applied sciences

MDPI

Article

Secure Data of Industrial Internet of Things in a Cement Factory Based on a Blockchain Technology

Samir M. Umran [1,2], Songfeng Lu [1,3,*], Zaid Ameen Abduljabbar [1,4,5], Jianxin Zhu [1] and Junjun Wu [1]

[1] Hubei Engineering Research Center on Big Data Security, School of Cyber Science & Engineering, Huazhong University of Science and Technology, Wuhan 430074, China; samirhust@gmail.com (S.M.U.); zaid.ameen@uobasrah.edu.iq (Z.A.A.); zjx@mail.hust.edu.cn (J.Z.); wujunjun@hust.edu.cn (J.W.)
[2] Ministry of Industry and Minerals, Iraqi Cement State Company, Baghdad 10011, Iraq
[3] Shenzhen Huazhong University of Science and Technology Research Institute, Shenzhen 518063, China
[4] College of Education for Pure Sciences, University of Basrah, Basrah 61001, Iraq
[5] Technical Computer Engineering Department, Al-Kunooze University College, Basrah 61001, Iraq
* Correspondence: lusongfeng@hust.edu.cn; Tel./Fax: +86-27-8754-0560

Abstract: The Industrial Internet of Things (IIoT) has become a pivotal field of development that can increase the efficiency of real-time collection, recording, analysis, and control of the entire activities of various machines, and can actively enhance quality and reduce costs. The traditional IIoT depends on centralized architectures that are vulnerable to several kinds of cyber-attacks, such as bottlenecks and single points of failure. Blockchain technology has emerged to change these architectures to a decentralized form. In modern industrial settings, blockchain technology is utilized for its ability to provide high levels of security, low computational complexity, P2P communication, transparent logs, and decentralization. The present work proposes the use of a private blockchain mechanism for an industrial application in a cement factory, which offers low power consumption, scalability, and a lightweight security scheme; and which can play an efficient role in controlling access to valuable data generated by sensors and actuators. A low-power ARM Cortex-M processor is utilized due to its efficiency in terms of processing cryptographic algorithms, and this plays an important part in improving the computational execution of the proposed architecture. In addition, instead of proof of work (PoW), our blockchain network uses proof of authentication (PoAh) as a consensus mechanism to ensure secure authentication, scalability, speed, and energy efficiency. Our experimental results show that the proposed framework achieves high levels of security, scalability and ideal performance for smart industrial environments. Moreover, we successfully realized the integration of blockchain technology with the industrial internet of things devices, which provides the blockchain technology features and efficient resistance to common cyber-security attacks.

Keywords: blockchain technology; industrial IoTs; IoT applications in Industry 4.0; decentralization applications; machine to machine communication; distributed databases

check for updates

Citation: Umran, S.M.; Lu, S.; Abduljabbar, Z.A.; Zhu, J.; Wu, J. Secure Data of Industrial Internet of Things in a Cement Factory Based on a Blockchain Technology. *Appl. Sci.* **2021**, *11*, 6376. https://doi.org/10.3390/app11146376

Academic Editor: Gianluca Lax

Received: 18 May 2021
Accepted: 6 July 2021
Published: 9 July 2021

1. Introduction

Recent revolutions in the industrial sector have come from innovative technological concepts such as big data, cloud computing, artificial intelligence, and cyber-physical systems. Merging the smart industry with Internet of Things (IoT) technology has given rise to new and diverse requirements to ensure a secure industrial environment [1]. With these technologies, the industrial process has evolved in new directions related to the provision of facilities, reducing production costs, and increasing production rates. The Fourth Industrial Revolution will be achieved by linking conventional industrial environments to internet networks [2,3].

Traditional IoT depends on the use of a centralized architecture, with information processing and analysis facilities provided by cloud-based servers. Each expansion in the use of IIoT networks is accompanied by renewed security and privacy challenges.

The main drawback of a centralized architecture is that it represents a bottleneck, latency, and a single point of failure, meaning that hacking can lead to the whole network going down [4]. The use of a centralized architecture therefore becomes unsuitable, especially for high-performance applications [5]. In the new IIoT, the amounts of sensor data are huge, and this would lead to a significant increase in the load on centralized verification systems. However, in the IIoT, challenges related to security and scalability can be overcome through the integration of blockchain technology with IoT devices [6].

The blockchain is an important technology that can provide a high level of secrecy, privacy and protection for control systems in real-time [7,8]. It is a distributed, decentralized, timestamp, and shared database ledger. That has ability to store the identity of registered nodes and all transactions between peers, cryptographic techniques and a hash algorithm are used to secure the transactions and authenticate the peers without the need for trusted third party services, blockchain uses hashing function (SHA-256) and elliptic curve cryptography (ECC) to provide robust cryptographic proof for data integrity and authenticity. Therefore, blockchain technology has unique advantages over other conventional technologies [6]. In addition, the most common problems associated with a centralized architecture can be solved through the use of a decentralized system. Blockchain technology can also help to improve the performance of IIoT platforms in various areas of application [9].

Blockchain features, such as distributed ledger, distributed database, distributed consensus mechanism, transparent log, timestamp, and traceability provide a trusted system that can efficiently resist many types of cybersecurity attacks [10]. By merging the blockchain technology and exploiting its features in a new environment (founded on industrial IoTs), we ensure the system's security and data integrity during the autonomous transfer of data between machines (M2M) in an industrial environment. This merging helps increase the possibility of a robotic control system with the remote observation of machine events, to make the right decisions in time. With our proposed architecture (depicted in Figure 1), we integrated the technology of blockchain, smart contract and IoTs in a cement factory as an industrial environment. Our proposed architecture consists of three layers: Physical, Blockchain Service and Application. These layers work together to build a lightweight security scheme by utilizing STM32 boards and a low-power STM32F427 processor. Moreover, adopting a fast, highly scalable, low energy proof of authentication (PoAh) as a consensus mechanism helps to enhance the computational performance [10,11].

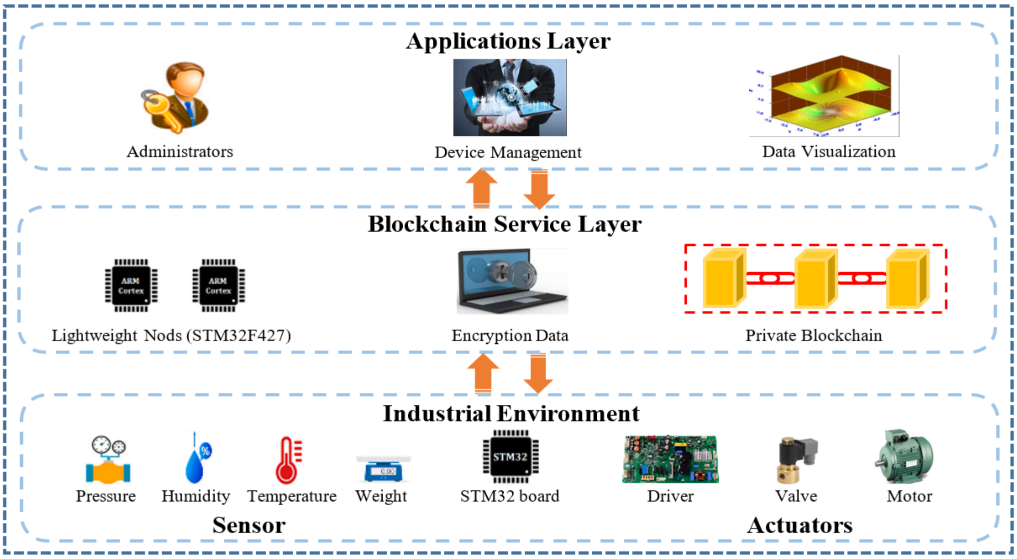

Figure 1. Blockchain architecture for IIoT.

Motivation and Contributions

The process of integrating the blockchain with IIoT systems is challenging due to the particular requirements involved. These challenges include the resource-constrained and low-power nature of IoT devices, the sensitivity of the information, low storage capacities, and the high numbers of devices contained inside large IIoT networks. To overcome these challenges, we proposed a trusted, highly scalable, low-power, transparent, and lightweight security scheme based on a private blockchain mechanism for a cement factory. Our architecture consists of three layers: a physical layer, a blockchain service layer, and an application layer. In the first of these layers, we utilized an STM32 development board to transmit data from sensors and actuators to the blockchain service layer, which contains private blockchain (permission) and lightweight nodes that are designed to give a faster performance for an asymmetric cryptographic algorithm (ECC). Proof of authentication (PoAh) is used for new blocks authentication in our architecture, as this eliminates the need for the reverse hash function used in proof of work (PoW) and makes the process lighter in weight [10,12].

The main contributions of the proposed architecture are as follows:

- It provides a security scheme that can guarantee the security of data transmission between peers in a Cement industry environment.
- It is based on integration between a blockchain technology and IoTs to provide a lightweight, trusted, low-power, scalable, transparent, and decentralized IIoT network. It is also resistant to common IoT attacks such as Sybil, modification, impersonation, replay, repudiation, man in middle (MIM), denial of service (DoS), and distributed (DoS) attacks.
- It offers low computational complexity and high performance due to the adoption of a blockchain service layer that contains lightweight nodes.
- It successfully eliminates the need for a third party service (a trusted authority) through the use of PoAh and smart contracts that are executed autonomously.

2. Related Works

The IIoT was developed to improve industrial processes and can provide real-time information collection, processing, storage, and event management [8,13]. Traditional IIoT mechanisms still suffer from several security threats such as Sybil, modification, impersonation, replay, MIM, repudiation, DoS, and distributed DoS attacks [14,15]. All of these threats can be prevented through the use of blockchain technology, which can play a pivotal role in ensuring secure communication between each type of activity and building trust among communicating nodes [16].

The IIoT is revolutionizing industry from many perspectives, such as manufacturing, supply, and retailing. In this section, we review several recent studies that are closely related to blockchain applications in the industrial sector. The first blockchain-based digital currency system is Bitcoin, which was introduced by Nakamoto in 2008 [17]. There are many similarities between the IIoT and Bitcoin systems, such as huge numbers of nodes, rigorous security and privacy requirements, and the continuous exchange of data. Blockchain technology is therefore acknowledged as the most suitable choice for industrial applications. Shen et al. [18] proposed a consortium blockchain to build trust between connected devices in various domains. For the authentication process, the author utilizes the identity-based signature (IBS), while Ephermeral Elliptic Curve Diffe-Hellman (EECDH) used for the key agreement process. Then, the authors design a new mechanism for identity management to preserve the privacy of participants devices, through it the authenticated devices remain anonymous. Rathee et al. [14] explored the provision of security in the industrial sector for offices distributed over several countries and proposed a hybrid Blockchain mechanism. Cao et al. [19] overcame the challenges associated with information traceability in a steel factory by presenting a blockchain-based quality traceability system. In this scheme, clients could gain access to process information and trace the quality of a product in a secure manner. Hu et al. [20] developed a distributed P2P energy transaction model in which smart contracts were used to ensure the transparency and tamper-resistance of credit scores. He et al. [21] presented a software status monitoring system based on the blockchain and IIoT, in which the blockchain was used for storage purposes. In their work, Gul et al. [22] focused on both a business and its customers, and proposed a smart healthcare business model for the prediction of patient status by collecting suitable data from the Internet of Medical Things.

In any communication system, the overall security of the system poses a significant challenge, and this is especially true for the IIoT sector [23]. However, blockchain technology can overcome a wide range of cybersecurity threats.

All of the research studies reviewed here are limited in that they use blockchain technology only for its efficiency in recording sensor data in industrial environments, and do not explore its applicability to other industrial operations; there is a lack of discussion in the literature of schemes for applications at the device level. Furthermore, most studies have relied on the use of open-source platforms and PoW as a consensus mechanism to provide blockchain services, which is exposed to 51% security attacks and required a high cost of energy and hardware [10,11,24–27].

To overcome the aforementioned challenges, we propose a trusted, scalable, low power, lightweight, and efficient security scheme based on a decentralized private blockchain architecture for a cement factory. By adopting a decentralized architecture, we address the problems of a single point of failure, latency, and bottlenecks, and eliminate the need for a relationship with a third party, which typically leads to an increase in the execution time needed for authentication and other services and poses a potential security threat to the whole system. In addition, we exploit the features of the blockchain to secure data at the device level. Using the proposed lightweight nodes (STM32F427), we achieve real-time encryption and data collection, processing, and storage in a blockchain network, and through the use of a private blockchain/smart contract, our architecture provides resistance to many common IoT attacks such as anonymity [28], tampering, impersonation, replay, repudiation, MIM, Sybil, 51%, Double spending, and DoS attacks [14,15]. The elliptic curve digital signature algorithm (ECDSA) is adopted due to its low complexity and low storage requirements [29].

In comparison to existing schemes, our experimental results show that we have created an efficient, secure architecture for the cement industry that satisfies the resource constraints by achieving the lowest execution time with the lowest energy consumption by utilizing ECDSA on an ARM Cortex-M4, as discussed in Section 5. Instead of PoW, we use a PoAh consensus mechanism to generate a highly scalable, fast, and energy-efficient scheme [30,31].

In our scheme, we successfully realized the integration of blockchain technology with IoT devices in the industrial sector at the device level, which is considered to be a challenging point in many research papers. The IoT devices classified as resource constraints (sensors, actuators) that founded new requirements, such as lightweight security scheme, lightweight algorithms, and low power consumption [20]. Our architecture satisfies these new requirements by building a lightweight security scheme, designed by utilizing a low-power ARM Cortex-M4 processor. Moreover, it adopts fast, highly scalable, low energy proof of authentication (PoAh) as a consensus mechanism that helps to enhance computational performance. In addition, our architecture brings many benefits and features to the internet of things network in an industrial sector, concerning increased overall system security, stability, offer information traceability, scalability, secure remote access to valuable data, transparency, and tamper-resistance (by using smart contract), and provides a real-time status monitoring system. The data collected from IoT sensors and actuators that could not be changed by any network participants (immutable) after recording them in a blockchain network, can also be used to predict future production capacity, maintenance, and many other factors, with excellent data management. In addition, this integration enables fast reactions to the newly received data, which helps enhance the quality and reduce the wastage of raw materials.

3. Architecture for a Cement Factory Based on Blockchain Technology

Merging blockchain technology into an IIoT system can improve the security of the whole system. In particular, the security and privacy characteristics of blockchain technology are important when using an IoT in smart industry. Figure 1 shows the proposed architecture for a cement plant in an internet-connected industrial environment.

3.1. Physical Layer

The proposed architecture applies numerous sensors and actuators and a microcomputer in the setting of a cement plant. We use five types of sensor to record the kiln temperature, the kiln rotation speed, the moisture of the mixture, the inlet-outlet pressure, and the weight. These sensors are interfaced with ultra-low-power STM32 Microcontroller, which pre-processes the collected data before transmitting them to the blockchain service layer. Several motors, actuators (variable frequency drive (VFD) gear-motors), and solenoid valves are used in this architecture.

3.2. Blockchain Service Layer

The blockchain service layer split into two subsections: a set of lightweight nodes and a private blockchain. This layer also contains the suitable modules, which work to organize the common services needed to provide features of blockchain technology. ECC [29] adopted in order to give a high-speed implementation. We designed the lightweight nodes using an STM32F427 that based on ARM Cortex-M4, which has been shown to be effective and efficient for IIoT applications and is an appropriate choice, especially for cryptographic algorithms [32]. The device authentication mechanism used public and private keys generated by ECDSA, which is an algorithm that is characterized by low complexity, very fast execution and requirements low storage capacity [29]. The use of ECDSA for industrial applications has been approved and certified by the NIST Cryptographic Algorithm Validation Program [32].

In our Blockchain service layer, we designed several lightweight nodes instead of a single node, which helps the registered users, devices or machines to efficiently access the blockchain network, reducing the pressure and preventing system failure from occurring, compared with a single node strategy, which can lead to problems of instability and overall system failure [9]. Our architecture also achieved the system stability and availability of services that make it an efficient solution for integrating blockchain technology with industrial IoTs, which require continuous data processing in real-time.

3.2.1. Private Blockchain

There are three types of blockchain: public, private, and consortium. For industrial applications, we found the most suitable choice is a private blockchain, as this can provide a high level of security [15]. The connections between blocks enable P2P communication, where data transmitted directly between peers. The block architecture of our proposed scheme is illustrated in Figure 2, only authorized nodes can access the private network to read or add new ledger entries through the use of smart contracts that are executed autonomously, without the need for a trusted third party that considered to be as disadvantage point of centralized architecture which adopted in other works. Due to the irreversible nature of smart contracts, it is almost impossible for an unauthorized node to make changes to the blockchain ledger [33]. Different from other works, in our architecture, the blockchain network receives the data from lightweight nodes as encrypted data; this efficiently helps increase the security of the valuable data with overall system security by adding another stage of encryption. This efficiently increases the difficulty of disclosing encrypted data, even if any unauthorized user can access the blockchain network. In addition, all blockchain ledgers used the hashing function mechanism, asymmetric encryption, and digital signature, already adopted inside the blockchain network to verify incoming new blocks.

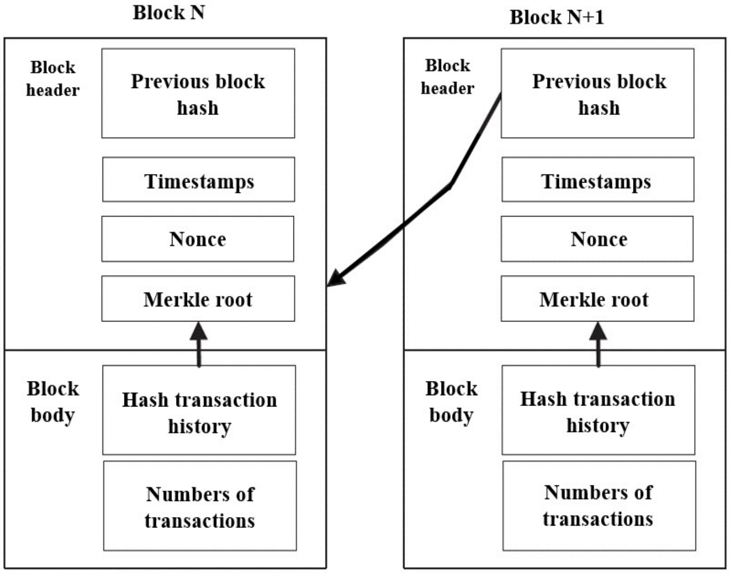

Figure 2. Block structure.

3.2.2. Consensus Algorithm

Blockchain networks never require an external third party, and each new transaction validated using a consensus mechanism. The main purpose of the consensus algorithm is to ensure there are no collisions between transactions. The use of the PoAh consensus algorithm helps the blockchain to be lightweight and suitable for resource-constrained devices, and can eliminate centralized dependencies [12,30]. A wide range of different consensus algorithms has been used in blockchain applications, including PoW, proof of space (PoSpace), a measure of trust (MoT), and proof of stake (PoS).

Although most classical blockchain networks use PoW as a consensus algorithm, this is not suitable for resource-constrained devices. The processes used in PoW are expensive for IoT and edge computing applications, which adopted with public blockchain [11]; in PoAh, the reverse hash function process used in PoW is eliminated, making the transaction process lightweight [10,12].

First, the participant nodes generate a transaction proposal to create a new block and then the nodes sign the new transaction with a private key and directly broadcast it to the blockchain network. After receiving the proposed block in the network, trusted nodes verify the signature with a public source key; the trusted nodes evaluate the MAC address and compare it with the received one. After completing the authentication step, the authenticated block is broadcast to the network with PoAh identification. The user adds a new block to the chain after computing the hash value to link the next block and then retrieves the previous block hash to save it to the current block. Otherwise, the nodes drop the unauthenticated block.

In our scheme, we used the PoAh consensus mechanism to update the blockchain and to validate each new block, PoAh uses cryptographic authentication to authenticate new blocks that make it faster than other traditional consensus algorithms. The approach means that the blockchain can be efficient integrated with IIoT devices. Algorithm 1 shows the steps of the PoAh consensus algorithm [12].

Algorithm 1. PoAh Execution Process.

```
Input: All participant nods in the BC network follow ECDSA
Output: Add authenticated Block to the Blockchain network
start:
    Nodes integrate transactions to form of blocks
    Nodes sign blocks with own private key
    Nodes broadcast signed blocks to the network
    Trusted nodes verifies signature with source public key
    Trusted nodes evaluate MAC address
        if (Block authentication == true)
            Valid Block | | PoAh, broadcast to network
            User add new blocks into chain
        else
            Drop the unauthenticated block
 end: Go to step 1 for next process
```

3.3. Application Layer

The top layer of our proposed architecture is the application layer, which provides a mechanism for efficient interaction between users and devices, and allows users to control the devices by visualizing data. Other services provided by this layer include administration, user management, and visualization of data from the physical devices, as shown in Figure 1.

Remark 1. *The integration of blockchain technology with IoTs in the industrial sector ensures system security and data integrity. In the physical layer of our proposed architecture, we utilized ultra-low-power STM32 boards. While, in the blockchain service layer, the lightweight nodes consists of four STM32F427 (based on ARM Cortex-M4) were designed to provide high performance of asymmetric cryptography algorithms (ECDSA) by improving computational performance. PoAh was utilized as a consensus mechanism that provides a prospective security solution for IoT structure and an adequate level of robustness when used with ECDSA. In addition, it is an ideal selection for resource-constraint devices. The application layer provides administration services, device management, and data visualization, which provides data access control and management.*

4. Process Flow of the Proposed Architecture

Our architecture is designed to provide a secure, energy-efficient, scalable, and trusted data sharing environment for cement manufacture, based on secure P2P data transmission between users, sensors, actuators and machines. All network participants must be registered in advance with the blockchain network, as described below.

4.1. User Registration

To register a new user with the blockchain network, the first step is for the administrator to generate a new and unique identification number (ID), and to send this as a transaction of registration to the members of the blockchain. Using a smart contract, the blockchain nodes check whether the new ID already exists in the blockchain network. If not, then the smart contract allows the new transaction. After the PoAh algorithm executed, the registration of the new user ID in blockchain network is completed and shared with all nodes. The blockchain then generates a certificate for the new user based on its private key and sends it to the administrator. Otherwise, the transaction denied, a notification is generated for the administrator and an error is returned. Algorithm 2 describes the process of user registration in more detail.

Algorithm 2. User Registration.

```
1   start:
2     Generate a unique users ID from admin
3     User ID: HUST37
4     Admin share new generated IDs to blockchain members
5       if (User ID not exist = = true)
6         Execute PoAh algorithm
7         Register new user ID in blockchain
8         Return user ID certificate
9       else
10        Deny transaction
11        Notify admin
12        Return error ( )
13   end: Go to step 1 for next process
```

4.2. Device Registration

The physical layer contains many sensors and actuators, and all of these devices must be pre-registered with the private blockchain network. These devices are responsible for providing data that processed by the STM32 Microcontroller to the lightweight nodes, which process the registration request to the blockchain nodes as a suggested new transaction. The IoT devices are responsible for generating a unique device ID, the ID verification process based on a smart contract, if the device ID does not exist, then the PoAh algorithm is executed and the registration of the new device ID in the blockchain network is completed, then new certificate shared with all blockchain nodes. Otherwise, the transaction denied and a notification is generated for the administrator with an error message is returned. Algorithm 3 summarizes the device registration process in the blockchain network.

Algorithm 3. Device Registration.

```
1   start:
2     IoTs generate a new device unique ID
3     Device ID: Temperature-Inlet
4     Microcontroller STM32 sends the information to light nodes
5     Lightweight nodes process the registration request
6       if (Device ID not exist = = true)
7         Execute PoAh algorithm
8         Register new devise ID in blockchain network
8         Notify nodes by share new device ID certificate
9       else
10        Deny transaction
11        Notify nods
12        Return error ( )
13   end: Go to step 1 for next process
```

4.3. Data Storage

Data storage starts after completion of the registration step for all of the sensors and actuators that the participants in the blockchain have networked successfully. The next step represents the process of storing data provided from these sensors and actuators to the blockchain network through lightweight nodes, as depicted in Figure 3. The process starts when new data from the sensors is fed to the STM32 board. The STM32 is responsible for preparing the received data (pre-possess) and sending it to the lightweight nodes in the blockchain service layer. The lightweight nodes (ARM Cortex-M4) check the registration ID of the device to verify it or deny the proposed transaction. If it is true, then it executes the ECDSA directly and generates the public and private key after encrypting the received data. The proposed transaction is sent to the blockchain network for storage purposes, after checking the PoAh, and a copy of all transactions is sent to the lightweight nodes to provide a backup of these transactions, that can be used in case of a single node crash. The smart contract and lightweight node interact with each other to execute the transaction. The smart contract responsible allows the transaction to store the encrypted data inside the blockchain network. Algorithm 4 summarizes the data collection and storage process.

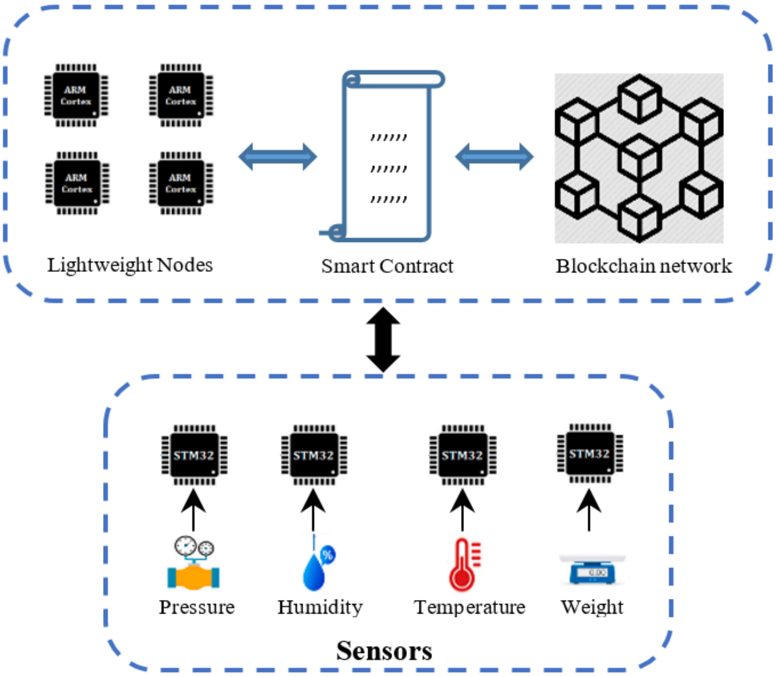

Figure 3. Collecting and storage process of sensor data.

Algorithm 4. Sensors Data Storage.

```
start:
  STM32 start pre-process sensors data
  STM32 send the processed information to lightweight nods
  ARM Cortex-M4 verifies the device through its registration ID
    if (Device authentication = = true)
      Execute ECDSA
      Generate public and private keys
      Submit proposed transaction to blockchain for data storage
      if (PoAh = = true)
        Store encryption data inside the blockchain network
      else
        Return error ( )
    else
       Deny transaction
       Return error ( )
 end: Go to step 1 for next process
```

5. A Blockchain-Based Cement Factory

Our blockchain-based architecture for cement plant is illustrated in Figure 4, from the start to the end of the process, a clinker product represented by a raw material passes through a specially designed rotary kiln, a cooler and iron conveyors. A VFD gear-motor controls the rotation of the kiln.

In cement processes, the temperature of the rotary kiln, the pressure of the inlet air actuator, the rotation speed of the kiln and the moisture of the mixture are highly important factors that are directly related to the quantity and quality of clinker production.

To control these critical factors effectively, four high-accuracy temperature sensors (kiln inlet, outlet, mixture, clinker) are used with an STM32 board. During the burning process of the raw material, the temperature sensors, rotation sensor, and pressure sensors are interfaced with the STM32 board to provide control over the state of the burner valve, the inlet air actuator, the raw material feed and the rotation speed. In the second stage, burning raw material at a high temperature (1450 °C) passed through the rotary kiln to produce the clinker. In this case, all of the sensors and actuators are used to ensure ideal burning conditions inside the rotary kiln, while the moisture sensor is used to check and control the moisture of the mixture before feeds to the kiln. Weight sensors are used with the STM32 board to record the weight of the product (clinker) in tons per hour. In the final stage (after cooling), iron chains are used to convey the product to the clinker store. Our architecture consists of several modules, all of which interact with the lightweight nodes (four STM32F427) of the blockchain service layer. Each of these modules has a copy of the recorded data, meaning that if a node crashes for any reason, then another node can provide a backup of the required data. Through this interaction, lightweight nodes can efficiently record the data and the states of actuators provided by the sensors. Real-time encryption is provided through the use of the ECC algorithm; this is applied by lightweight nodes to the acquired data, which are then sent to the private blockchain. The ECDSA was chosen for our architecture due to its low storage requirements and low complexity, which make it suitable for resource-constrained devices [34]. It also used to create public and private keys and to provide an authentication mechanism for devices. Encrypted data are stored in a secure, private blockchain network, and only the administrator and authorized users can connect to and access services. Blockchain is a promising technology for use in a factory, as it can ensure the security required in a smart industrial environment.

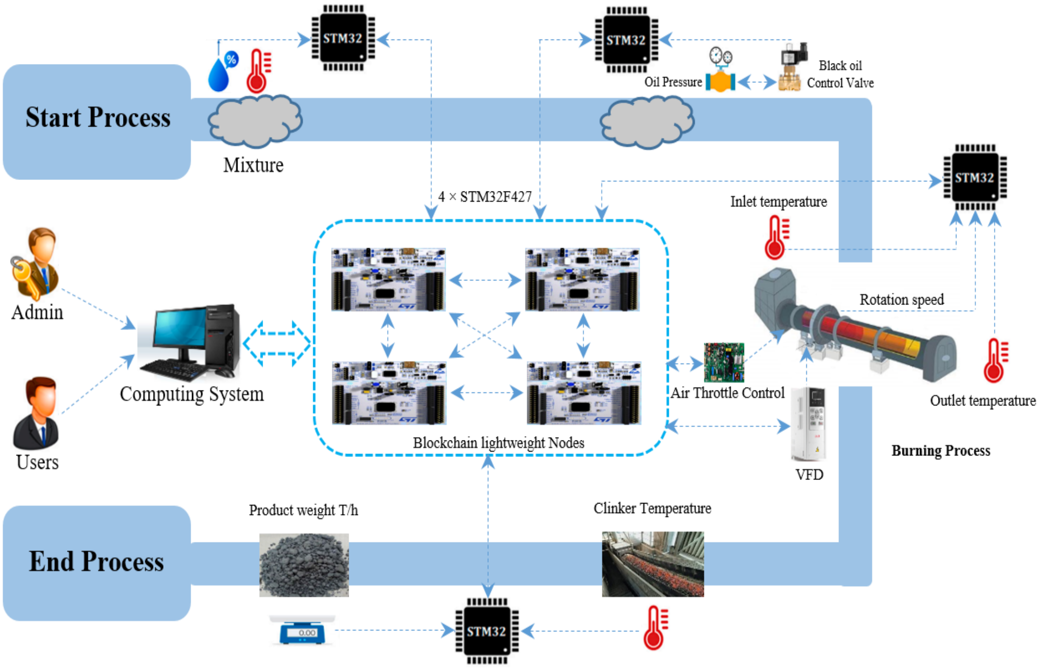

Figure 4. A blockchain-based cement production plant.

6. Performance Analysis

We evaluated our proposed architecture in terms of the cryptography and consensus algorithms used.

6.1. Performance of the ARM Cortex-M for Asymmetric Cryptography

Our implementation was applied at the device level for cryptographic algorithm to the blockchain network. An evaluation was carried out using four series of ARM Cortex-M that are characterized by their low cost, energy efficiency and high performance, making them the ideal option for real-time processing applications [32]. The series of processors used here were M0, M3, M4, and M7. We computed the execution time and power consumption for each series based on the mean $\bar{X}$, standard error $\delta\bar{X}$, and standard deviation δX, as shown in Tables 1 and 2. The X-CUBE CRYPTOLIB library was used to implement ECDSA, which helped to meet the requirements of the application in terms of gathering data, integrity, confidentiality, non-repudiation and authentication.

Table 1. ECDSA execution time.

M-Series	$\bar{X}$ (s)	δX (s)	$\delta\bar{X}$(s)
M0	13.8124	0.002	0.0001
M3	21.0815	0.004	0.0013
M4	1.1236	0.000	0.0000
M7	0.9256	0.000	0.0000

Table 2. Elliptic Curve Digital Signature Algorithm (ECDSA) power consumption.

M-Series	$\bar{X}$ (mW)	δX (mW)	$\delta\bar{X}$(mW)
M0	134.582	25.540	8.095
M3	224.813	12.335	3.901
M4	209.915	14.170	4.480
M7	298.651	14.500	3.905

6.1.1. Execution Time

Execution time represents the actual time consumed in encryption, decryption and key generation with ECDSA, which implemented using a HP pavilion laptop with a Core(TM) i7-7700HQ CPU @ 2.80 GHz, 16 GB RAM, 64-bit. We recorded 10 execution times for ECDSA for each of the processors (M0, M3, M4, and M7) and computed the mean value for each. The lowest execution times were obtained for the M4 and M7 processors, while the highest was obtained for M0 and M3 as shown in Table 1, from Figure 5 we can easily see that the optimal choices for executing the ECDSA were the M4 and M7 processors, due to their high performance. We selected the M4 processor for our architecture in order to strike a balance between the two factors of execution time and power consumption.

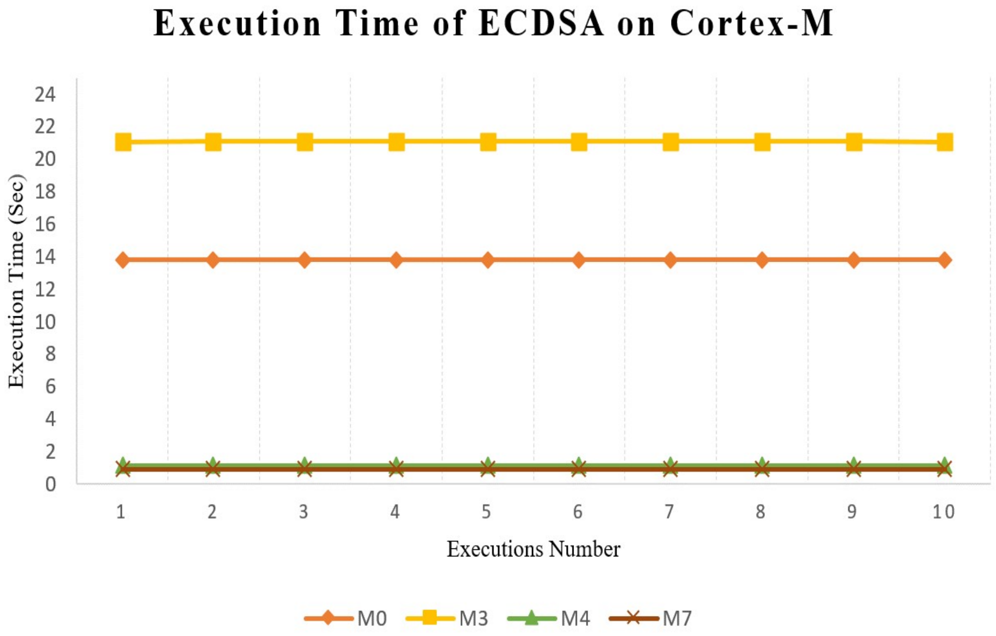

Figure 5. Execution time for each M-series.

6.1.2. Power Consumption

Power consumption was considered a very important factor, especially for the resource-constrained devices used in IoT or certain IIoTs. The power consumed by the ARM Cortex-M in the execution of the cryptographic algorithm was calculated using Ohms Law, as shown in Equations (1) and (2):

$$I = \frac{v}{R} \tag{1}$$

where I represents the microprocessor current, V represents the voltage supplied to the microprocessor, R represents the resistance (1.0 Ω), and V represents the supply voltage (5.0 V):

$$P = V \times I \tag{2}$$

We calculated the average power consumption for the microprocessor by running ECDSA 10 times. The results presented in Figure 6 and Table 2 show that all of the processors (M0, M3, M4 and M7) had low values of power consumption; they were therefore energy-efficient in terms of implementing ECDSA and could satisfy the requirements for resource-constrained devices.

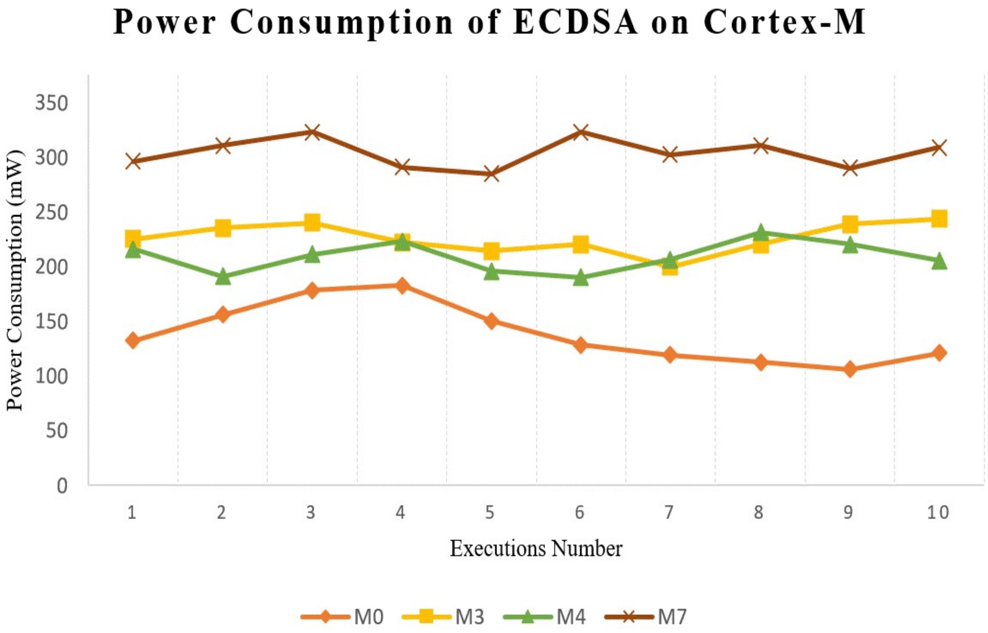

Figure 6. Consumption for each processor.

6.2. PoAh Consensus Algorithm

We analyzed the PoAh algorithm from several different perspectives. In terms of providing security, PoAh provides a prospective security solution for IoT structure. For decentralized IIoT networks, PoAh provides an adequate level of robustness when used with ECDSA, and addresses the main drawbacks of existing blockchain consensus algorithms, such as instabilities in network connectivity and the 51% attack [10,11,22,24]. In the PoAh algorithm, all participating nodes are qualified to generate new blocks for the blockchain network, but only trusted nodes can authenticate or add new blocks to the chain. Furthermore, 51% attacks that pose a threat in PoW, are mitigated through the dynamic nature of trust values [9,11].

From the perspective of execution time, PoAh is a lightweight consensus algorithm that much more effective than other traditional consensus. In addition, the major impact of PoAh is the low latency and energy consumption that designed especially for IoTs applications. From the point of view of resource utilization, PoAh is an ideal selection for resource-constrained devices in IoTs private networks as it consumes minimal energy [10–12,26,30].

7. Comparative Performance Analysis

Most the recent studies have focused on the features of the blockchain in the field of data storage, and have not dealt with the other features of blockchain technology regard to an industrial environment. They have also not provided a clear method for protecting the sensor data on the devices [14,19–22]. In view of this, we propose a trusted, lightweight, low power, high-performance and secure communication network for a cement plant as an industrial environment. Our approach ensures the protection of the data transferred between peers, even outside the blockchain network, through the integration of the blockchain with IIoT. Since the blockchain operates based on asymmetric key cryptography, we can achieve security of information, protection of user identities, and guaranteed transactions.

Our architecture successfully achieves trust for all network operations and components, meaning that security and transparency can be ensured at all levels of the cement industry. Table 3 shows a comparison of various methods in the literature in terms of the consensus mechanism used, the blockchain platform, the cryptographic scheme, hardware dependency, energy efficiency, and speed.

Table 3. Performance comparison of our study with state-of-the-art.

Author	Consensus Mechanism	Blockchain Platform	Cryptography Scheme	Hardware Dependency	Energy Efficiency	Consuming Time	Security Attack
Rathee et al. [14]	PoW	Consortium Blockchain	SHA-256	Yes	No	High	51%, and Sybil
Shen et al. [18]	IBS	Consortium Blockchain	ECDHE	Yes	Fair	High	Sybil and DoS
Cao et al. [19]	PoC	Hyperledger	SHA-256	Yes	Fair	High	51% and Sybil
Hu et al. [20]	PoW	Ethereum Blockchain	SHA-256	Yes	No	High	51% and Sybil
He et al. [21]	PBFT	Hyperledger Fabric v0.6	Local Public-Key	No	Fair	High	Sybil and DDoS
Gul et al. [22]	Delegate PoS	Public Blockchain	Local Public-Key	No	Fair	Midding	51% and Sybil
Our study	PoAh	Private Blockchain	ECDSA	Yes	Yes	Low	No

The first criterion in our comparison is the consensus mechanism through which new transactions are authenticated and added to the blockchain network. Due to the use of resource-constrained devices in IoTs and the associated scalability issues, the consensus mechanism must be lightweight. The authors of [18] used identity-based signature (IBS), and the authors of [14,20] used PoW in their work, while the authors of [19] used PoC. In [21] PBFT used in their scheme, while in [22] delegate PoS adopted as shown in Table 3, most of these traditional consensus mechanisms are not compatible with resource-constrained devices. For example, the PoW algorithm has higher energy requirements than PoS, PoC and PoA, although none of these approaches is suitable for low-power computational devices. In our scheme, we used PoAh as a consensus algorithm, which has the lowest energy consumption for block authentication. PoAh is based on a cryptographic authentication scheme that makes it faster than other consensus algorithms, which designed to reduce the latency and energy consumption for each transaction. In addition, its specialized to resource-constraint IoTs nodes [10–12,26,30].

The second criterion, the use of an open-source platform, is used in most schemes, which can provide an appropriate quality of service, however, an open-source platform fully depends on a third party (central authority). In general, external dependency can lead to many kinds of security and computational issues, such as single point of failure, bottleneck problems, and slow execution for the whole of the network activities due to an increase in the mutual authentication messages between the internal network and the trusted authority; this dramatically increases the network's component power consumption. Our scheme is designed to work based on a private blockchain network; participants must be pre-registered in the network to be an authorized user or device. This makes it more feasible for use in industrial applications and eliminates the need for third-party services, with its related problems.

The third criterion is the cryptography used to ensure transactions and user identities, and to secure the data. There are several cryptographic schemes that have been adopted in blockchain applications, such as elliptic curve Diffie-Hellman key exchange (ECDHE) that adopted by the authors of [18] , and the authors of [14,19,20] used SHA-256, while the authors of [21,22] adopted on the local public key, as shown in Table 3. There are also other cryptography approaches such as the advanced encryption standard (AES), ECDSA, and identity-based signature (IBS), all of which have certain advantages and disadvantages. We used ECDSA in our scheme due to its low memory requirements and low computational complexity.

The hardware dependency is another important criterion that we considered when designing our scheme. Our results from the implementation of ECDSA on an ARM Cortex-M4 show that this was the faster and optimum selection. The fifth criterion is energy consumption, which depends on the type of consensus mechanism and encryption method used. We utilized PoAh, as it is energy efficient in comparison with other consensus algorithms, as discussed above. The sixth criterion represents the time it takes to complete a task, which relates to the performance of the proposed framework and depends on consensus algorithm type, utilizing resources, execution time, and energy efficiency. From experimental results, our framework requires less time than other frameworks.

The last criterion of our comparison is the security attacks, in which attackers can exploit the vulnerable points in the system to satisfy their goals. As in Table 3, the authors of [14,20] used PoW as a consensus algorithm, which is susceptible to 51%, Sybil, balance, and double-spending attacks [11,35]. The authors of [18] utilized the IBS as a consensus mechanism, which is susceptible to Sybil and DDoS attacks [9]. The authors of [19] adopted PoC, which is also susceptible to 51%, double spending and Sybil attacks [35]. In addition, the authors of [21] utilized the PBFT for the verifying process and this algorithm is exposed to Sybil attacks, while the authors of [22] depend on Delegate PoS, and this algorithm is also vulnerable to 51%, double spending and Sybil attacks [35]. With our architecture, we succeeded in being resistant to all of the aforementioned types of attacks by utilizing the private blockchain, smart contract, ECDSA, lightweight nodes and PoA algorithm.

In our experiments, we achieved faster performance with a lower power consumption than other similar frameworks. Our proposed architecture successfully implements a decentralized, secure, energy-efficient, fast and effective blockchain platform for an industrial environment (a cement factory) by combining the advantageous features of the ECDSA, a private blockchain network, and the PoAh consensus mechanism.

Recall, our scheme fast and secure than other schemes due to the utilization of PoAh as a consensus mechanism to authenticate new blocks in the blockchain network that featuring by lowest time to authenticate the new blocks, also it solved the security problem of 51% and Sybil attack founded with traditional consensus algorithms such as PoW, PoC, and DPoC. ECDSA used for data encryption that is secure and low computational complexity; in addition, the use of blockchain technology (private blockchain platform) helps in eliminate the dependence on third-party services, which address the problems related to a single point of failure, bottleneck, and slow execution. Moreover, using of smart contract gives the immutability of the ledger that help to resistance for many common security attacks such as tampering, 51%, replay, modification, Sybil, Man in Middle, DoS, and distributed DoS. While other schemes that adopted on other consensus algorithms and platforms that expose to most of the mentioned common security attacks.

8. Conclusions

In our work, we have proposed a decentralized, scalable, lightweight, low power, trusted security architecture for a cement factory as an industrial application area based on blockchain technology. We successfully integrated blockchain technology with IoT devices in an industrial environment.

Our proposed system carries out user and device registration using a private blockchain. Then, all transmitted data are stored as transactions in blocks while sending a copy of all transactions to the lightweight nodes to provide a backup of these transactions for use in case of a single node crash, which ensures the stability of operation for the machines through a P2P connection. Our proposed architecture is shown to be efficient, as it had reduced computational complexity and achieved the lowest execution time (1.1236 s) and lowest energy consumption (209.915 mW) compared to other schemes. It also offers enhanced security for an industrial environment through the use of an asymmetric cryptography algorithm. Furthermore, due to the use of a private blockchain, our architecture provides resistance to most kinds of common cybersecurity attacks on IoT networks of devices, such as Sybil, 51%, tampering, impersonation, replay, repudiation, DoS, and distributed DoS. All of this achieved through the decentralized architecture and the immutable features of blockchain ledgers, in which entries are made using smart contracts. In addition to the fast, highly scalable, and low energy proof of authentication (PoAh) adopted as a consensus mechanism that helps to enhance the computational performance by eliminating the reverse hash function process used in PoW, it also eliminated centralized dependencies, which makes blockchain lightweight and more suitable for resource-constrained devices.

In comparison with centralized architectures, our proposed scheme yields excellent performance, as demonstrated by our experimental results. Our system integrates blockchain technology with IIoT, and can therefore guarantee secure authentication and privacy preservation for the transmitted data. With this level of security, authorized clients (blockchain network participants) would be able to gain access to the private network and find out information on the cement production process, such as the quality, quantity, production capacity, production dates and power consumption. Security authentication and privacy preservation typically not considered in conventional IIoT systems, unlike in our work. We can successfully modernize conventional cement factories based on our new architecture in which the blockchain technology integrated with IIoT to create a secure industry environment.

Author Contributions: Conceptualization, S.M.U.; Funding acquisition, S.L.; Resources, S.M.U. and Z.A.A.; Software, S.M.U.; Supervision, S.L.; Visualization, S.M.U., J.Z. and J.W.; Writing—original draft, S.M.U.; Writing—review and editing, S.M.U. and Z.A.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Hubei Provincial Science and Technology Major Project of China grant number 2020AEA011 and the Key Research and Development Plan of Hubei Province of China grant number 2020BAB100. and the Science and Technology Program of Shenzhen of China grant number JCYJ20170818160208570.

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

References

1. Wan, J.; Li, J.; Imran, M.; Li, D.; e Amin, F. A Blockchain-Based Solution for Enhancing Security and Privacy in Smart Factory. *IEEE Trans. Ind. Inform.* **2019**, *15*, 3652–3660. [CrossRef]
2. Chen, Y. A Survey on Industrial Information Integration 2016-2019. *J. Ind. Integr. Manag.* **2019**, *5*, 33–163. [CrossRef]
3. Zyskind, G.; Nathan, O. Decentralizing privacy: Using blockchain to protect personal data. In Proceedings of the 2015 IEEE Security and Privacy Workshops, San Jose, CA, USA, 21–22 May 2015; pp. 180–184. [CrossRef]
4. Hang, L.; Kim, D.H. Reliable task management based on a smart contract for runtime verification of sensing and actuating tasks in IoT environments. *Sensors* **2020**, *20*, 1207. [CrossRef] [PubMed]
5. Bertino, E.; Islam, N. Botnets and internet of things security. *Computer* **2017**, *50*, 76–79. [CrossRef]
6. Khan, M.A.; Salah, K. IoT security: Review, blockchain solutions, and open challenges. *Future Gener. Comput. Syst.* **2018**, *82*, 395–411. [CrossRef]
7. Ren, W.; Wan, X.; Gan, P. A double-blockchain solution for agricultural sampled data security in Internet of Things network. *Future Gener. Comput. Syst.* **2021**, *117*, 453–461. [CrossRef]
8. Fernández-Caramés, T.M.; Fraga-Lamas, P. A Review on the Application of Blockchain to the Next Generation of Cybersecure Industry 4.0 Smart Factories. *IEEE Access* **2019**, *7*, 45201–45218. [CrossRef]
9. Latif, S.; Idrees, Z.; Ahmad, J.; Zheng, L.; Zou, Z. A blockchain-based architecture for secure and trustworthy operations in the industrial Internet of Things. *J. Ind. Inf. Integr.* **2021**, *21*, 100190. [CrossRef]
10. Prashar, D.; Jha, N.; Jha, S.; Joshi, G.P.; Seo, C. Integrating IOT and blockchain for ensuring road safety: An unconventional approach. *Sensors* **2020**, *20*, 3296. [CrossRef]

11. Sayeed, S.; Marco-Gisbert, H. Assessing blockchain consensus and security mechanisms against the 51% attack. *Appl. Sci.* **2019**, *9*, 1788. [CrossRef]
12. Puthal, D.; Mohanty, S.P.; Nanda, P.; Kougianos, E.; Das, G. Proof-of-authentication for scalable blockchain in resource-constrained distributed systems. In Proceedings of the 2019 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 11–13 January 2019; pp. 1–5. [CrossRef]
13. Wang, F.Y.; Yuan, Y.; Zhang, J.; Qin, R.; Smith, M.H. Blockchainized Internet of minds: A new opportunity for cyber–physical–social systems. *IEEE Trans. Comput. Soc. Syst.* **2018**, *5*, 897–906. [CrossRef]
14. Rathee, G.; Ahmad, F.; Sandhu, R.; Kerrache, C.A.; Azad, M.A. On the design and implementation of a secure blockchain-based hybrid framework for Industrial Internet-of-Things. *Inf. Process. Manag.* **2021**, *58*, 102526. [CrossRef]
15. Hassan, M.U.; Rehmani, M.H.; Chen, J. Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions. *Future Gener. Comput. Syst.* **2019**, *97*, 512–529. [CrossRef]
16. Wang, Q.; Zhu, X.; Ni, Y.; Gu, L.; Zhu, H. Blockchain for the IoT and industrial IoT: A review. *Internet Things* **2020**, *10*, 100081. [CrossRef]
17. Nakamoto, S.; Bitcoin, A. A peer-to-peer electronic cash system. *Gen. Philos. Sci.* **2008**, *39*, 53–67. [CrossRef]
18. Shen, M.; Liu, H.; Zhu, L.; Xu, K.; Yu, H.; Du, X.; Guizani, M. Blockchain-assisted secure device authentication for cross-domain industrial IoT. *IEEE J. Sel. Areas Commun.* **2020**, *38*, 942–954. [CrossRef]
19. Cao, Y.; Jia, F.; Manogaran, G. Efficient traceability systems of steel products using blockchain-based industrial Internet of Things. *IEEE Trans. Ind. Inform.* **2019**, *16*, 6004–6012. [CrossRef]
20. Hu, W.; Li, H. A blockchain-based secure transaction model for distributed energy in Industrial Internet of Things. *Alex. Eng. J.* **2021**, *60*, 491–500. [CrossRef]
21. He, S.; Ren, W.; Zhu, T.; Choo, K.K.R. Bosmos: A blockchain-based status monitoring system for defending against unauthorized software updating in industrial internet of things. *IEEE Internet Things J.* **2019**, *7*, 948–959. [CrossRef]
22. Gul, M.J.; Subramanian, B.; Paul, A.; Kim, J. Blockchain for public health care in smart society. *Microprocess. Microsyst.* **2021**, *80*, 103524. [CrossRef]
23. Gottheil, A. Can Blockchain Address the Industrial IOT Security? 2018. Available online: http://www.mendeley.com/research/1d757d78-43de-3238-9fbe-690c96c5f960/ (accessed on 26 November 2020).
24. Lee, M.S.; Jang, D.J. A survey of blockchain security issues. *JP J. Heat Mass Transf.* **2020**, *2020*, 29–35. [CrossRef]
25. Shrestha, R.; Nam, S.Y. Regional blockchain for vehicular networks to prevent 51% attacks. *IEEE Access* **2019**, *7*, 95033–95045. [CrossRef]
26. Yang, X.; Chen, Y.; Chen, X. Effective scheme against 51% attack on proof-of-work blockchain with history weighted information. In Proceedings of the 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 14–17 July 2019; pp. 261–265. [CrossRef]
27. Ye, C.; Li, G.; Cai, H.; Gu, Y.; Fukuda, A. Analysis of security in blockchain: Case study in 51%-attack detecting. In Proceedings of the 2018 5th International Conference on Dependable Systems and Their Applications (DSA), Dalian, China, 22–23 September 2018; pp. 15–24. [CrossRef]
28. Yin, C.; Zhang, S.; Xi, J.; Wang, J. An improved anonymity model for big data security based on clustering algorithm. *Concurr. Comput. Pract. Exp.* **2017**, *29*, e3902. [CrossRef]
29. STMicroelectronics. X-CUBE-CRYPTOLIB: STM32 Cryptographic Firmware Library Software Expansion for STM32cube (UM1924). 2020. Available online: https://www.st.com/en/embedded-software/x-cube-cryptolib.html (accessed on 5 January 2021).
30. Puthal, D.; Mohanty, S.P. Proof of authentication: IoT-friendly blockchains. *IEEE Potentials* **2018**, *38*, 26–29. [CrossRef]
31. Alharbi, S.; Rodriguez, P.; Maharaja, R.; Iyer, P.; Bose, N.; Ye, Z. FOCUS: A fog computing-based security system for the Internet of Things. In Proceedings of the 2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 12–15 January 2018; pp. 1–5. [CrossRef]
32. Arm Ltd. Microprocessor Cores and Technology. 2020. Available online: https://www.arm.com/products/silicon-ip-cpu (accessed on 5 January 2021).
33. Teslya, N.; Ryabchikov, I. Blockchain platforms overview for industrial IoT purposes. In Proceedings of the 2018 22nd Conference of Open Innovations Association (FRUCT), Jyvaskyla, Finland, 15–18 May 2018; pp. 250–256. [CrossRef]
34. Tamboli, M.B.; Dambawade, D. Secure and efficient CoAP based authentication and access control for Internet of Things (IoT). In Proceedings of the 2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), Bangalore, India, 20–21 May 2016; pp. 1245–1250. [CrossRef]
35. Bamakan, S.M.H.; Motavali, A.; Bondarti, A.B. A survey of blockchain consensus algorithms performance evaluation criteria. *Expert Syst. Appl.* **2020**, 113385. [CrossRef]