electronics

MDPI

Article

Schloss: Blockchain-Based System Architecture for Secure Industrial IoT

Fatemeh Ghovanlooy Ghajar *, Axel Sikora and Dominik Welte

Institute of Reliable Embedded Systems and Communication Electronics (ivESK), Offenburg University of Applied Sciences, 77652 Offenburg, Germany; axel.sikora@hs-offenburg.de (A.S.); dominik.welte@hs-offenburg.de (D.W.)

* Correspondence: fatemeh.ghovanlooy@hs-offenburg.de

Abstract: Industrial companies can use blockchain to assist them in resolving their trust and security issues. In this research, we provide a fully distributed blockchain-based architecture for industrial IoT, relying on trust management and reputation to enhance nodes' trustworthiness. The purpose of this contribution is to introduce our system architecture to show how to secure network access for users with dynamic authorization management. All decisions in the system are made by trustful nodes' consensus and are fully distributed. The remarkable feature of this system architecture is that the influence of the nodes' power is lowered depending on their Proof of Work (PoW) and Proof of Stake (PoS), and the nodes' significance and authority is determined by their behavior in the network. This impact is based on game theory and an incentive mechanism for reputation between nodes. This system design can be used on legacy machines, which means that security and distributed systems can be put in place at a low cost on industrial systems. While there are no numerical results yet, this work, based on the open questions regarding the majority problem and the proposed solutions based on a game-theoretic mechanism and a trust management system, points to what and how industrial IoT and existing blockchain frameworks that are focusing only on the power of PoW and PoS can be secured more effectively.

Keywords: security; trust management; authorization; authentication; blockchain; Industry 4.0; game theory

Citation: Ghovanlooy Ghajar, F.; Sikora, A.; Welte, D. Schloss: Blockchain-Based System Architecture for Secure Industrial IoT. *Electronics* **2022**, *11*, 1629. https://doi.org/10.3390/electronics11101629

Academic Editors: Junaid Arshad, Jonathan Loo and Omair Shafiq

Received: 19 April 2022
Accepted: 18 May 2022
Published: 20 May 2022

1. Introduction

The Internet of Things (IoT) has fundamentally altered how individuals interact with their environment during the last several years [1]. However, it may also be used in industrial domains, such as machinery, control systems, and information systems, as part of the so-called Industrial Internet of Things (IIoT) [2]. The IIoT seeks to revolutionize conventional production and usher in an intelligent age of highly linked machines. Industrial data should be collected and then utilized to improve production performance and management efficiency. However, owing to the geographical dispersion of IIoT devices and the variance of standards, connectivity is difficult [1]. Additionally, there are concerns about the security of the device's massive volume of data.

Despite the technical challenges, a vast number of companies have embraced IIoT solutions as a way to enhance their operations. However, as was quickly discovered, one of the major problems with this approach is that these new technologies greatly increase the industrial environment's exposure to cyberattacks [3].

Moreover, with the emergence of IIoT, the security vulnerabilities posed by it are even more devastating. As a distributed ledger and decentralized database, blockchain has the ability to establish a secure value exchange system. Due to its appealing characteristics, blockchain is an excellent option for use in IIoT systems [4]. Although IIoT and blockchain are two distinct technologies, their convergence represents a paradigm change that is predicted to boost industrial communication.

By adding blockchain to IIoT, the security risks are reduced due to the immutability feature of blockchain, and the system becomes more reliable [5]. The combination of blockchain and the Internet of Things (BIoT) has attracted a great deal of interest from academics and industry practitioners in recent years [6], and is viewed as a future trend in technological advancement.

However, there are some blockchain vulnerabilities, which will be detailed in Section 3. These vulnerabilities need to be considered and addressed by our proposed system architecture.

Furthermore, because it eliminates the need for a central authority, no individual can easily modify the network's properties to their advantage. Encryption by the blockchain adds an additional layer of protection to the system. This is why blockchain promises to solve the security challenges for the IoT, where most of the devices are connected through the public trustless and insecure Internet [7]. While the convergence of BIoT has the potential to address the significant shortcomings of current solutions, its adoption is still in its infancy, plagued by a variety of issues, necessitating the need to address significant challenges such as trust, privacy, authorization, and security. This finding has been considered as a possible cause of centralization in these cryptocurrencies' governance [8]. The implementation of blockchain-based IoT (BIoT) services is proprietary and autonomous, which makes confidence in IoT-based services an essential problem. Viriyasitavat et al. provide a proposed architectural design for Public Key Infrastructure (PKI)-based trust for BIoT services [9].

Rajendra Sai et al. argue that the majority problem of blockchain poses a security concern and is dangerous with regard to centralization [10]. However, the majority problem, including computing power and stake power, must be considered. Moreover, the degree to which blockchain is viewed as completely dispersed of power and fully distributed in order to prevent majority-related implementation difficulties is crucial.

Our proposed system architecture helps to improve security levels in communication and application. Moreover, it creates a trustworthy foundation for industrial factories to collaborate. The novelty of this work covers the above issues, such as trust issues and data privacy. The system architecture, which covers legacy machines, suggests an application-level authentication method based on a distributed trust management system. Regarding this system, we recommended authorized management that covers privacy, is resistant to hacking, and is a fault-tolerant system.

The main contributions of this paper can be summarized as follows:

1. We propose a system architecture to establish a secure IIoT environment by employing trust management and authorization management. The suggested system architecture is operating on the blockchain. In this architecture, manufacturing devices construct a private blockchain to cooperate and share their data and resources in a fully distributed fashion.
2. We suggest a dynamic authorization management that uses the result of trust management to control access of devices to the network.
3. We used a combination of ultimatum games and bargaining games to have fair taxation. Taxation-based game theory is used to design mechanisms that direct network nodes toward honest behavior. It is using rewards for the top trusted nodes as an incentive and blocking deposits as a punishment for malicious nodes.

The rest of this paper is organized as follows. Section 2 addresses the state of the art, while Section 3 discusses security and trust issues. Section 4 describes our system architecture, which is to be implemented as a next step. Finally, Section 5 brings this paper to a conclusion.

2. State of the Art

Today, as the internet and the Internet of Things grow in popularity, the necessity for the communication and administration of distributed devices becomes apparent. Numerous academics have integrated blockchain technology into the Internet of Things, allowing

apps to operate only via a trusted middleman [11]. Blockchain, which is tamper-proof and has high-level data security and distribution coordination, is a great choice for the foundation of home and business networks with many IoT devices. Two successful instances of this concept are proposed and implemented in the following works: Dorri et al. present a hierarchical design for the Internet of Things based on blockchain, using the smart home as an example [12]. It is divided into three tiers: the local network (which utilizes a private blockchain), the overlay network (which utilizes a public blockchain), and cloud storage (with a private blockchain). The solution addresses the problem of identity and the majority of security and privacy issues, while also taking into account the primary concern of resource restrictions in IoT devices. Nonetheless, since the local network layer is not disseminated, its availability is limited. Moreover, Panda et al. presented a decentralized architecture based on blockchain technology that is capable of effectively managing numerous smart devices [13].

Nonetheless, one of the most critical concerns in computer networks is how to keep nodes safe and secure when they utilize the network and interact with each other. However, authentication and authorization are the two most critical aspects of this subject. Khalid et al. propose an IoT authentication and access control technique that enables safe communication between devices that are part of the same IoT system, as well as between devices that are part of other IoT systems [14]. However, there is still centralized administration in place, providing a single point of failure. For this reason, it is suggested that blockchain be used to aid with authentication and authorization.

Wu et al. suggest a two-factor authentication approach that makes use of blockchain-enabled device interactions. Even if the first factor fails (e.g., the attacker steals the access token), the secondary authentication technique may prevent external malicious devices from gaining access [15].

Jia et al. offer the A2 Chain, a decentralized IoT authentication strategy that combines application-domain blockchains with alliance blockchains and provides a safe authentication information exchange procedure [16]. Ferreira et al. propose an API gateway for IoT devices and a network gateway for message signing, identification, and authorization. This is accomplished by utilizing the keys and fundamental characteristics of previously registered devices on the blockchain [17].

As the trust issue is an important factor in human societies, it is also one in computer networks. Using the trust factor in these networks can assist with authentication and authorization. There are some studies that use the trust idea: Hammi et al. propose a unique architecture for Semantic Web of Things (SWoT) systems that is based on blockchain [18]. The resource discovery layer utilizes smart contracts to conduct registration, discovery, selection, and finalization processes in a distributed and trusted way, with each transaction maintaining a verifiable record on the blockchain. However, the suggested architecture is limited in its use due to the private blockchain. Hammi et al. propose BCTrust, a strong, transparent, flexible, and energy-efficient blockchain-based authentication mechanism optimized for devices with computational, storage, and energy consumption restrictions [19].

Unfortunately, despite the importance of distribution in industry topics, authentication and authorization for distributed devices receive less attention in industry research. A data breach in IIoT systems might have disastrous consequences for the industry, the factory, or even key infrastructures, such as the water supply system and electrical power grid. As a result, authentication and authorization are the most significant security problems in both the IoT and the IIoT.

Some research is described in the following that indicates how authentication systems are being used for industrial reasons, with an emphasis on distributed issues: Yu et al. propose a blockchain-based anonymous authentication with selective revocation for smart industrial applications that supports attribute privacy, selective revocation, credential soundness, and unlinkability across several shows. Specifically, an efficient selective revocation process based on dynamic accumulators and the Point–Chevy and Sanders signature algorithm is proposed as an overlay on the BASS technique [20]. Lupascu et al. describe

a decentralized authentication and integrity assurance framework for IIoT devices that utilizes a private blockchain and master nodes to monitor the administrators' policies [21].

Kim et al. present a private blockchain system based on field-programmable gate arrays (FPGAs) for boosting the integrity and trustworthiness of IIoT device data [22]. A soft processor, PUF, external register, and local memory are combined into the bitstream-protected FPGA to create a transaction in an isolated and enclaved manner [23]. Xu et al. propose a revolutionary blockchain system based on FPGAs. It makes use of the FPGA to provide a simple yet efficient trusted execution environment for IIoT devices and eliminates the need for a single root of trust by enabling all stakeholders to participate in device management [24].

Table 1 shows an overview and comparison between the mentioned works. Based on this table, the requirements of blockchain-based projects are examined. The proposed systems' security level is also determined by the authentication level and the procedures they use, as well as the access control mechanisms they employ. These discussions are a guide to suggestions and innovations for future research and suggested models.

Table 1. Overview of state of the art for secure blockchain applications.

#	Technique	Fully Distributed	Security Level	Blockchain Type	IIoT Suitable
[15]	Two-factor authentication scheme	✗	***	Eris	✓
[19]	Blockchain-based authentication mechanism	✓	***	ETH	✗
[13]	IoT devices are not included as a part of the blockchain network	✗	**	ETH	✗
[16]	Edge computing to decentralize the processing of authentication requests via identity-based cryptography (IBC) algorithm	✗	**	N/A	✗
[20]	Anonymous authentication with selective revocation with blockchain	✗	***	ETH	✓
[22]	PUF- and FPGA-based	✗	***	N/A	✓
[14]	Fog computing cryptographic properties	✓	**	ETH	✗
[17]	API gateways network's edge	✗	*	ETH	✓
[21]	Architectural framework	✗	**	Fabric	✓
[25]	Trust management framework	✗	***	N/A	✓
[26]	Dynamic trust management model	✗	*	N/A	✓
Schloss	Dynamic trust management model based on game theory	✓	***	ETH	✓

3. Security and Trust Issues in Industrial Blockchain

The vulnerabilities concerning blockchain and the Industrial IoT are discussed in this section. In order to highlight the system's weaknesses as well as showing how to overcome them, the most serious assaults that can possibly be launched against the IIoT blockchain have been chosen.

3.1. Security Issues in Industrial IoT

Security in IT often assumes a client–server model, where communication between the client and server happens using well-known protocols such as IP, TCP, UDP, or HTTP. The damage caused by a successful attack usually involves money or reputation, and rarely involves safety threats. However, OT systems were designed to operate industrial processes safely and reliably. Isolating the OT networks may prevent an attack from a

different network, but it cannot prevent the attacks inside the network. Inside an isolated network, malware can be effectively deployed to compromise the system. Hence, we need to study the possible attacks at various levels of the IIoT architecture.

We can list the attacks on an industrial infrastructure by the path or means by which an attacker can gain access to a computer or network. Attack vectors are subdivided into cyberattacks and physical attacks. The cyberattack vectors contain the entry points in IT networks wherein no physical access is required, whereas the physical attack vectors need the attacker to interact with the device or people in the industry. Various attack vectors listed in the taxonomy are as follows:

Spoofing: In a spoofing attack, an attacker acts on behalf of another person by impersonating a legitimate user, which allows the delivery of a payload into a system. Using techniques such as IP spoofing, the attacker can change the emerging or source IP address of packets. In industrial devices, authentication happens only at the beginning of the session. Hence, an attacker can craft the packets with an authenticated IP address to send malicious code [27].

Replay: A replay attack is the repeated transmission of valid data or requests maliciously or fraudulently. Here, the valid request can be captured and resent after a periodic interval to send time-critical data, which can raise false alarms in industries [28].

Code Injection: Code injection happens when malicious code is passed as input to a vulnerable computer program or web application, which results in unexpected output [3].

Session Hijacking: Session/HTTP cookies are used to validate a session; if an attacker can steal the live session cookies, he can take over the session, which is known as session hijacking. Session hijacking can be prevented by using hashing techniques [3].

Malware: Malware comprises a huge collection of potential unwanted programs that are designed for malicious purposes. In IIoT, malware is the most common attack vector [28].

Device Tampering: In this type of attack, the attacker, having physical access to the device, interferes with the device to disable the security mechanisms applied to it. Some devices have a hardware lock that restricts any modification in the configurations of the device [29].

3.2. Security Issues in Blockchain

With the continuous growth of global attention towards the blockchain, blockchain-related research is expanding significantly. However, objectively, as seen from the application layer, blockchain is still in its exploratory stage. There is still a long process of integration and development ahead until a profound combination of this technology and the application layer can be achieved. Despite the innovative changes of blockchain, the technology itself still has some inherent security risks. Moreover, the revolutionary nature of decentralization and self-organization in blockchain has already triggered security problems that cannot be ignored.

Vulnerability of cryptographic operations: Blockchain security depends on the strength and robustness of the cryptographic primitives used to conduct transactions and maintain a detailed history of past activity [30].

Cryptographic key vulnerability: Some of these standardized elliptic curves either have theoretical weaknesses or were generated using questionable parameters. For example, the NIST P-256 curve is viewed skeptically by some cryptographers because the derivation of the curve parameters is not well explained and they allow for some possibility of manipulation such that the curve may contain intentional weaknesses or backdoors [31]. There is some precedence for this type of intentional weakness, as NIST previously published a standard for a supposedly cryptographically secure random number generator based on elliptic curve operations called Dual_EC_DRBG, which is known to have serious design flaws [32].

Replay attack: Stealing the key and reusing it to make the attacker a valid user is a common threat to the blockchain community. However, using a key pair-based exchange protocol is effective to protect users from these types of attacks [33].

Sybil attack: These are general types of attacks on peer-to-peer networks in which multiple fraudulent identities are created and controlled by a single rogue entity. In

blockchain networks, this type of attack is used to isolate a target node from the rest of the honest network, which in turn is used to launch different types of attacks [34].

A blockchain framework called TrustChain [35] tackles this issue by using an immutable chain. This chain is the product of interactions between each user, which is temporally ordered. It computes the trustworthiness of an agent in an online community based on prior history. It uses a system called "NetFlow", which makes sure that every user who is consuming resources is also sharing some resources back to the other nodes in the network.

Manipulation-based attacks: Various types of routing attacks are possible, where one or more nodes in a blockchain network may be partially or fully partitioned from the rest of the network for malicious purposes. Using such attacks, it may be possible to delay the block propagation time for a significant amount of time, perform DoS attacks, isolate a large portion of the network's mining power, and perform other attacks [33].

3.3. Possible Attacks on IIoT Blockchains

IIoT infrastructure comprises various components, which are needed for the proper functioning of the industrial process. Each of these components can have a security vulnerability and hence can be the target of attacks. A list of attack targets is given below:

Industrial Network: Industrial networks can be a target of an attack as most industrial protocols do not implement proper authentication and encryption [36]. We will discuss this in detail in the next section.

Workstation: Workstations are targeted to mislead the operator to perform certain actions or manipulate the alarm system. A successful attack can manipulate the behavior of the machines without the knowledge of the operator [37].

Data Server / Auxiliary DB: servers are used to host information about the industrial system, which is used to share necessary information with the stakeholders. Potential attack surfaces are malware, spyware, trojans, viruses, and worms and unauthorized access [3].

Sensors: These devices are used to detect or measure a physical property such as temperature, pressure, flow, etc. Potential attack surfaces are reverse engineering, malware, injecting crafted packets or input, eavesdropping, and brute-force search attacks. Because we do not have security protocols in this section and physical layer, the issue of security is becoming more important [37].

Actuator and Machines: This is a fundamental component of a machine, responsible for moving and controlling a mechanism or system by sending appropriate signals to the devices. Possible attacks are the same as with the sensors and edge devices [38].

Human: Social engineering attacks are targeted towards humans, such as operators and other employees, wherein the employees are deceived into revealing confidential data [38].

General Network Infrastructure: In industrial environments, certain devices are used to manage or operate other devices, such as routers and power controllers. DNS cache poisoning attacks target the routers to manipulate the flow of traffic on the network [38].

4. Proposed System Architecture

Manufacturing is frequently dispersed around the globe to make use of the most cost-effective raw supplies, labor, capital, and customer markets. Because organizations are linked by extensive, multinational supply and demand chains, a failure in a single vital link may bring the entire operation to a stop.

Across corporate and national boundaries, blockchain offers reliable data sharing and process automation. Monitoring the source of components and produced items helps to rebuild weak supply chains and commercial connections that have been decimated by an epidemic [39]. It also allows more ethical purchasing [40].

This section aims to provide a tamper-proof and secure foundation to help with the collaboration of different industrial factories. By using this system architecture, separate parts of industry components are able to securely share data and resources. In addition, this system architecture provides a foundation for the distributed management of the whole network.

4.1. Physical Aspects

According to Figure 1, we have a set of factories that work together. This cooperation is based on the common interests that industrial factories have with each other. Based on these common interests, they need to share their resources and work together. Therefore, they need joint decisions and the approval of all members of the group of factories. This gathering shares data, storage, and computing resources. Therefore, these factories can help to solidify each other's strengths by sharing resources and joint decisions and meeting each other's needs and have better efficiency in producing final products. In addition, this collaboration appears even more successful in financial markets. Therefore, this partnership causes their progress and growth.

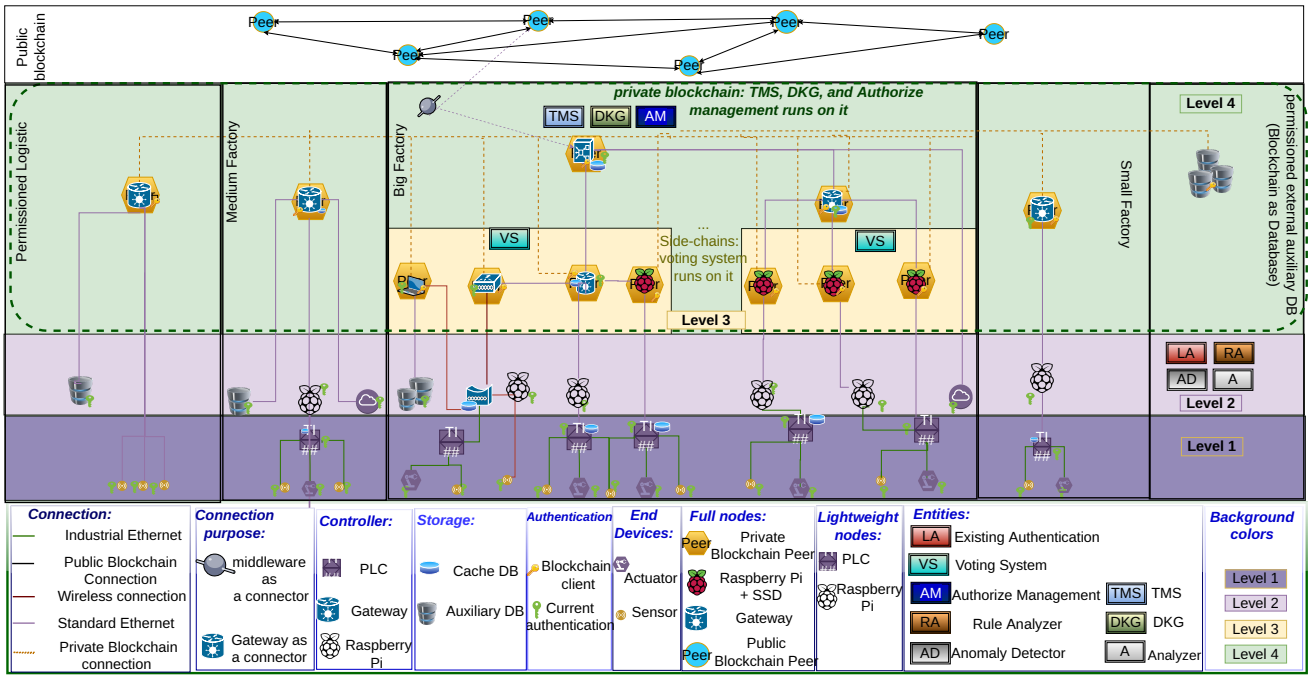

Figure 1. General Schloss architecture.

On the one hand, data sharing and transparency of information shared between factories is essential for the fulfilment of their purpose. On the other hand, ensuring the security and immutability of the data after sharing is a prerequisite for the formation and continuation of this cooperation. By using blockchain, we can ensure that data are shared transparently among blockchain members. As a result, they cannot be changed by malicious agents after this. Moreover, the interaction of company members as blockchain nodes and the use of consensus algorithms and blockchain services, such as smart contracts, allows companies to make joint decisions by interacting with each other.

There are several machine sets in a plant. As a result, the data produced by these machines, as well as the environmental sensors, are sent through industrial Ethernet to a PLC, and then via conventional Ethernet to a gateway or Raspberry Pi. Due to the limitation of end devices in terms of memory, processing capacity, and internet connection, level 1 and 2 in Figure 1 are handled in the usual manner by a central management system. Raspberry Pi devices and gateways have the potential to be utilized as blockchain clients. After this, the data are sent to the full nodes, and the rest of the operations for calculating trust and authorization management are performed in a decentralized way. Data are then stored on the blockchain or in an auxiliary database.

The data flow from the end devices to the auxiliary database and the endpoints of the different blockchains. In the interim, to prevent data loss, we installed caching databases on the points sending data. Additionally, by using the "OPC UA" historical data protocol in devices capable of re-sending data from a certain era, we ensure that we will not lose

any data in the event of a temporary loss of connection [41]. In the logistics industry, where items are transported to their final destination, only the data collected from sensors are relevant to the nodes, which are recorded by the gateway and subsequently sent to the database and the private blockchain node. Of course, the gateway, as with the other gateways in this architecture, is capable of data processing, which enables it to preprocess data received from sensors and to limit the amount of data being sent.

The sensors communicate with the PLC, which communicates with the gateway. The PLC communicates with the actuators. Depending on the data type and the factory's internal privacy, the gateway decides whether to store the data in the auxiliary database, private blockchain, or public blockchain peers. Additionally, if the members of the private blockchain agree, part of the information recorded on the private blockchain may be transferred to the public blockchain through middleware acting as an adapter between the different blockchains. Naturally, since this is a public blockchain with no access limitations, all data are public, and it must be established in advance, in accordance with each company's standards, whose data and information will be transferred to the public blockchain and made publicly accessible.

The ability to establish access privileges in a private blockchain alleviates worries about the security of data shared between businesses. As a result, constraints on each job may be enforced depending on the factories' or private blockchain component committee's internal regulations. However, access will vary according to the use case. As a result, it is advisable to verify specifics in each use case, where data types and access privileges may be provided. Integration of blockchain technology into IIoT systems enables automatic communication between potentially faulty, dispersed, and verified devices. The blockchain layer may be thought of as a conduit connecting the communication layer to industrial applications. Users may access blockchain-based services.

4.2. Issues

There are a number of Industry 4.0 difficulties that blockchain technology may readily address. This technology can digitally save all data in order to improve industrial operations. Only with the right personnel will a company be able to adopt new technologies while being profitable. With correct application, this technology can address data privacy concerns. Many companies can simply share data and enable cross-organizational data sharing. Another key source of concern is the potential of present and emerging manufacturing weaknesses. Smart factories on the blockchain provide real-time interoperability. This technology is capable of connecting to one or more networks. Any of these pieces of equipment might have flaws, making the system open to attacks. Various security challenges can be addressed by Industry 4.0.

The future of IIoT applications is based on trustful data exchange between various devices. In order to enable trustful cross-platform IoT collaboration, we aim to design our trust management and authorization management system to effectively address the following objectives:

1. How to create trust in the product and provide product traceability for your customers.
2. How to create a trusted environment for factory internal devices and ensure that results or operations are not compromised by a malicious actor. This addresses the concern of factories that rely solely on physical isolation and ignore cybersecurity in the factory environment, particularly with older machines.
3. How to create secure and trustworthy collaboration between factories to share data and trust each other.

4.3. Addressing the Issues

Addressing Issue 1: Customers can monitor and inspect items through a smart tag thanks to the notion of utilizing the public blockchain and an interpreter to convey information about them. Moreover, using crypto-anchor plugins, Parda et al. provide a platform

that gives a generic representation of an item protected by a crypto-anchor and supports any number of product authentication mechanisms [42].

Hence, each product is assigned a unique identifier to facilitate tracking on the blockchain. Additionally, a check mark for end consumers may be used. In this way, we have two-way communication via, e.g., an app. The customer can scan the code and validate it on the blockchain. The code contains unique aspects of the product. This way, it is simple to detect fake QR codes, e.g., unique aspects do not match the fake QR codes.

Monitoring the blockchain to avert any illegal activity involving the theft of information from one product and reselling it under a different smart tag can be used to spot such occurrences. It is managed in this manner through the collaboration of private and public blockchains, therefore guaranteeing to safeguard the shared data and the privacy of businesses. Additionally, it educates the consumers about product tracking and ensures that they are aware of the product's authenticity. Honest and trustworthy nodes have access to the network and disseminate data based on TMS output and permitted management responsibilities. They are capable of addressing the issue.

Addressing Issue 2 The system design ensures the security of the OT and end devices. They use existing authentication with existing protocols such as PROFINET/OPC UA to authenticate and receive a valid certificate. As a result of not directly connecting end devices to the internet, the danger of direct access by malicious agents is reduced with this system design. Additionally, a network anomaly detector, used to identify any anomalies inside a business, exists. Finally, with the use of the TMS and an authorized management system, users' access to the network is determined by their trust value. This entire technique is dedicated to resolving the issue.

Addressing Issue 3 As mentioned earlier, the TMS and DKG committees are supported by all full nodes from all factories, and hence each plant has a representative on both committees. To do this, the most trustworthy node is picked. As a consequence, this collaboration across factories and within private blockchain networks is secure. Regarding DKG, all significant transactions are approved by the DKG committee, and they require consensus and majority consent to open. As a result, data privacy is a major priority in this system architecture.

4.4. Definition and Benefits

The proposed system architecture introduces a network of industrial factories that come together for specific purposes, such as secure data sharing or sharing computational resources. Communication and connections in this architecture are divided into three main parts:

1. Intra-factory communication, where devices within a factory collaborate and exchange collected data; no data are written to the blockchain for privacy and performance reasons.
2. Communication between factories, which contains communication between private blockchain nodes and factory full nodes, where it is decided which data must be shared based on privacy rules.
3. Communication between private blockchain nodes and public blockchain nodes, i.e., which data must be shared with the public blockchain.

Important components for this architecture are:

1. Devices, which can be a full node or a light node, depending on the characteristics of the device and its position in the network in the proposed architecture.
2. Roles that devices have in the network; based on its role, a device can have access to the network or not. The roles are predefined, but can be changed based on the behavior of the device access level.
3. Another important component to consider is legacy devices and legacy protocols. To have a secure system, legacy devices must be able to connect to the blockchain. Using the output of legacy protocols can also be helpful for the trust management system.

As mentioned earlier, the main concern is to establish a secure connection between the factories' devices. It is also necessary to integrate legacy devices into the blockchain network with minimal cost. Overall, adding a simple and inexpensive device (e.g., Raspberry Pi)

to the legacy system enables the execution of our system architecture. This allows us to establish a secure connection between factory nodes and have distributed authentication and authorization that is compatible with the legacy system. As shown in Figure 2, the system consists of two layers, the first of which is implemented in each factory. This layer contains lightweight nodes or blockchain clients, which mainly comprise end devices (sensors and actuators). Due to the idea of keeping legacy machines (and not replacing them due to the high investment cost of new acquisition) and their inability to connect to the internet or lack of memory and processing power, we added a Raspberry Pi running existing authentication, rule analysis, anomaly detection, and intrusion detection.

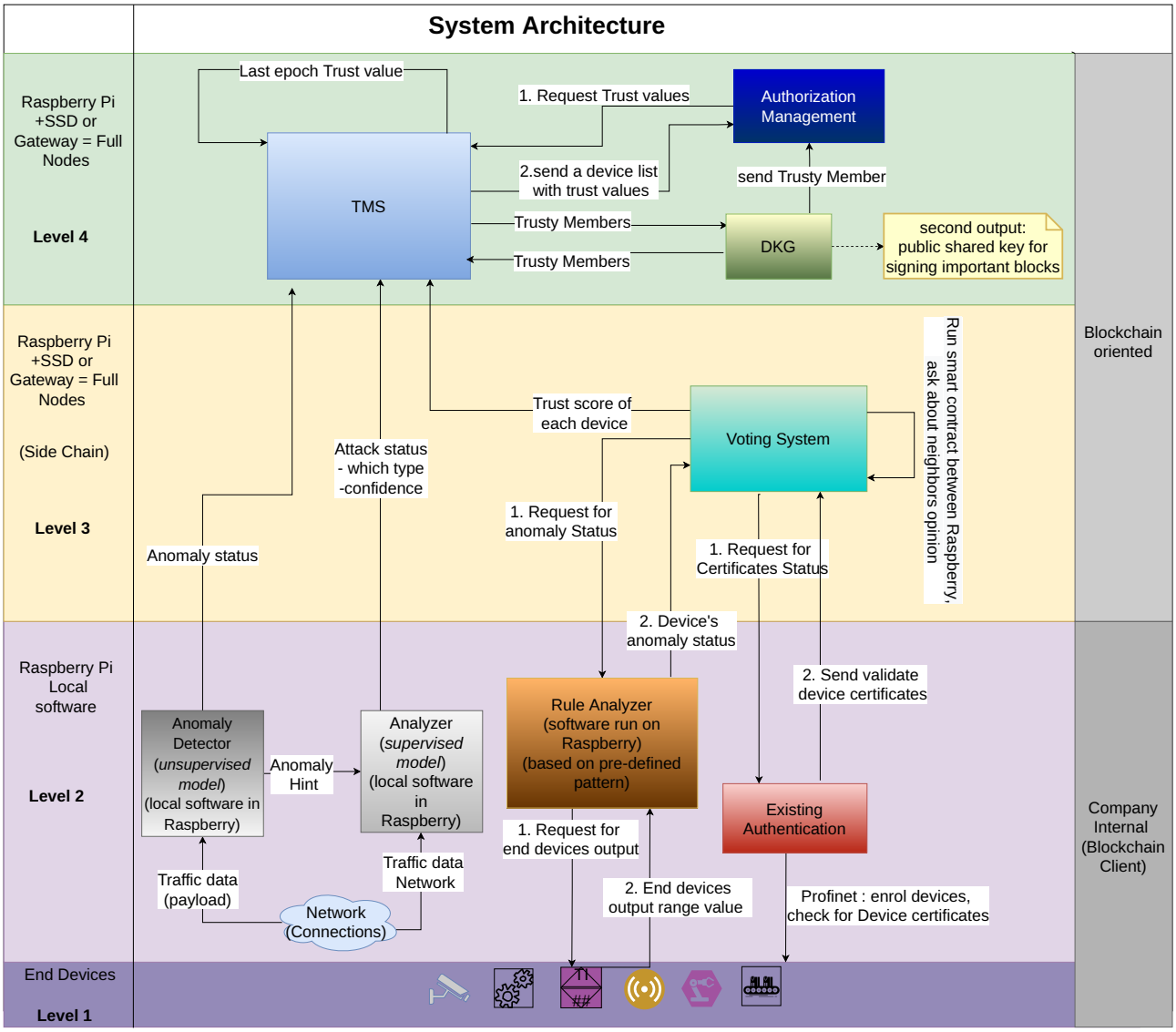

Figure 2. Hierarchy diagram of the Schloss system architecture.

The second layer, which includes the private blockchain, contains the full nodes that run entities such as the voting system, TMS, DKG, and authorization management. The voting system has to be implemented at the side blockchain level due to the need for voting by neighboring partner nodes, so the smart contract can only be executed in the local subnet.

4.5. Logical Aspect and Mechanism behind the System Architecture

In this system architecture, the main focus is on the interaction between full nodes to run the system. The second-layer entities are run on an Ethereum private blockchain platform that is running on factory devices. Therefore, the trust management system

and decentralized authorization run in a distributed manner on these nodes. The entities running on the blockchain for the execution process need consensus and the algorithms are executed through smart contracts.

By running the system on the devices of the participating factories, manipulating the results or voting incorrectly on an option can be in the best interest of the participating nodes on the blockchain. An example of this would be to vote for a competing factory node with a "low trust value" or to vote with a "high trust value" for one's own node or a partner factory node. The nature of the blockchain prevents this in part by consensus. However, consensus cannot avert all attacks of this kind: if a participant can obtain 50% + 1 of the votes, he can change the results in his favor.

To prevent this, we have defined a mechanism of incentive and punishment. Defining a system strategy based on game theory helps to define the process of the entity algorithms implemented in the second layer so that honest behavior prevails and everyone reaches the point of Nash equilibrium [43]. At this point, the behavioral strategy of each node moves in the right direction, meaning that honest behavior is the best strategy for the participating nodes.

4.6. System Level and Entities Proposed

Central administration is not necessary in this system architecture, because of the distributed manner and interaction of the majority of components as blockchain nodes. Along with existing authentication, we need a blockchain-based authentication system. Additionally, authorized administration is essential to maintain an integrated system and to guard against malicious access and harmful behavior on the part of malicious agents.

Both systems require certain variables to calculate and evaluate these network component conditions. The trust value of each node in the network, which is determined by the trust management system, serves as the starting point for these calculations (TMS).

The trust value is determined by many criteria, including the device's behavior in relation to its neighbors' judgment of its dependability, the device's history of behavior, the influence of device performance within the network, and the device's certification status in the existing authentication system. Depending on the level of privacy and network behavior, we may need many entities at various tiers to guarantee that the stated criteria are completely accessible to fulfill all the parameters.

As shown in Figure 2, the system architecture is hierarchical at two layers: within the factory and at the blockchain. Data are passed from the bottom of the diagram, from the end devices and light nodes, to the private blockchain and the full nodes for processing and decision making. Additionally, it contains four levels, which are detailed in the next subsections.

This system's ultimate purpose is to strengthen security by using distributed authentication and authorized management. This makes it more difficult for hackers to obtain access to system data. This system is composed of the following components: the end device's existing authentication, rule analyzer, anomaly detector, and analyzer will be discussed in Section 4.6.1. The voting system, TMS, DKG, and authorization management will be discussed in Section 4.6.2.

As previously mentioned, the objective of this system architecture is to enable safe communication and network security between several factories with shared interests and benefits. A distributed platform is required because industrial factories are geographically dispersed. Additionally, as a result of the high cost of machine replacement, the greatest issue is keeping legacy machines updated and capable of utilizing modern technology. As a result, the suggested solution is divided into two parts: one inside the factory (blockchain client) and the other on the blockchain (full nodes).

In the first part, due to the presence of legacy machines and related technologies, centralized management is required in the end devices among factories and within the subnetwork of each factory. This central/semi-central management enables legacy machines and end devices to connect to a private blockchain in order to cooperate across all factories and use all the legacy platform's capabilities. It is needed in order to use existing authentication methods and in order to monitor the network for anomaly detection.

By applying all this to legacy and end device parts, it is possible to have some assistance by adding a Raspberry Pi and running all entities on it. The combination of these entities in this layer makes it possible for the system to protect these two layers and send updates regarding network and device situations to the blockchain part and obtain feedback to change access levels depending on the behavior and trust situation of devices. The coupling of the entities operating on the additional Raspberry Pi to the legacy portion enables this part to be controlled and managed semi-centrally for each factory subnetwork.

On the other hand, distributed management encompasses both full nodes and side chains in private blockchains. The voting system entity is spread over each side chain via smart contracts and votes for subnetworks. However, the remainder of the entities responsible for authentication and authorization are spread across all full nodes, with all factories totally dispersed via full node consensus.

Figure A1 shows the cooperation of the entities in an epoch. An epoch is a time interval during which the complete system is run, and trust values are determined. The control analyzer evaluates the behavioral and physical aspects of light nodes that generate data (sensors) and operate with their environment (actuators).

4.6.1. Central Management

As previously stated, there is presently no way to link end devices directly to the blockchain due to their inherent limitations. This is why we refer to it as central management and consider gateways or a Raspberry Pi to be blockchain clients or lightweight nodes, upon which full nodes may decide and act upon depending on the data supplied by these lightweight nodes.

Level One

The end devices are positioned at this level. For the majority of the time, they are connected through industrial Ethernet. Due to the nature of this level, physical constraints apply and there is no internet connection. Level two controllers transmit all outputs and inputs, and devices are authenticated using the existing authentication technique. Due to the limitations of end devices, this level has no direct link to the blockchain, but it is managed by the second level's light nodes.

Level Two

At this level, controllers, such as the Raspberry Pi and PLCs, are linked through standard Ethernet. Additionally, they may be employed as blockchain lightweight nodes in the system's architecture. Typically, lightweight nodes have fewer resources. They are limited in their capacity to store and process modest quantities of data per blockchain. Lightweight nodes trigger new transactions, which are subsequently distributed to full nodes. The new blocks are then added to the blockchain through a consensus process.

This level has four components: existing authentication, rule analyzer, analyzer, and anomaly detection.

Existing Authentication: Communication is encrypted, and each client must submit a client certificate that is compatible with the protocol. This is used to authenticate its affiliation (i.e., the organization to which it belongs) and access privileges. No client may access the blockchain and make modifications without a valid certificate. Full nodes or light nodes with sufficient power to operate protocols, such as OPC UA and PROFINET, or nodes that are part of the private blockchain, may conduct existing authentication. However, existing authentication does not imply that contemporary factories are unprotected or lack an authentication system. They may use certain authentication systems and protocols, which we should include into our suggested system, since overhauling the whole system would be too expensive and unfeasible. As a result, it employs standard authentication mechanisms and stores its credentials in a private blockchain for each device.

Rule Analyzer: Each device has its own peculiarities and, of course, its own unique hardware features. Each device's output may have its unique pattern. Thus, by creating

a pattern for each kind of device's features, the output of the device may be monitored using a pre-stored pattern. If a device develops a malfunction or exhibits unusual behavior while being attacked, the system will report an anomaly. The output of devices serves as the entity's input. It compares outputs to the device's stored pattern. The experiment's output is the anomaly state of each device, as well as a suggestion to the human agent.

Anomaly Detector: This is an unsupervised machine learning model that is used to identify network anomalies. The machine learning model has been trained on a data collection of network anomalies, and it performs a payload analysis on the network. This model continuously monitors the network and transmits data to the TMS, analyzer, and human agent.

Analyzer: This is a supervised machine learning model that is used to identify network attacks. The machine learning model has been trained on a data set of network attacks. This model continuously monitors the network and transmits data to the TMS and the human agent.

4.6.2. Distributed Management

In this stage, the data are being distributed to all the nodes and the remainder of the actions are fully decentralized. Calculating trust values, making permission decisions, and managing all associated tasks are all decentralized.

Level Three

A regular Ethernet connection and the internet are available at this level. It comprises many full nodes. Typically, full nodes are required to load and verify all blocks and chain transactions. These nodes may also operate as mining nodes, generating blocks for the blockchain. Any device with adequate storage space and processing power to process and run the blockchain node is considered a full node. To add older devices (legacy devices), a Raspberry Pi with an extra SSD may be added to operate a full blockchain node. At this point, the sole point of contention is the voting mechanism. Due to the need for neighbors' local reputation, each subnetwork has its own side chain. Each side chain has a number of full nodes that operate voting systems for their respective subnetworks.

*Voting System:*The voting system obtains certificate and rule anomaly status and, using them as inputs, requests the opinion of their subnet device for the trust in their neighbor. In order to create a trust preference list across subnets, voting is required for this purpose. Due to the necessity for exact opinions and to prevent the manipulation of network opinion results via unpriced votes or malicious behavior, a tax mechanism must be designed using game theory. The tax amount is used to transmit funds around the network, and the tax total for each epoch is used to reward the most trustworthy nodes.

A deposit is also required in order to participate in the voting process. To penalize malicious nodes for cheating, the blockchain will block deposits in the event of cheating. In order to attain this objective, it uses a mix of ultimatum games and negotiating games to ensure equitable taxes. Taxation-based game theory is used in the design of systems that steer network nodes toward honest conduct. As an incentive, it blocks deposits for poorly behaved nodes and provides prizes to the most trustworthy nodes. The voting is handled by a smart contract on the side chain, and the Schulze method [44] is used to rank the sub-network's community preference list in the entire node.

Level Four

This is the section reserved for private blockchain transactions. It holds all the full nodes, along with those with whom they have communicated via the internet. This level contains entities such as the TMS, the DKG, and the authorization management system.

*TMS:*Trust management is a generic term that refers to an abstract system that manages symbolic representations of social trust. It is a completely decentralized trust management system that is managed by full nodes (a fair distribution of full nodes among all companies). This system's output enables the specification of trustworthy nodes in the network. "Trust value" is a critical characteristic of the TMS. This trustworthiness is the numeric output of the TMS, which ranges between 0 and 1 and indicates a device's or person's dependability.

DKG: A DKG is a cryptographic approach that involves many parties participating in the computation of shared public and private key sets [45]. In contrast to the majority of public-key encryption approaches, distributed key generation does not depend on third-party trust. Due to the participation of several parties, distributed key generation is required to preserve confidentiality in the event of malicious contributions to the key computation. DKG obtains a list of trustworthy members from the TMS and then establishes consensus on a higher level of trustworthy members in order to form a committee of trustworthy full nodes for the private blockchain. DKG produces trustworthy members and shared public keys for signing spatial data in blocks.

Authorization Management: Authorization management is a committee of trustworthy full nodes of the private blockchain that determines access to the network for the next epoch based on the trust value determined for each device from the TMS and the function of each device. At the conclusion of each epoch, the authorized management output is computed. Different access levels are provided to devices based on their determined trust values to avoid harmful behavior by untrusted devices that might be manipulated by an attacker.

4.7. Application of System Architecture

The suggested system design, as described in Section 4.3, facilitates clear and trustworthy communication between industrial partners and provides transparency and product traceability for end customers. A strong justification for employing this system design is that it is advantageous for end users and industry stakeholders to have a trustworthy environment in which to share data and resources without fear of malicious behavior. The capacity to shift power from nodes with large processing power or wealth to the most trustworthy nodes as a consensus commitment for TMS, DKG, and authorized management is an additional strength of this system architecture, reducing the influence of the majority in the factory community.

However, distributed decision making for a network is achievable, even for nodes in small factories, assuming that they are trustworthy. It aids in making impartial judgements and finding the most dependable nodes based on their behavior. On the one hand, the incentive mechanism behind taxation encourages them to contribute, specifically so that they may win a prize. On the other hand, due to taxation and the payment of deposits to network members, they also block deposits for nodes with poor conduct, as punishment serves to minimize bad behavior and reduces the likelihood of an attack in the proposed system architecture. It is expensive for cybercriminals and harmful nodes. Ultimately, based on logic and Nash equilibrium, all nodes will move to a position where being honest is most advantageous for them.

In the real world, Ghanaian oil businesses will utilize this system design to collaborate and share product information with final consumers.

4.8. Security Analyses

The suggested architecture's privacy and security are discussed in this subsection.

Privacy: The usage of private and public keys is a crucial feature of privacy in blockchains. Blockchain systems use asymmetric cryptography to protect user transactions. Each user in these systems has a public and private key. These keys are random sequences of integers that are connected cryptographically. It is technically impossible for a user to deduce the private key of another user from the public key. This makes it impossible for malicious nodes to track an overlay node. Furthermore, authorization management prevents network access for nodes that are not trustworthy or have recently enlisted.

Security: Blockchain is primarily accountable for the design's security. Each transaction in BC is accompanied by the data's hash, which safeguards the data's integrity. All transactions are encrypted using methods of asymmetric encryption that assure confidentiality. The next section assesses the proposed architecture's resilience to various security attacks. Therefore, we focus on attacks that undermine the security of blockchain nodes and identify numerous attack scenarios that allow an attacker to take control of nodes or the network:

1. Man-in-the-middle attack: The communication data of any two communicating parties are symmetrically encrypted using the TLS session key, which removes the possibility of exposing sensitive information. Perfect Forward Secrecy prevents an attacker from deciphering future ciphertexts to obtain useful information, even if the data are compromised [46].
2. 51 % attack: According to the blockchain consensus technique, an attacker may only undermine the blockchain system's security if they control more than 51 % percent of the nodes or arithmetic power [47], which Schloss believed would lower the computing power or money and transfer it to the trusted nodes.
3. Replay attack: The use of random values and a counter for each session's nodes ensures that communication messages stay current between sessions, hence preventing replay attacks [46]. To make it more difficult for an attacker to launch an attack, we also award new identifiers to trustworthy nodes and update the authorized node in the blockchain for each epoch created by the change.
4. Sybil Attack: Schloss has a TMS that accomplishes the objective via the use of a trust-based mechanism. Schloss is used as a trust factor when routing choices are made and rogue nodes are detected. The choice is made entirely on the basis of node trust, and bad nodes are swiftly separated from the network.
5. Eclipse attack: To defend against Eclipse attacks, Schloss maintains trustworthy IP addresses, implements methods that monitor the blockchain for misbehaving nodes, and performs behavior analysis using the TMS on a per-epoch basis. The AM may reject device addresses that perform badly on the network. Additionally, nodes monitor and verify incoming and outgoing connections to mitigate the effect of Eclipse attacks. As a result, this is a viable strategy to prevent this attack.
6. Spam attack: Blockchain technology has the potential to guard against spam assaults [48]. All communication is handled as transactions, and each transaction is given a time stamp, indicating that it requires a consensus phase to take effect. As a result, an attacker cannot insert spam messages since they would be rejected by the consensus process.

5. Conclusions and Future Work

The Industrial Internet of Things and blockchain are two essential technologies to enable the development and continuation of Industry 4.0. We developed a blockchain-based system architecture for a group of manufacturers in order to solve the issue of secure cooperation. Our strategy aims to eliminate communication and trust obstacles between businesses that have partnered but do not trust one another in the absence of a third party. We utilized game theory methodologies to construct a system that creates a trustworthy environment depending on the trust value of individual devices. Specifically, the identification of devices is controlled dynamically via the use of a multi-signature smart contract, which allows for more flexibility in authenticating while still maintaining privacy. Additionally, the immutability of blockchain technology offers technical support for security audits and the construction of an accountability framework.

Furthermore, one of the next steps is the integration of smart sensors and sensor networks as well as data processing in our system architecture. However, the integration of smart sensors is a technical limitation, as such sensors currently do not have the necessary capabilities. Based on this, it can be assumed that such an interaction still requires some research and time.

Author Contributions: : Conceptualization, F.G.G., A.S. and D.W.; methodology, F.G.G., A.S. and D.W.; validation, F.G.G., A.S. and D.W.; formal analysis, F.G.G.; investigation, F.G.G.; writing—original draft preparation, F.G.G.; writing—review and editing, F.G.G., A.S. and D.W.; visualization, F.G.G.; supervision, A.S.; funding acquisition, A.S. All authors have read and agreed to the published version of the manuscript.

Funding: The authors would like to acknowledge the financial support from the German Federal Ministry of Research and Education (Bundesministerium für Bildung und Forschung, BMBF) and the

German Academic Exchange Service (Deutscher Akademischer Austauschdienst, DAAD). This paper was written as part of the Distributed IoT-Platforms for Safe Food Production in Education, Research and Industry (Dipper) project, which is co-financed by the BMBF (Förderkennzeichen: 01DG21017) and DAAD (Projekt-ID: 57557211).

Data Availability Statement: Not Applicable, the study does not report any data.

Acknowledgments: The article processing charge was funded by the Baden-Württemberg Ministry of Science, Research and Culture and the Offenburg University of Applied Sciences in the funding programme Open Access Publishing.

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

Appendix A

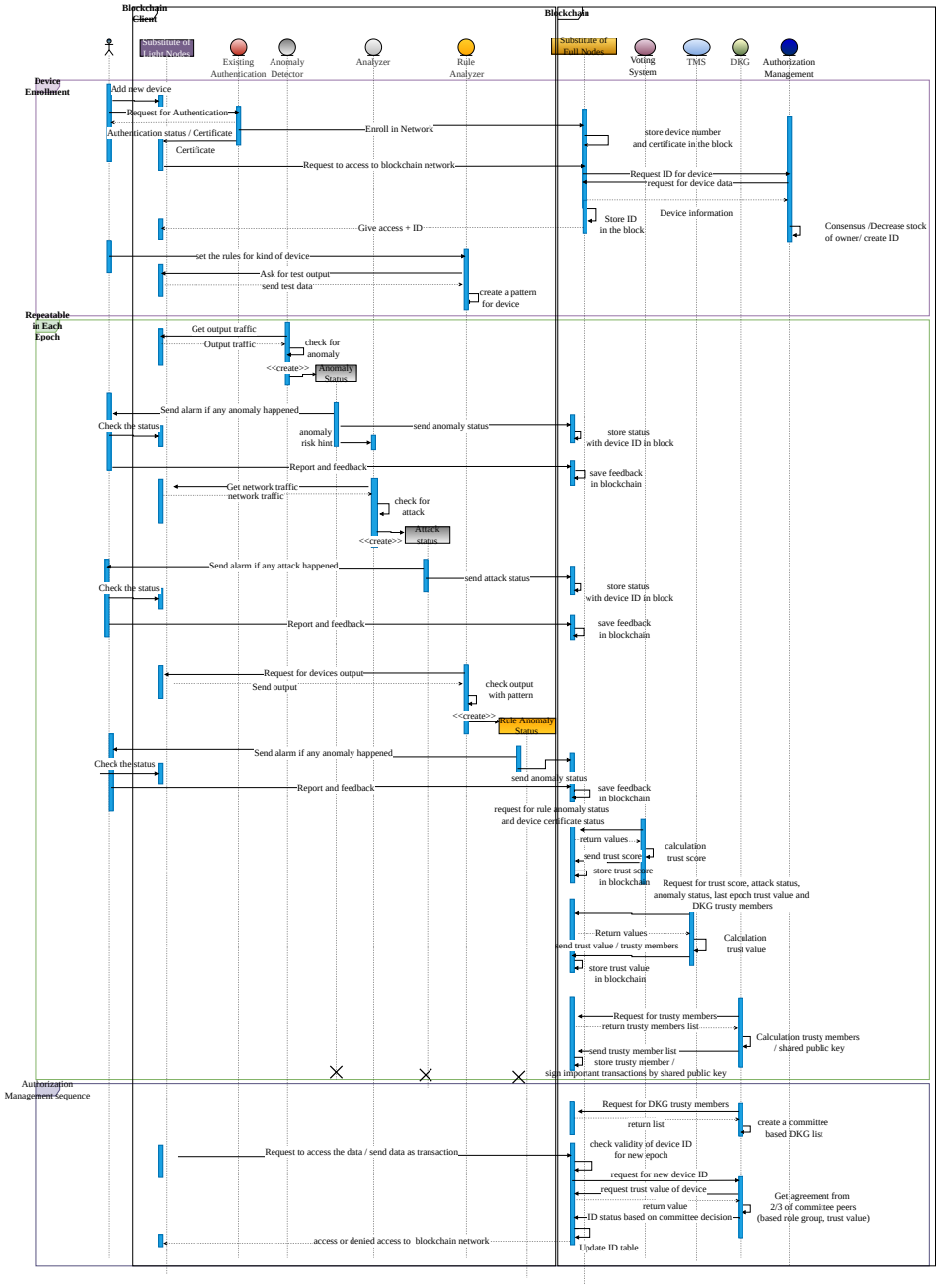

Figure A1. Sequence diagram of system.

References

1. Sikora, A.; Walz, A.; Zimmermann, L. Research aspects for secure communication in the industrial internet of things. In Proceedings of the 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kyiv, Ukraine, 14–18 May 2020; pp. 284–289.
2. Tsochev, G. Some Security Problems and Aspects of the Industrial Internet of Things. In Proceedings of the 2020 International Conference on Information Technologies (InfoTech), Varna, Bulgaria, 17–18 September 2020; pp. 1–5.
3. Stodt, J.; Schönle, D.; Reich, C.; Ghovanlooy Ghajar, F.; Welte, D.; Sikora, A. Security audit of a blockchain-based industrial application platform. *Algorithms* **2021**, *14*, 121. [CrossRef]
4. Lu, Y. Implementing blockchain in information systems: a review. *Enterp. Inf. Syst.* **2021**, 1–32.. [CrossRef]
5. Schönle, D.; Wallis, K.; Stodt, J.; Reich, C.; Welte, D.; Sikora, A. Industry Use Cases on Blockchain Technology. In *Industry Use Cases on Blockchain Technology Applications in IoT and the Financial Sector*; IGI Global: Hershey, PA, USA, 2021; pp. 248–276.
6. Tsang, Y.; Wu, C.; Ip, W.; Shiau, W.L. Exploring the intellectual cores of the blockchain–Internet of Things (BIoT). *J. Enterp. Inf. Manag.* **2021**, *34*, 1287–1317. [CrossRef]
7. Ghovanlooy Ghajar, F.; Salimi Sratakhti, J.; Sikora, A. SBTMS: Scalable Blockchain Trust Management System for VANET. *Appl. Sci.* **2021**, *11*, 11947. [CrossRef]
8. Gervais, A.; Karame, G.O.; Capkun, V.; Capkun, S. Is bitcoin a decentralized currency? *IEEE Secur. Priv.* **2014**, *12*, 54–60. [CrossRef]
9. Viriyasitavat, W.; Xu, L.D.; Sapsomboon, A.; Dhiman, G.; Hoonsopon, D. Building trust of Blockchain-based Internet-of-Thing services using public key infrastructure. *Enterp. Inf. Syst.* **2022**, 1–24. [CrossRef]
10. Sai, A.R.; Buckley, J.; Fitzgerald, B.; Le Gear, A. Taxonomy of centralization in public blockchain systems: A systematic literature review. *Inf. Process. Manag.* **2021**, *58*, 102584. [CrossRef]
11. Berdik, D.; Otoum, S.; Schmidt, N.; Porter, D.; Jararweh, Y. A survey on blockchain for information systems management and security. *Inf. Process. Manag.* **2021**, *58*, 102397. [CrossRef]
12. Dorri, A.; Kanhere, S.S.; Jurdak, R.; Gauravaram, P. Blockchain for IoT security and privacy: The case study of a smart home. In Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kona, HI, USA, 13–17 March 2017; pp. 618–623.
13. Panda, S.S.; Satapathy, U.; Mohanta, B.K.; Jena, D.; Gountia, D. A blockchain based decentralized authentication framework for resource constrained iot devices. In Proceedings of the 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kanpur, India, 6–8 July 2019; pp. 1–6.
14. Khalid, U.; Asim, M.; Baker, T.; Hung, P.C.; Tariq, M.A.; Rafferty, L. A decentralized lightweight blockchain-based authentication mechanism for IoT systems. *Clust. Comput.* **2020**, *3*, 1–21. [CrossRef]
15. Wu, L.; Du, X.; Wang, W.; Lin, B. An out-of-band authentication scheme for internet of things using blockchain technology. In Proceedings of the 2018 International Conference on Computing, Networking and Communications (ICNC), Maui, HI, USA, 5–8 March 2018; pp. 769–773.
16. Jia, X.; Hu, N.; Yin, S.; Zhao, Y.; Zhang, C.; Cheng, X. A2 Chain: A Blockchain-Based Decentralized Authentication Scheme for 5G-Enabled IoT. *Mob. Inf. Syst.* **2020**, *2020*, 12–40. [CrossRef]
17. Ferreira, C.M.S.; Garrocho, C.T.B.; Oliveira, R.A.R.; Silva, J.S.; Cavalcanti, C.F.M.d.C. IoT Registration and Authentication in Smart City Applications with Blockchain. *Sensors* **2021**, *21*, 1323. [CrossRef] [PubMed]
18. Ruta, M.; Scioscia, F.; Ieva, S.; Capurso, G.; Di Sciascio, E. Semantic blockchain to improve scalability in the internet of things. *Open J. Internet Things* **2017**, *3*, 46–61.
19. Hammi, M.T.; Bellot, P.; Serhrouchni, A. BCTrust: A decentralized authentication blockchain-based mechanism. In Proceedings of the 2018 IEEE Wireless Communications and Networking Conference (WCNC), Barcelona, Spain, 15–18 April 2018; pp. 1–6.
20. Yu, Y.; Zhao, Y.; Li, Y.; Du, X.; Wang, L.; Guizani, M. Blockchain-based anonymous authentication with selective revocation for smart industrial applications. *IEEE Trans. Ind. Inform.* **2019**, *16*, 3290–3300. [CrossRef]
21. Lupascu, C.; Lupascu, A.; Bica, I. DLT Based Authentication Framework for Industrial IoT Devices. *Sensors* **2020**, *20*, 2621. [CrossRef] [PubMed]
22. Kim, H.Y.; Xu, L.; Shi, W.; Suh, T. A Secure and Flexible FPGA-Based Blockchain System for the IIoT. *Computer* **2021**, *54*, 50–59. [CrossRef]
23. Abdolinezhad, S.; Zimmermann, L.; Sikora, A. A Novel Key Generation Method for Group-Based Physically Unclonable Function Designs. *Electronics* **2021**, *10*, 2597. [CrossRef]
24. Xu, L.; Chen, L.; Gao, Z.; Kim, H.; Suh, T.; Shi, W. FPGA based blockchain system for industrial IoT. In Proceedings of the 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Guangzhou, China, 29 December 2020–1 Janruary 2021; pp. 876–883.
25. Kumar, R.; Tripathi, R. DBTP2SF: A deep blockchain-based trustworthy privacy-preserving secured framework in industrial internet of things systems. *Trans. Emerg. Telecommun. Technol.* **2021**, *32*, e4222. [CrossRef]
26. Boudagdigue, C.; Benslimane, A.; Kobbane, A.; Liu, J. Trust management in industrial Internet of Things. *IEEE Trans. Inform. Forensics Secur.* **2020**, *15*, 3667–3682. [CrossRef]

27. Shoukry, Y.; Martin, P.; Yona, Y.; Diggavi, S.; Srivastava, M. Pycra: Physical challenge-response authentication for active sensors under spoofing attacks. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, Denver, CO, USA, 12–16 October 2015; pp. 1004–1015.
28. Varga, P.; Plosz, S.; Soos, G.; Hegedus, C. Security threats and issues in automation IoT. In Proceedings of the 2017 IEEE 13th International Workshop on Factory Communication Systems (WFCS), Trondheim, Norway, 31 May–2 June 2017; pp. 1–6.
29. Abdolinezhad, S.; Schappacher, M.; Sikora, A. Secure wireless architecture for communications in a parcel delivery system. In Proceedings of the 2020 IEEE 5th International Symposium on Smart and Wireless Systems within the Conferences on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS), Dortmund, Germany, 17–18 September 2020 pp. 1–6.
30. Singh, S.; Hosen, A.S.; Yoon, B. Blockchain security attacks, challenges, and solutions for the future distributed iot network. *IEEE Access* **2021**, *9*, 13938–13959. [CrossRef]
31. Bernstein, D.J.; Lange, T. Security Dangers of the NIST Curves. Invited Talk, International State of the Art Cryptography Workshop, Athens, Greece, 2013. Available online: http://www.hyperelliptic.org/tanja/vortraege/20130531.pdf (accessed on 19 April 2022)
32. Gottwald, S. Das Dual-EC-DRBG Desaster. Available online: http://www.math.uni-leipzig.de/MI/diem/math-krypto/DualEC_DRGB.pdf (accessed on 19 April 2022)
33. Anita, N.; Vijayalakshmi, M. Blockchain security attack: A brief survey. In Proceedings of the 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kanpur, India, 6–8 July 2019; pp. 1–6.
34. Hasanova, H.; Baek, U.J.; Shin, M.G.; Cho, K.; Kim, M.S. A survey on blockchain cybersecurity vulnerabilities and possible countermeasures. *Int. J. Netw. Manag.* **2019**, *29*, e2060. [CrossRef]
35. Otte, P.; de Vos, M.; Pouwelse, J. TrustChain: A Sybil-resistant scalable blockchain. *Future Gener. Comput. Syst.* **2020**, *107*, 770–780. [CrossRef]
36. Drias, Z.; Serhrouchni, A.; Vogel, O. Taxonomy of attacks on industrial control protocols. In Proceedings of the 2015 International Conference on Protocol Engineering (ICPE) and International Conference on New Technologies of Distributed Systems (NTDS), Paris, France, 22–24 July 2015 pp. 1–6.
37. Jin, X.; Haddad, W.M.; Yucelen, T. An adaptive control architecture for mitigating sensor and actuator attacks in cyber-physical systems. *IEEE Trans. Autom. Control.* **2017**, *62*, 6058–6064. [CrossRef]
38. Ruf, P.; Stodt, J.; Reich, C. Security Threats of a Blockchain-Based Platform for Industry Ecosystems in the Cloud. In Proceedings of the 2021 Fifth World Conference on Smart Trends in Systems Security and Sustainability (WorldS4), IEEE, London, UK, 29–30 July 2021; pp. 192–199.
39. Nguyen, D.C.; Ding, M.; Pathirana, P.N.; Seneviratne, A. Blockchain and AI-based solutions to combat coronavirus (COVID-19)-like epidemics: A survey. *IEEE Access* **2021**, *9*, 95730–95753. [CrossRef] [PubMed]
40. Dierksmeier, C.; Seele, P. Blockchain and business ethics. *Bus. Ethics Eur. Rev.* **2020**, *29*, 348–359. [CrossRef]
41. Leitner, S.H.; Mahnke, W. OPC UA–service-oriented architecture for industrial applications. *ABB Corp. Res. Cent.* **2006**, *48*, 22.
42. Prada-Delgado, M.A.; Dittmann, G.; Circiumaru, I.; Jelitto, J. A blockchain-based crypto-anchor platform for interoperable product authentication. In Proceedings of the 2021 IEEE International Symposium on Circuits and Systems (ISCAS), Daegu, Korea, 22–28 May 2021. pp. 1–5.
43. Holt, C.A.; Roth, A.E. The Nash equilibrium: A perspective. *Proc. Natl. Acad. Sci. USA* **2004**, *101*, 3999–4002. [CrossRef]
44. Schulze, M. The Schulze method of voting. *arXiv* **2018**, preprint. arXiv:1804.02973 .
45. Kate, A.; Goldberg, I. Distributed key generation for the internet. In Proceedings of the 2009 29th IEEE International Conference on Distributed Computing Systems, IEEE, Montreal, QC, Canada, 22–26 June 2009; pp. 119–128.
46. Esfahani, A.; Mantas, G.; Matischek, R.; Saghezchi, F.B.; Rodriguez, J.; Bicaku, A.; Maksuti, S.; Tauber, M.G.; Schmittner, C.; Bastos, J. A lightweight authentication mechanism for M2M communications in industrial IoT environment. *IEEE Internet Things J.* **2017**, *6*, 288–296. [CrossRef]
47. Yin, D.; Zhang, L.; Yang, K. A DDoS attack detection and mitigation with software-defined Internet of Things framework. *IEEE Access* **2018**, *6*, 24694–24705. [CrossRef]
48. Kshetri, N. Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommun. Policy* **2017**, *41*, 1027–1038. [CrossRef]