approach using blockchain technology offers several benefits for IoT security. Firstly, it enhances the integrity and authenticity of firmware updates. Through the decentralized nature of blockchain, the update process becomes more resistant to tampering and unauthorized modifications. By leveraging the consensus mechanism of blockchain networks, updates can be verified by multiple nodes, reducing the risk of malicious attacks or the introduction of compromised firmware. Secondly, blockchain technology provides a transparent and auditable update process. The decentralized ledger allows all participants in the network to have visibility into the updated transactions, ensuring accountability and traceability. This transparency enables easier detection of any malicious activities and promotes a higher level of trust among IoT device users. Furthermore, the blockchain technology software update approach can mitigate the risk of unauthorized or malicious updates. By incorporating cryptographic techniques and public-key infrastructure, the blockchain ensures that only authorized updates, digitally signed by trusted entities, are applied to IoT devices. This helps to prevent the installation of compromised firmware or the introduction of malware that can compromise the security of the IoT system. However, it is important to acknowledge the challenges associated with the software update approach using blockchain in IoT systems. The size and complexity of the blockchain can impose limitations on resource-constrained IoT devices' storage and processing capabilities. Therefore, efficient mechanisms should be developed to address these challenges and optimize the update process, particularly in IoT environments where many devices need to be updated simultaneously.

4.2. Access Control Systems

Centralized access control systems have long been relied upon to ensure data security by providing and revoking user rights. However, these systems are susceptible to a single point of failure, which can compromise the system's overall security. In contrast, blockchain technology offers a decentralized access control manager to address this limitation and provide secure access control in heterogeneous IoT topologies. Researchers have proposed access control techniques that leverage blockchain technology to enhance the security of IoT systems. For instance, authors in [34] introduced an access control system that utilizes blockchain to provide secure access controls to users who need to exchange resources. This system has been successfully certified in a scenario where users inquire about traffic lights and patterns to find open parking spaces for their automobiles. By utilizing blockchain for access control, the system ensures a decentralized and tamper-resistant environment. The blockchain's distributed ledger allows for transparent and auditable user rights management [35]. The access control manager, implemented as smart contracts on the blockchain, enables users to securely grant or revoke access rights without relying on a central authority. This decentralized approach eliminates the single point of failure present in centralized access control systems. The use of blockchain for access control in IoT systems offers several benefits. Firstly, it ensures the transparency and immutability of access control policies. The blockchain's distributed ledger allows all participants to have visibility into access control transactions, providing transparency and accountability. Additionally, the immutability of the blockchain ensures that once access rights are granted or revoked, they cannot be altered or tampered with, enhancing the integrity of the access control system [36]. Secondly, blockchain-based access control enables secure and decentralized management of user rights. Users have greater control over their data and can grant or revoke access without relying on a central authority. This enhances privacy and reduces the risks associated with centralized access control systems, such as unauthorized access or abuse of privileges. One challenge is the performance and scalability of the blockchain network [37]. As the number of IoT devices and access control transactions increases, the blockchain may face scalability issues, potentially affecting the efficiency of access control operations. Efforts should be made to optimize the blockchain protocols and explore scalability solutions, such as off-chain transactions, to ensure the smooth operation of access control in large-scale IoT deployments [38,39].

4.3. Protection Approach

Research in the field of blockchain technology has seen a growing focus on approaches that solely rely on blockchain for various applications, including Internet of Things (IoT) security [40,41]. One recent development is the emergence of a double-chain architecture that merges transactional and data chains to enhance data integrity, distributed data storage and overall security. The double-chain architecture consists of two interconnected chains: the data blockchain and the transaction blockchain. The data blockchain is responsible for ensuring data integrity and distributed data storage. It utilizes a consensus technique to create data blocks that safeguard the integrity of the stored data. This consensus mechanism ensures that all blockchain network participants agree on the data blocks' validity, preventing tampering or unauthorized modifications. On the other hand, the transaction blockchain focuses on managing data registration effectiveness, resource management and transfer [42]. It employs a distributed accounting system that tracks and records transactions within the blockchain network. This accounting system ensures the transparency and accuracy of data exchanges, allowing for efficient resource allocation and effective management of data transfer operations. The double-chain architecture addresses the security challenges associated with IoT data exchange [43]. The architecture provides a compact IoT information-sharing security framework by separating the data and transaction functions into distinct chains. This framework has proven exceptionally resilient against various attacks, including device injection attacks and denial of service (DoS) attacks [44]. Using a double-chain architecture and other blockchain-based approaches for IoT data exchange

offers several benefits. Firstly, blockchain's distributed and decentralized nature ensures that data exchanges occur among multiple participants without intermediaries. This enhances the trustworthiness and security of IoT data exchange, as there is no single point of failure or reliance on a central authority. Secondly, the immutability and transparency of the blockchain provide an audit trail for data exchanges in IoT systems. Every transaction and data modification are recorded in the blockchain, allowing for accountability and traceability [45,46]. This audit trail can be valuable in identifying and mitigating potential security breaches or unauthorized access to IoT data.

As shown in Table 1, while blockchain has potential benefits in resolving IoT security and authentication constraints, several research gaps need to be addressed. Firstly, there is a need for further exploration of the specific mechanisms and protocols for secure transmission and storage of sensitive user data among IoT devices. Scalability and performance considerations pose another challenge, requiring efficient solutions to handle the increasing volume of data and transactions generated by IoT devices. Moreover, comprehensive evaluations and empirical studies are necessary to validate the proposed blockchain-based model's feasibility, efficiency and security in real-world PLC IoT environments. Additionally, addressing memory and tracing problems faced by different PLC manufacturers requires developing specific solutions tailored to the diverse nature of PLC devices. Bridging these research gaps will enhance the understanding and effectiveness of blockchain-based solutions, contributing to IoT systems' secure and resilient operation, particularly in critical PLC networks. The proposed research aims to address IoT systems' security and privacy concerns, particularly in programmable logic controller (PLC) networks, by leveraging blockchain technology. This paper focuses on the drawbacks of using blockchain in critical IoT systems, precisely programmable logic controller (PLC) networks. It contributes in the following ways: establishing a solid understanding of existing security and privacy vulnerabilities in the IoT through literature review, proposing solutions for security and privacy issues in IoT devices, identifying limitations and potential security risks of a blockchain-based IoT network, implementing a secure and effective blockchain in a PLC IoT environment and providing recommendations and a blockchain-based IoT model to enhance the robustness of PLCs in an IoT setting.

Table 1. Comparative study on IoT security using blockchain.

Paper	Method	Limitations	Strengths
Lee et al. [32]	Blockchain-based secure firmware update for embedded devices	Lack of real-world deployment evaluation	Enhances security of firmware updates for embedded IoT devices
Boudguiga et al. [33]	Accountability for IoT updates by means of a blockchain	Limited discussion on scalability and performance considerations	Improves availability and accountability of IoT updates through blockchain
Dukkipati et al. [34]	Blockchain-based access control framework for the heterogeneous IoT	Need for efficient mechanisms to handle a large number of access control transactions	Provides a decentralized and secure access control framework for IoT
Lone et al. [35]	Applicability of blockchain smart contracts in securing Internet	Systematic literature review without specific experiments	Highlights the use of smart contracts for securing Internet and IoT
Maesa et al. [36]	Blockchain-based for auditable access control systems	Lacks discussion of scalability and performance aspects	Provides auditable access control system using blockchain
Zhang et al. [37]	A smart-contract-driven framework	Limited discussion of scalability and performance	Utilizes smart contracts for secure access control
Nakamura et al. [38]	Exploiting smart contracts for capability-based IoT access control	Need for further evaluation in real-world IoT environments	Leverages smart contracts for capability-based access control in IoT

Table 1. *Cont.*

Paper	Method	Limitations	Strengths
Abdi et al. [39]	Hierarchical blockchain-based multi-chaincode access	No specific experimental evaluation; the need for further assessment of IoT	Presents a hierarchical access control framework for securing IoT
Si et al. [40]	IoT information-sharing security mechanism based on blockchain	Inefficient storage and processing of blockchain in resource-constrained IoT	Provides a secure mechanism for IoT information sharing using blockchain
Jia et al. [41]	Blockchain-enabled federated learning data protection aggregation	Need for further evaluation in real-world IoT environments	Ensures data protection in federated learning using blockchain
Alzubi [42]	Blockchain-based Lamport Merkle digital signature:	Limited discussion of scalability and performance considerations	Presents a blockchain-based authentication tool for IoT healthcare
Cha et al. [43]	Blockchain-empowered cloud architecture based on secret sharing	No specific experimental evaluation; lack of real-world deployment evaluation	Proposes a blockchain-based cloud architecture for smart cities
Sheron et al. [44]	Decentralized scalable security framework for end-to-end authentication communication	Scalability challenges of blockchain networks	Provides a decentralized security framework for IoT communication
Chen et al. [45]	Improved algorithm for practical Byzantine fault tolerance to large-scale consortium chain	Focuses on Byzantine fault tolerance, not specific to IoT; need for further evaluation in real-world IoT consortium chain scenarios	Presents an improved algorithm for practical Byzantine fault tolerance
Corusa et al. [20]	Marktübersicht der Blockchain in der Energiewirtschaft	Market overview, not specific to IoT; limited discussion of technical limitations and challenges	Provides a market overview of blockchain in the energy industry

5. The Proposed Approach: IoTBChain

This paper proposes an innovative method focusing on IoT capabilities and PLC device security. The new approach will incorporate a proof-of-work-based blockchain into the IoT ecosystem. This blockchain enables the transmission of binary data and the data logging of PLC signals. This novel technique uses fewer resources than other sophisticated ways that PLC devices communicate data while maintaining high transmission, encryption and decoding speed. The IoTBChain proposal in this novel method accomplishes this by using a straightforward hashing algorithm for the encryption and validation mechanism. Another new feature of the IoTBChain is that it verifies the validity of the timestamp while maintaining data integrity and ensuring data authenticity. In addition to ensuring repeatability, our new model addresses the memory and tracing problems that different PLC manufacturers encounter.

5.1. Proposed Model—Block Structure

This new method uses a basic blockchain protocol. As such, the chain consists of blocks with a predefined format. This means that a superclass known as the block class is responsible for the structure of the to-be-transmitted data. The encryption, validity and authentication processes and methods are declared here. In the case of the IoTBChain, the data are structured as shown in Figure 5. Every block has an index, as defined in the superstructure. It is important to identify which block/position in the blockchain sequence the data are stored, but it is also vital to ensure reproducibility. Another important aspect for ensuring the security, reproducibility and ability to trace/log what happened within a PLC system is the timestamp, which acts as a nonce. A nonce is a random or nonrepeating value

inserted into a protocol's data exchange to ensure that only live data—rather than replayed data—are sent, hence identifying and thwarting replay attacks [30]. As a timestamp is used, it also enables the chain to check for a malicious attempt to alter information. The data have been altered if the block's timestamp is before the previous block. Additionally, suppose the timestamp between two blocks in a response setting exceeds a predefined limit for the transmission time, in that case, the chain can assume there was an attempt to alter or manipulate the information. A block also contains the binary input and output signal of the PLC. This is the data that need to be transmitted and stored. Additionally, the chain includes the sender device's IP address and the designated receiver's IP address. Knowing which information was transmitted between devices is essential in the error analysis in the PLC environment.

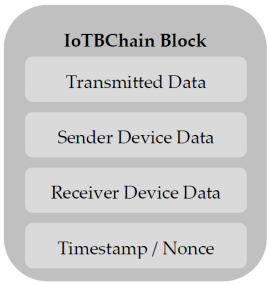

Figure 5. The IoTBChain block structure.

The block in the IoTBChain approach contains various components, including an index (represented by "I"), timestamp (represented by "T"), PLC signals data (represented by "S"), sender's IP address (represented by "A_s") and receiver's IP address (represented by "A_r"). Mathematically, the block structure can be expressed as:

$$\text{Block} = (I, T, S, A\_s, A\_r) \tag{5}$$

5.2. Proposed Model Implementation

When the communication protocol/blockchain is initialized, the chain protocol checks if it is the first block. Once confirmed, the protocol will automatically generate a genesis block. The genesis block is sometimes referred to as Block 0. It is the initial block in a blockchain, where all subsequent blocks are added. Since each block relates to the one before it, it serves as the ancestor to all subsequent blocks—all subsequent blocks can trace their descent back to this block. Each block is linked to the previous block through a hash value. Once the genesis block has been created, the protocol initiates the first data transfer/storage. When creating the following block, the protocol first attains and decodes the previous block's data. Here, the timestamp of the previous block is decrypted. Then the validity of the timestamp is analyzed. If validity is confirmed, the previous block's hash value is compared to the hash it should possess based on the transmitted data. The new block is generated after verifying the authenticity and validity of the previous hash. The generation of the new block involves the hashing of the data, the new timestamp as well as the hash value of the previous block. These data are then added to the IoTBChain as a new block with an incremented index to the previous block, as illustrated in Figure 6.

To ensure the validity of the timestamp, the IoTBChain approach checks whether the timestamp of a block is later than the previous block's timestamp. If the timestamp is earlier, it indicates that the data may have been altered. Mathematically, the validity of the timestamp can be verified as:

$$T(i) > T(i-1) \tag{6}$$

where,

- Ti: timestamp of the current block
- $T(i-1)$: timestamp of the previous block

- Block generation: when generating a new block, the protocol calculates the hash of the current block data (S), the new nonce (N) and the hash value of the previous block (H_(i − 1)).

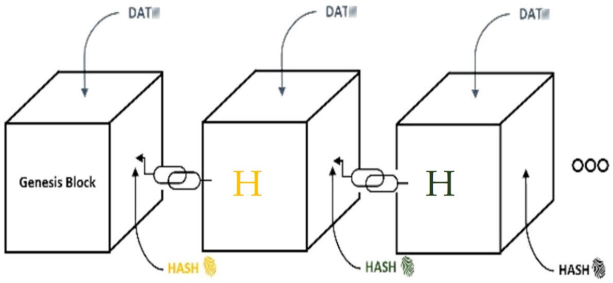

Figure 6. Blockchain structure.

The block generation can be represented as:

$$H(i) = Hash(S + N + H\_(i - 1)) \quad (7)$$

where,

- H(i): hash value of the current block (Block i)
- S: block data (PLC signals)
- N: nonce for the current block
- H(i − 1): hash value of the previous block (Block i − 1)

As more blocks need to be generated for communication between a few PLCs, the protocol repeats the beforementioned process, as seen below. The protocol will start a new chain whenever a restart, retrofit or other devices are introduced to the communication channel. For logging and simulation reasons, the information from the old chain can be stored externally. All devices with the appropriate hashing method can participate in this protocol by transferring the data in an IoT/edge environment. Thus, a reliable Internet connection is the only need for using this strategy. Additionally, it implies that a single PLC device with a variety of hashing algorithms can securely connect to several different devices at once without running the danger of disclosing sensitive information to the incorrect party, as shown in Figure 7.

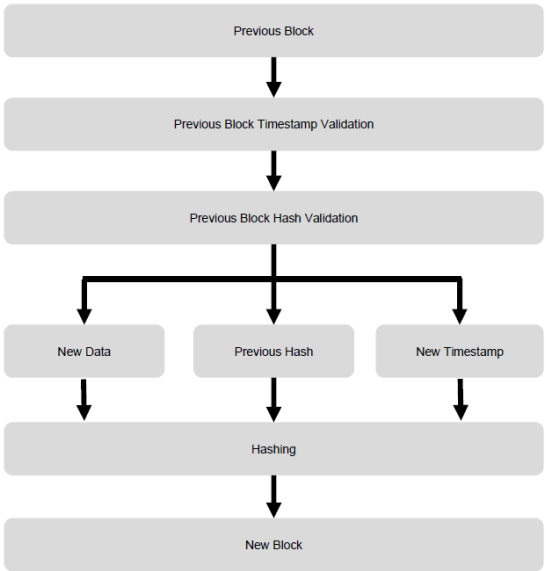

Figure 7. The processing flow diagram—IoTBChain.

6. Performance Evaluation

This section outlines the simulation options and evaluation methods used to assess the performance of the contrasted algorithms. This section will also go over methodology-related variables, such as system parameters.

6.1. System Parameters

An Intel i7 11th generation processor with 64 GB of RAM was used to run the simulation. The simulation software uses Visual Studio's (2022). NET default settings for C++ Windows apps. The simulations were run several times to ensure the findings were reliable and valid compared to the various methods.

6.2. Experimental Factors

Criteria for testing the algorithm must be established to assess the performance and for comparison. The speed at which the algorithm generates blocks of various lengths was chosen as the performance parameter because the security attributes of blockchain and the other methods are already well known. Let us define the block generation time "T_gen" as a function of block length "L" and any other relevant system parameters:

$$T\_gen(L) = f(L, P, RAM) \quad (8)$$

Here, "f" represents the function that determines the block generation time based on the block length, processor specifications and RAM.

6.3. Block Generation Speed

To quantify the performance parameter of block generation speed, let us define the average block generation time "T_avg" as a function of block length "L" and the number of times the simulation was run "N" to obtain reliable results:

$$T\_avg(L) = (\Sigma(T\_gen\_i(L)))/N \quad (9)$$

where "T_gen_i(L)" represents the block generation time for the i-th simulation run with block length "L."

6.4. Simulation Procedure

The IoTBChain was only initialized with the genesis and following blocks for testing purposes. The hashing procedure used the Windows 11 integrated hashing function [46]. To prove the security of the blockchain, a man-in-the-middle (MIM) attack with the correct decryption key was simulated. Therefore, the blockchain was attacked and the input data of the last block were altered. The initialization process for validating the last block was then performed to check if the protocol identified the alteration. After the MIM attack simulation, the initialization process validates the last block to check whether any alterations to the input data were correctly identified. Let us represent the validation process as "V(D_original, D_altered)":

$$V(D\_original, D\_altered) = Valid \text{ or } Invalid \quad (10)$$

7. Simulation Results

7.1. Valid Chain

The conducted test examined the resource consumption and processing speed of a valid blockchain chain. Let us represent the time taken to initialize the genesis block as "T_init," the time taken to generate the block with index 1 as "T_block1," and the time taken to generate subsequent blocks as "T_block(i)" for the i-th block. We can use a function "f(L)" to represent the time taken to generate a block with a specific index "L":

$$f(L) = T\_block(L) \quad (11)$$

The function "f(L)" allows us to quantify the processing speed of the blockchain as it generates blocks of different indices.

The results, depicted in Figure 8, revealed that the initialization of the genesis block took approximately 19 ms, indicating a relatively quick setup process. Subsequently, the generation of the block with index 1 required approximately 2006 ms, followed by the generation of the subsequent block, which took around 2014 ms. The slight increase in processing time for each subsequent block can be attributed to the validation of the previous block's data, ensuring the integrity and consistency of the blockchain. The IoTBchain, when properly initialized and with correctly generated blocks, only demonstrates the validity and integrity of the entire chain and provides the capability to visualize the data stored in previous blockchain elements. This feature enables efficient data retrieval and analysis, enhancing traceability and transparency within the blockchain. To understand the slight increase in processing time for each subsequent block, let us represent the time taken to validate the previous block's data as "T_validation." The block generation time for each subsequent block can be represented as the sum of the time taken to validate the previous block's data and the time taken to generate the current block:

$$T\_block(i) = T\_validation + T\_data\_generation(i) \quad (12)$$

where "T_data_generation(i)" represents the time taken to generate the data for the i-th block.

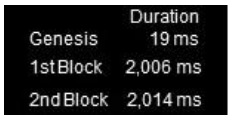

Figure 8. Benchmarking IoTBChain.

Figure 9 showcases an example of a valid chain in the IoTBchain, illustrating the sequential arrangement of blocks and the associated data within each block. This visual representation aids in understanding the chronological flow of information within the blockchain and allows for the verification of data authenticity at each stage. By conducting these tests and presenting a valid chain example, the study demonstrates the functionality and effectiveness of the IoTBchain in maintaining the integrity of data and providing a robust and transparent framework for IoT applications.

7.2. Corrupted Chain

In the second simulation, the blockchain's initialization and creation process was performed as in the first simulation. However, in this case, a man-in-the-middle (MIM) attack was introduced to test the security protocol of the IoTBchain. Initially, the data in the last block were created with the same content as the valid block, maintaining consistency with the original chain. However, during the implementation of the MIM attack, the IoT binary data within the block were altered to "110101011". Furthermore, the automatically derived "Sender Device" ID was modified to match the original sender ID.

In the simulation, let us represent the original data in the last block as "D_original," the altered data after the MIM attack as "D_altered," the original sender device ID as "ID_original," and the altered sender device ID as "ID_altered.". The security protocol of the IoTBchain involves validating each block's data and sender device ID to ensure its integrity. Let us represent the validation process as "V(D, ID)", where "D" is the data in the block and "ID" is the sender device ID. The validation process checks the correctness of both the data and the sender device ID. The simulation results can be represented mathematically as follows:

- D_original = original data in the last block
- D_altered = altered data after the MIM attack
- ID_original = original sender device ID

- ID_altered = altered sender device ID
- V(D_original, ID_original) = valid (block remains unchanged)
- V(D_altered, ID_altered) = invalid (block detected as compromised)

As depicted in Figure 10, the security protocol of the IoTBchain detects the MIM attack and identifies this block as invalid. Consequently, the boolean validity indicator of the IoTBchain protocol is adjusted to false, signifying that the chain has been compromised. In response, the IoTBchain terminates and a new chain must be initialized to ensure the integrity and security of the system. This simulation demonstrates the robustness of the IoTBchain's security protocol in detecting and handling MIM attacks. By promptly identifying and marking compromised blocks as invalid, the IoTBchain ensures the trustworthiness of the blockchain and prevents the propagation of tampered data within the network.

7.3. Discussion and Comparative Analysis

Comparing the novel approach to currently used technology reveals its benefits and shortcomings. Prior research has focused on conventional security measures such as encryption and authentication protocols. While these approaches provide protection, they may not adequately address IoT networks' evolving and complex security challenges. Additionally, these methods often rely on centralized systems, which can introduce single points of failure and vulnerability to cyberattacks. Other studies have investigated using traditional centralized databases for data storage and management in IoT systems. However, these approaches may face scalability issues and can be prone to data manipulation and unauthorized access. Centralized databases also raise concerns regarding trust and data ownership. In contrast, the new model proposed in this paper leverages blockchain technology to overcome the limitations of previous studies. The model provides enhanced security, authentication and data logging capabilities by incorporating a proof-of-work-based blockchain into the PLC IoT ecosystem. The decentralized nature of the blockchain ensures resilience and eliminates single points of failure. Moreover, the new model's efficient resource utilization and high-speed data transmission address the limitations of conventional methods.

```
*********************************
*      Valid Chain is created     *
*********************************


=========== Block ===========
BlockIndex: 0
IoT Data: 0
Sender Device: Genesis
Receiver Device: Genesis
Timestamp: 1669950257
Hash: 11545659985266398967
Previous Hash: 0
Is Block Valid?: True




=========== Block ===========
BlockIndex: 1
IoT Data: 111111111
Sender Device: 192.168.200.1
Receiver Device: 192.168.200.5
Timestamp: 1669950259
Hash: 10719109965991397002
Previous Hash: 11545659985266398967
Is Block Valid?: True




=========== Block ===========
BlockIndex: 2
IoT Data: 101010101
Sender Device: 192.168.200.5
Receiver Device: 192.168.200.1
Timestamp: 1669950261
Hash: 3412545740145777589
Previous Hash: 10719109965991397002
Is Block Valid?: True
```

Figure 9. A valid chain.

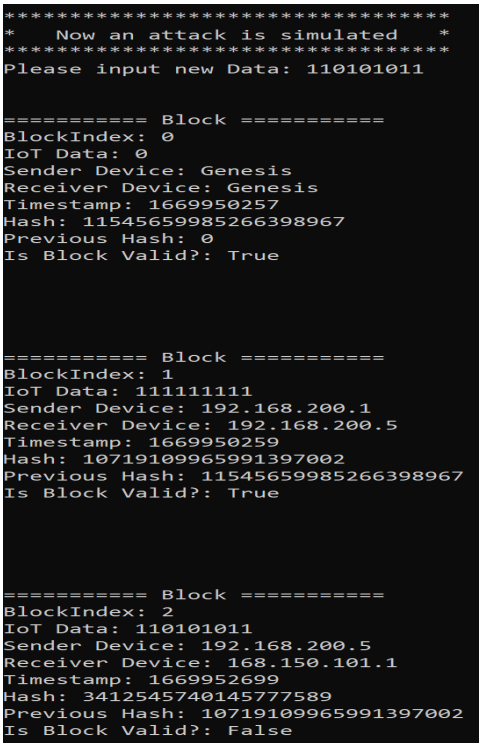

Figure 10. A corrupted chain.

A benchmark was run against symmetric encryption, the industry standard for benchmarking, to compare the newly developed approach to other methods available on the market [47]. In this instance, symmetric key encryption was contrasted with the blockchain system. By combining the existing hash value with a nonce, blockchain communications offer an encryption method that is more reliable and secure, as shown in the simulation (Figures 9 and 10). Along with authenticating the sender's identity, verifying the data's legitimacy and integrity is possible. The newly suggested method does, however, have a few minor drawbacks. The two primary drawbacks compared to symmetric encryption are a slightly higher resource demand and a marginally longer processing time. This occurs because the encryption and decryption procedures are more sophisticated. These problems will only have a minor effect in the future due to ongoing technological advancements and an increase in the processing capacity and speed of microcontrollers and PLCs [48]. There is also a data transferring limit per block, so some PLC data transfer protocols may need to be modified to use this approach. When comparing the IoTBChain to other modern security measures, its advantages and disadvantages become even more visible. As shown in Table 2, compared to secure communication units or security chips and public key infrastructures (PKIs), the IoTBChain offers the same protection. Additionally, the speed of the security chip is comparable to that of the IoTBChain, according to the data from Farahmandi et al. [49] and the results of the IoTBChain simulation. The speed is, however, slower than that of most symmetric encryptions. The IoTBChain has a cost and physical space advantage over the security chip as it does not need additional hardware. This makes the IoTBChain a more viable solution compared to other industrially applied solutions. While the proposed approach leveraging blockchain technology for PLC IoT networks offers several advantages, it is important to consider its limitation. The reliance on a blockchain introduces a dependency on network connectivity. If the network connection is disrupted or latency issues arise, it can impact the real-time operation of IoT devices and the efficiency of data transmission and logging.

Table 2. Technology comparison.

	Symmetric Encryption	Security Chip	PKI and Digital Certificate	IoTBChain
Security	0	++	++	++
Speed	0	−	−−	−
Processing consumption	0	−	−−	−
Additional hardware	0	−−	++	++
Transfer limit	0	0	0	−
Total score	**0**	**−−**	**0**	**+**

8. Conclusions and Future Directions

Integrating blockchain into IoT systems can cause serious security and adaptability difficulties, as well as the ubiquitous rise in technology. Consequently, this paper evaluates the IoT security needs to determine potential security and privacy weaknesses and reduce these risks by implementing blockchain technology. We created a method that provides a solid strategy to address the approaching issues since the volume of data generated will expand tremendously in the future and the number of cyberattacks will increase accordingly. After additional investigation and testing, we anticipate that this method—or one like it—will be used for safety functions as the world becomes more digital.

Exploring alternative, more energy-efficient and scalable consensus mechanisms, such as proof-of-stake or practical Byzantine fault tolerance, could mitigate the computational overhead concern [50–53]. Developing techniques to manage blockchain storage requirements, such as pruning or sharding, could also help address the storage limitations. Furthermore, investigating the integration of blockchain with other emerging technologies, such as edge computing and machine learning, could enhance the capabilities and efficiency of the proposed model. Additionally, exploring interoperability and standardization efforts to ensure compatibility and seamless integration of IoT devices and blockchain platforms would be crucial for broader adoption.

Author Contributions: Conceptualization, P.S., A.S. and R.K.; methodology, P.S., A.S. and R.K.; software, P.S., A.S. and R.K.; validation, P.S., A.S. and R.K. formal analysis, P.S., A.S. and R.K.; investigation, P.S., A.S. and R.K.; resources, P.S., A.S. and R.K.; data curation, P.S., A.S. and R.K.; writing—original draft preparation, R.K.; writing—review and editing, P.S., A.S. and R.K.; visualization, R.K.; supervision, R.K.; project administration, R.K.; funding acquisition, R.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Toronto Metropolitan University, Faculty of Engineering and Architectural Science, And the APC was funded by Toronto Metropolitan University, Faculty of Engineering and Architectural Science.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

References

1. Kumar, N.M.; Mallick, P.K. Blockchain technology for security issues and challenges in IoT. *Procedia Comput. Sci.* **2018**, *132*, 1815–1823.
2. Hung, M. Leading the IoT, Gartner Insights on How to Lead in a Connected World. 2017. Available online: https://www.securityweek.com/mirai-basedbotnet-launches-massive-ddos-attack-streaming-service (accessed on 12 November 2022).
3. Lewis, T.; Liwen, W.; Safa, O.; Moayad, A.; Jalel Ben, O. Blockchain for managing heterogeneous internet of things: A perspective architecture. *IEEE Netw.* **2020**, *34*, 16–23.

4. Ali, F.; Aloqaily, M.; Alfandi, O.; Ozkasap, O. Cyberphysical blockchain-enabled peer-to-peer energy trading. *Computer* **2020**, *53*, 56–65.
5. Aloqaily, M.; Boukerche, A.; Bouachir, O.; Khalid, F.; Jangsher, S. An energy trade framework using smart contracts: Overview and challenges. *IEEE Netw.* **2020**, *34*, 119–125.
6. Hassan, W.H. Current research on internet of things (IoT) security: A survey. *Comput. Netw.* **2019**, *148*, 283–294.
7. Kushner, D. The Real Story of Stuxnet. 2013. Available online: https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet (accessed on 20 December 2022).
8. Arghire, I. Mirai-Based Botnet Launches Massive DDOS Attack on Streaming Service. 2019. Available online: https://www.securityweek.com/mirai-based-botnet-launches-massive-ddos-attack-streaming-service/ (accessed on 22 December 2022).
9. Subramanian, H. Decentralized blockchain-based electronic marketplaces. *Commun. ACM* **2017**, *61*, 78–84. [CrossRef]
10. Christidis, K.; Devetsikiotis, M. Blockchains and smart contracts for the internet of things. *IEEE Access* **2016**, *4*, 2292–2303.
11. Lee, I. The internet of things for enterprises: An ecosystem, architecture, and IoT service business model. *Internet Things* **2019**, *7*, 100078.
12. Radoglou Grammatikis, P.; Sarigiannidis, P.; Moscholios, I. Securing the internet of things: Challenges, threats and solutions. *Internet Things* **2019**, *5*, 41–70.
13. FIDO Alliance. How Fido Works. Available online: https://fidoalliance.org/howfido-works/ (accessed on 15 December 2022).
14. Tewari, A.; Gupta, B. Security, privacy and trust of different layers in internet-of-things (IOTS) framework. *Future Gener. Comput. Syst.* **2018**, *108*, 909–920.
15. Salman, T.; Zolanvari, M.; Erbad, A.; Jain, R.; Samaka, M. Security services using blockchains: A state of the art survey. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 850–880. [CrossRef]
16. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available online: http://bitcoin.org/bitcoin.pdf (accessed on 13 December 2022).
17. Antonopoulos, A.M. *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*; O'Reilly Media Inc.: New York, NY, USA, 2014.
18. Tschorsch, F.; Scheuermann, B. Bitcoin and beyond: A technical survey on decentralized digital currencies. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 2084–2123.
19. Ethereum Blockchain App Platform. 2017. Available online: www.ethereum.org/ (accessed on 22 December 2022).
20. Andreas, C.; Johannes, P.; Nikolas, S. Eine Marktübersicht der Blockchain in der Energiewirtschaft. Von der Idee zum Geschäftsmodell, von der Technologie zur aktuellen Anwendung. 2020. Available online: https://d-nb.info/121815991X/34 (accessed on 15 December 2022).
21. Khalilov, M.C.K.; Levi, A. A survey on anonymity and privacy in bitcoin-like digital cash systems. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 2543–2585.
22. Baraniuk, C. Bitfinex Users to Share 36% of Bitcoin Losses after Hack. BBC News. Available online: https://www.bbc.com/news/technology-37009319 (accessed on 20 October 2022).
23. Saad, M.; Spaulding, J.; Njilla, L.; Kamhoua, C.; Shetty, S.; Nyang, D.; Mohaisen, A. Exploring the attack surface of blockchain: A systematic overview. *arXiv* **2019**, arXiv:1904.03487.
24. Hyperledger. 2017. Available online: https://www.hyperledger.org (accessed on 11 December 2022).
25. Castro, M.; Liskov, B. Practical byzantine fault tolerance. *OSDI* **1999**, *99*, 173–186.
26. Sachs, G. Blockchain' Putting Theory into Practice. Available online: https://www.blockchain.com/ (accessed on 14 December 2022).
27. Gu, J.; Sun, B.; Du, X.; Wang, J.; Zhuang, Y.; Wang, Z. Consortium blockchain based malware detection in mobile devices. *IEEE Access* **2018**, *6*, 12118–12128.
28. Zhang, A.; Lin, X. Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain. *J. Med. Syst.* **2018**, *42*, 140.
29. Tao, F.; Wang, Y.; Zuo, Y.; Yang, H.; Zhang, M. Internet of things in product life-cycle energy management. *J. Ind. Inf. Integr.* **2016**, *1*, 26–39.
30. Gaetani, E.; Aniello, L.; Baldoni, R.; Lombardi, F.; Margheri, A.; Sassone, V. Blockchain-based database to ensure data integrity in cloud computing environment. In Proceedings of the Italian Conference on Cybersecurity, Venice, Italy, 17–20 January 2017.
31. Xie, S.; Zheng, Z.; Chen, W.; Wu, J.; Dai, H.N.; Imran, M. Blockchain for cloud exchange: A survey. *Comput. Electr. Eng.* **2020**, *81*, 106526. [CrossRef]
32. Lee, B.; Lee, J.H. Blockchain-based secure firmware update for embedded devices in an internet of things environment. *J. Supercomput.* **2017**, *73*, 1152–1167.
33. Boudguiga, A.; Bouzerna, N.; Granboulan, L.; Olivereau, A.; Quesnel, F.; Roger, A.; Sirdey, R. Towards better availability and accountability for IoT updates by means of a blockchain. In Proceedings of the IEEE European Symposium on Security and Privacy Workshops (EuroS and PW), Paris, France, 26–28 April 2017; pp. 50–58.
34. Dukkipati, C.; Zhang, Y.; Cheng, L.C. Decentralized, blockchain based access control framework for the heterogeneous internet of things. In Proceedings of the Third ACM Workshop on Attribute-Based Access Control, Tempe, AZ, USA, 21 March 2018.
35. Lone, A.H.; Naaz, R. Applicability of Blockchain smart contracts in securing Internet and IoT: A systematic literature review. *Comput. Sci. Rev.* **2021**, *39*, 100360.

36. Maesa, D.D.F.; Mori, P.; Ricci, L. A blockchain based approach for the definition of auditable access control systems. *Comput. Secur.* **2019**, *84*, 93–119.
37. Zhang, Y.; Yutaka, M.; Sasabe, M.; Kasahara, S. Attribute-based access control for smart cities: A smart-contract-driven framework. *IEEE Internet Things J.* **2020**, *8*, 6372–6384.
38. Nakamura, Y.; Zhang, Y.; Sasabe, M.; Kasahara, S. Exploiting smart contracts for capability-based access control in the internet of things. *Sensors* **2020**, *20*, 1793.
39. Abdi, A.I.; Eassa, F.E.; Jambi, K.; Almarhabi, K.; Khemakhem, M.; Basuhail, A.; Yamin, M. Hierarchical blockchain-based multi-chaincode access control for securing IoT systems. *Electronics* **2022**, *11*, 711.
40. Si, H.; Sun, C.; Li, Y.; Qiao, H.; Shi, L. IoT information sharing security mechanism based on blockchain technology. *Future Gener. Comput. Syst.* **2019**, *101*, 1028–1040. [CrossRef]
41. Jia, B.; Zhang, X.; Liu, J.; Zhang, Y.; Huang, K.; Liang, Y. Blockchain-enabled federated learning data protection aggregation scheme with differential privacy and homomorphic encryption in IIoT. *IEEE Trans. Ind. Inform.* **2021**, *18*, 4049–4058.
42. Alzubi, J.A. Blockchain-based Lamport Merkle digital signature: Authentication tool in IoT healthcare. *Comput. Commun.* **2021**, *170*, 200–208. [CrossRef]
43. Cha, J.; Singh, S.K.; Kim, T.W.; Park, J.H. Blockchain-empowered cloud architecture based on secret sharing for smart city. *J. Inf. Secur. Appl.* **2021**, *57*, 102686.
44. Sheron, P.F.; Sridhar, K.P.; Baskar, S.; Shakeel, P.M. A decentralized scalable security framework for end-to-end authentication of future IoT communication. *Trans. Emerg. Telecommun. Technol.* **2020**, *31*, e3815.
45. Chen, Y.; Li, M.; Zhu, X.; Fang, K.; Ren, Q.; Guo, T.; Chen, X.; Li, C.; Zou, Z.; Deng, Y. An improved algorithm for practical byzantine fault tolerance to large-scale consortium chain. *Inf. Process. Manag.* **2022**, *59*, 102884.
46. SHA 256 Algorithm Explained by a Cyber Security Consultant. Available online: https://sectigostore.com/blog/sha-256-algorithm-explained-by-a-cyber-security-consultant/ (accessed on 20 December 2022).
47. He, K.; Chen, J.; Zhou, Q.; Du, R.; Xiang, Y. Secure dynamic searchable symmetric encryption with constant client storage cost. *IEEE Trans. Inf. Forensics Secur.* **2020**, *16*, 1538–1549.
48. Yao, Z.; Tan, L.; She, K. 5G-BSS: 5G-Based Universal Blockchain Smart Sensors. *Sensors* **2022**, *22*, 4607.
49. Farahmandi, F.; Huang, Y.; Mishra, P. *System-on-Chip Security: Validation and Verification*; Springer: Cham, Switzerland, 2020.
50. Franco, C.; Walter, C.; Marco, R. Man-in-the-Middle Attack to the HTTPS Protocol. *IEEE Secur. Priv. Mag.* **2009**, *7*, 78–81.
51. Yeh, T.Y.; Kashef, R. Trust-Based collaborative filtering recommendation systems on the blockchain. *Adv. Internet Things* **2020**, *10*, 37–56.
52. Jebamikyous, H.; Li, M.; Suhas, Y.; Kashef, R. Leveraging machine learning and blockchain in E-commerce and beyond: Benefits, models, and application. *Discov. Artif. Intell.* **2023**, *3*, 3.
53. Saleminezhadl, A.; Remmele, M.; Chaudhari, R.; Kashef, R. IoT Analytics and Blockchain. *arXiv* **2021**, arXiv:2112.13430.