applied sciences

MDPI

Article

BBAP-WSN: A New Blockchain-Based Authentication Protocol for Wireless Sensor Networks

Murat Dener [1,*] and Abdullah Orman [2]

[1] Information Security Engineering, Graduate School of Natural and Applied Sciences, Gazi University, 06560 Ankara, Turkey
[2] Department of Computer Technologies, Ankara Yıldırım Beyazıt University, 06010 Ankara, Turkey
* Correspondence: muratdener@gazi.edu.tr

Abstract: Wireless Sensor Networks—WSNs, an important part of IoT—consist of sensor nodes with limited processing, memory capacities, and energy. Wireless Sensor Networks face many dangers as they are often distributed into untrusted regions. The accuracy of the data obtained in a WSN, where security threats cannot be prevented, is also questioned. In WSNs, the authentication of the resources and the data can be verified with the authentication mechanism. Authentication in WSNs allows the node to verify whether data have been sent from authorized sources and protects the original data from changes. However, there are some deficiencies in terms of security in existing authentication protocols such as ID spoofing attacks. In addition, blockchain, one of the emerging technologies, gives significant successful results in security applications. Cryptographically secured, immutable, non-repudiable, irrevocable, auditable, and verifiable can be given as security-related characteristics of the blockchain. This study aims to use these features of the blockchain in WSNs. In this study, a new blockchain-based authentication protocol was developed for WSNs. Based on the study's system model, sensor nodes, cluster nodes, base station, and blockchain networks were created using a private blockchain, and users. A detailed security analysis was carried out for the study. At the same time, efficiency analysis was performed by implementing the proposed model on the WiSeN sensor node.

Keywords: blockchain; authentication; security; wireless sensor networks; WSN

check for updates

Citation: Dener, M.; Orman, A. BBAP-WSN: A New Blockchain-Based Authentication Protocol for Wireless Sensor Networks. *Appl. Sci.* **2023**, *13*, 1526. https://doi.org/10.3390/app13031526

Academic Editor: Christos Bouras

Received: 9 December 2022
Revised: 18 January 2023
Accepted: 18 January 2023
Published: 24 January 2023

1. Introduction

Wireless networks consisting of many sensor nodes designed to measure the physical conditions in the environment are called Wireless Sensor Networks (WSN). Wireless Sensor Networks are used in many areas such as home automation, industry, the military, health, the environment, commerce, and transportation. Hundreds of applications can be made in each area. For example, many applications can be made in the environmental area, such as monitoring agricultural land, measuring water pollution, and monitoring forest fires. Wireless Sensor Networks can be found in controlled environments such as gardens or stadiums. However, they can also be found in uncontrolled environments in applications such as monitoring border security and monitoring forest fires.

The number of WSNs can vary depending on the application. For example, while ten-level sensor nodes are used to monitor a small pool, thousands of sensor nodes are used for the fire monitoring of a large forest. Furthermore, each application has its own priority. For example, while the priority is energy in some applications, it is delay in some applications or security in others.

Wireless Sensor Networks are an important part of the IoT [1]. Especially recently, the smart city concept has become widespread in increasing people's comfort and improving their living standards. Security is an important need for data and applications in the IoT and WSNs, which pioneered the establishment of smart cities. In particular, the security threat to WSNs in uncontrolled environments is quite high. Attacking nodes can be left to the relevant environment, causing many negative effects such as the transmission of false information to the network, and causing the nodes to fail. As a result, the WSN cannot achieve its purpose and the costs incurred for this network are wasted. While message listening is performed in passive attacks in the WSN, wrong packets may be injected into the network in active attacks. Because the wireless medium is insecure, communications between nodes are considered insecure.

Authentication is used to prevent such security breaches [2]. Data authentication in sensor networks allows the system to verify whether data have been sent from authorized sources and protects the original data from changes. Authentication is very important in communication security for WSNs. Thanks to authentication, during communication between two sensor nodes, the source node knows that the node to which it sent a message is a real node. With authentication, only sensor nodes that can be authenticated can access the network, while others cannot. In this way, unauthorized users are prevented from accessing the network.

Authentication in WSNs can be achieved in many ways [3]. Different options such as IDs, certificates, cryptographic protocols, MAC addresses, and passwords can be used while providing authentication. However, there are some disadvantages to the methods used. ID-based authentication methods are vulnerable to an ID spoofing attack. The memory-processor needs of certificate-based authentication methods are very high in terms of sensor nodes. In cryptographic protocol-based authentication methods, security depends on the strength of the encryption protocol. Nonrepudiation is impossible for MAC address- and ID/Password-based authentication methods.

A robust authentication mechanism does not allow any sensor node to join the network except its own members. It should also be strong against Data Integrity, Non-Repudiation, Sybil Attacks, Spoofing Attacks, Message Substitution Attacks, Message Replay attacks, Man in the Middle Attacks, and Denial of Service attacks [4]. It should be scalable. A well-designed authentication protocol should have Mutual Authentication. All the while, the limited energy, processing, and memory capacities of the WSN need to be considered.

Blockchain, one of the emerging technologies, gives successful results in security [5]. In WSN applications that require security, messages sent for data capture or deception by infiltrating the system will be blocked by the ability to transfer information over the blockchain. Blockchain and smart contracts-based solutions can successfully perform authentication and access control over networks [6]. In addition, security models made from a single center are attractive to all attackers. As a result, different attacks can be made to capture the relevant center. However, this threat can be eliminated since blockchain applications have no single center.

As data increase in blockchain networks, the number of blocks increases, so the need for memory increases [7]. At the same time, as the data increase, the number of transactions and the energy requirement will increase in verifying blocks and adding new blocks to the chain [8]. Since the sensor nodes in the WSN are also thought to have limited capacity, it is necessary to integrate the WSN and blockchain together without increasing excessive transaction and energy consumption in order to use the important features of blockchain to meet the security needs of the WSN.

In this study, a new blockchain-based authentication protocol has been developed for WSNs. In summary, the contributions of the study are as follows:

- A blockchain-based authentication protocol is developed for high-security applications. While non-blockchain authentication protocols are vulnerable to certain attacks, the blockchain structure, proven to be high security, is applied in this study. Compared to the existing limited work involving blockchain-based WSNs, very good results are achieved in terms of security and efficacy.
- Blockchain-based WSN authentication models in the literature are examined.
- A private blockchain structure is created considering security, transaction speed, ownership criteria, and suitability for WSNs.

- Proof of Authentication (PoAh) is used as the consensus mechanism.
- A WSN System model is created as Sensor Node (SN), Cluster Node (CN), Base Station (BS), Blockchain Network (BCN), and User (U).
- The developed protocol consists of the Initialization section, where the initial values are generated, the registration section, where the nodes in the network are registered, the authentication section, where the nodes in the network are verified, and the unregistration section, which is the removal of the nodes leaving the network for any reason.
- The Elliptic Curve Digital Signature Algorithm (ECDSA), ECC, and Smart Contract are used in the developed protocol.
- A detailed security analysis of the study is made.
- The proposed protocol is implemented to real sensor nodes and efficiency analysis is carried out in this way.
- In addition to being used in applications requiring high security, the proposed authentication protocol is also efficient considering the latency-energy-memory usage criteria.

The remaining sections of the study are as follows: While the related studies are mentioned in Section 2, blockchain is explained in Section 3. Then, in Section 4, the system model, in Section 5, the introduction of the proposed protocol, and in Section 6, the security and efficiency analysis of the study are given. Finally, the last section includes the results of the study and the topics for future work.

2. Related Works

Many studies have been conducted to address authentication in WSNs. These studies can be divided into blockchain-based and non-blockchain studies.

In non-blockchain studies [2,9–11], there is low security [12] due to central controls, client-server architecture, and exposure to many attacks. Some of these studies are as follows:

In the study [13], a secure user authentication model is proposed for wireless sensor networks used in the healthcare area. The authentication model that provides security and confidentiality comes into play when medical personnel want to see or approve patients' information. The study consists of three phases: model registration, login, and authentication. Medical personnel can safely process the health conditions of patients with the proposed study. Smart cards and bilinear pairing-based encryption are used for data verification. It is stated that the proposed model is resistant to the following attacks: impersonation attacks, replay attacks, online and offline password guessing attacks, and stolen verifier attacks.

In another study [14], an authentication model was proposed by making use of users' biometric data. In order to keep the network secure, only authenticated users were able access the network. Fingerprint data were used with the help of users' PDAs or smart phones without the need for any additional equipment. It consisted of two phases, enrollment and authentication. The validity of the model was tested with the Burrows–Abadi–Needham (BAN) logic.

In another study [15], an authentication center was created using RSA, AES, SHA-1. Sensor nodes were able to join the network after receiving approval from the relevant central unit. The central unit contained a microcontroller Unit and a WiFi module.

In another study [16], a data authentication model is proposed for data integrity and availability. In the model, all sensor nodes go through the validation process. It consists of three stages: preparing a signature packet, data storage and authentication, and data verification and collection. The MAC value is generated for the data and the signed packet is obtained in the model.

In another study [17], an authentication model based on a digital watermark was proposed. The model consists of three stages: watermark generation, embedding, and detection. In these processes, techniques such as XOR, insertion, and extraction of bits are used.

In another study [18], a secure authentication and integrity technique was proposed. Digital signature and public key encryption were used in the model.

In another study [19], an authentication model was proposed. The model consists of four phases: pre-deployment, registration, login and authentication, and password-change. The hash function and XOR computation are used in the model. The model is resistant to the following attacks: replay attack, stolen smart card attack, and off-line password guessing attack.

In most of the non-blockchain studies, the authentication method has been developed by using known techniques. For example, in a study [20], a secure authentication protocol was developed for wireless sensor networks using machine learning techniques. The behavior of the nodes is monitored. Trust value is calculated according to these behaviors. In the verification process, if the trust value is lower than the specified threshold, the node cannot join the network. The threshold value is calculated by the Support Vector Machine (SVM) method using the collected traffic data. While calculating these values, Packet Delivery Ratio, Delay, Residual Energy, and Computational Overhead values are used. While there are many machine learning methods, SVM is preferred because it requires less computation. In another study [21], an adaptive trust-based authentication model was proposed. Authentication is performed using the trust score. The trust score is calculated by considering the location information of the nodes. The timestamp is also taken into account when calculating the trust score. The Honey Encryption (HE) technique is used for encryption. In another study [22], the K-means technique was used for validation. Authentication takes place between cluster leaders and cluster member nodes. In another study [23], a deep learning-based authentication model was proposed. The deep neural network (DNN), the convolutional neural network (CNN), and the convolution preprocessing neural network (CPNN) algorithms are implemented on the nodes. The most effective solution among them has been with CPNN. The model consists of three stages: Initialization, Authentication, Retraining. In another study [24], authentication was performed using the fuzzy technique.

Unfortunately, the above studies without blockchain cannot be used in applications that need high security requirements.

In terms of the IoT, the concept of things has a very broad meaning. All kinds of monitoring devices, sensors, and access devices are considered as things. For example, when we think in terms of a house, air conditioners, cameras, lamps, TVs, modems, dishwashers, and refrigerators can be considered as things. The IoT, on the other hand, defines the communication network in which physical objects relate to each other or with larger systems. Wireless Sensor Networks are a subset of the IoT. Wireless Sensor Networks are one of the technologies often used in an IoT system [25]. The WSN has sensor nodes with limited capacity. Each sensor node has a limited memory, processor, and power to be cost-effective as their number is huge according to the application. In summary, there is a difference in capacity between IoT and WSN hardware. High-capacity devices can be found in the IoT, while more limited devices are available in WSNs. That is why the IoT–blockchain relationship and the WSNs–blockchain relationship are different.

Since blockchain-based WSN studies are not enough, IoT–blockchain studies [6,26–35], IoT–blockchain–cloud studies [36], IIoT–blockchain studies [37–39], and smart system–blockchain studies [40–42] were researched. It has been seen that the studies are not suitable for WSNs when considered in terms of cost. The communication protocols used in these studies cannot be used directly in sensor nodes due to the required processing and memory capacity.

The limited studies involving blockchain-based WSNs are as follows: In the review study [43], studies involving blockchains in WSNs were discussed. The studies are classified as Data Security and Reliability, Data Management and Storage, Node Recovery, Energy Efficiency. These studies [44–47] include WSN-blockchain and are incomplete and undetailed studies. There is not much to know, such as the type of blockchain implemented, the consensus mechanism, and how smart contracts work. In another study [48], blockchain was used with AES and the accuracy of the proposed methodology was measured on a temperature–humidity-sensing IoT-based WSN. In another study [49], blockchain technology was implemented in real nodes and the transaction steps were explained in detail. This study was carried out as a basic study at a simple level.

The limited number of studies that fully combine blockchain-based WSN technology are as follows: In the study [50], a hybrid model is proposed in the form of a local blockchain with cluster leaders and a public blockchain with base stations. While the public blockchain is used to verify the cluster leaders, the local blockchain is used to verify the cluster member sensor nodes. The authentication model consists of four stages: initialization, registration, authentication, and node logout. In another study [51], a hybrid model is proposed, including an internal blockchain with sensor nodes and a global blockchain with cluster leaders. It consists of four stages, namely Security Parameter Fixing, Blockchain Joining, Authorization, and Sensor Deregistration. Structurally, it is similar to the study numbered [50]. In another study [52], a trust model and blockchain-based authentication are suggested for secure routing. A smart contract, public and private blockchains, are used for authentication. A local blockchain is created using the private blockchain between the cluster nodes, and a global blockchain is created using the public blockchain for the base station. In another study [53], a secure routing mechanism based on blockchain is proposed for WSNs. The sensor nodes and cluster nodes in the network are verified and, using the public blockchain also known as permissionless blockchain, the cluster nodes–base station is verified by using the private blockchain also known as permissioned blockchain.

The common aspect of these studies is that they use private blockchain technology for cluster nodes and public blockchain technology for the base station. However, cluster nodes with limited capacity in the WSN need to increase their capacity to take part in this process. Therefore, the cost of WSN increases. This situation is not fully compatible with the structure of the WSN.

In this study, a new blockchain-based authentication protocol has been developed for WSNs by eliminating the stated deficiencies.

3. Blockchain

Blockchain [54], a distributed ledger form, is a special data storage tool. Data are added to structures called blocks. Each block consists of two parts, the head and the body. The block number, nonce value, timestamp, the previous block's hash value, and the block's hash value are kept in the head section. The transactions/data are kept in the body section.

The hash value of the previous block in the head section is not included in the genesis block called the starting block. The block number indicates the number of the block, while the Nonce value, "Number Only Used Once", refers to a number or value that can be used only once. The nonce is often used in authentication protocols and cryptographic hash functions. In blockchain technology, a nonce refers to a pseudo-random number used as a counter during the mining process. The timestamp indicates the time the block was generated.

In addition, each block's hash values are stored for itself and for the previous block. In this way, each block carries information about the previous block. The fact that blocks are connected in the form of a chain characterizes the meaning of blockchain. Therefore, once data are stored in the blockchain, it is almost impossible to change or delete them. The basis of almost every blockchain is the mining process based on hash algorithms. It takes an input of any length and produces an output that will always be the same length. The output is called a "hash" and consists of 64 characters (256 bits). Because it is a one-way function, it is almost impossible to calculate the input from the output.

A Merkle tree is a way of organizing and structuring large amounts of data. In the Merkle tree structure, when a transaction is made, it is hashed and then an equivalent hash value is given. After each transaction is hashed in the Merkle tree, the generated hashes are matched against another hash value and then hash again. This process of matching hash values is repeated until a final hash value is generated. The last hash value, the Merkle root, provides a summary of all the transactions it contains. The Merkle root digest is then appended to the block header. The resulting output is the block hash and will serve as the identifier of the newly created block. SHA-256 is used as the hash. These situations are illustrated in Figure 1. In the study, information about the node and data in the network were kept in the blocks. While the information about the node consists of an ID, PVK, PBK, IDcard, and CN to which SN belongs, the data in the network consist of SN, Temp, and Hum data. Each SN datum is considered as a unit. Therefore, the capacity of each block is set to 100 units of data. After sufficient data are received, a new block is created.

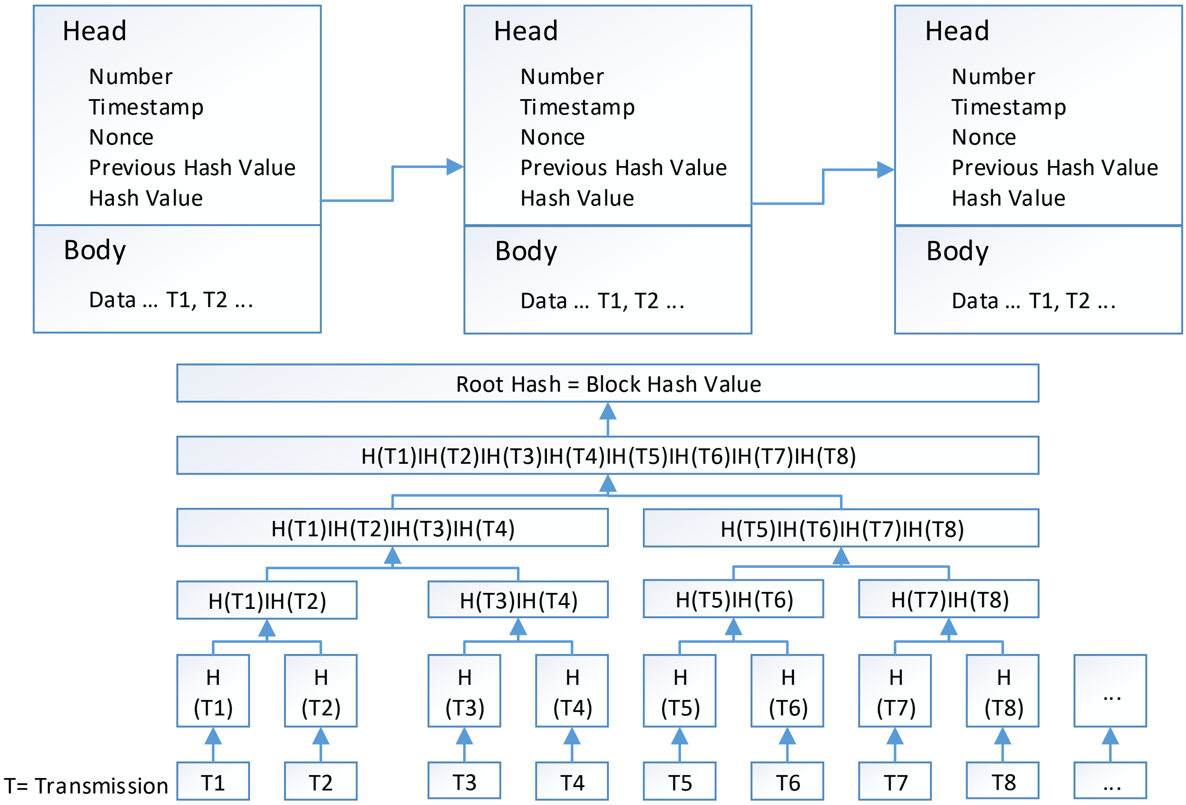

Figure 1. Blockchain system.

There are four types of blockchains. These are Public Blockchain, Private Blockchain, Hybrid Blockchain, and Consortium Blockchain. Public Blockchain is the ledger where records of all transactions are kept publicly. A public blockchain network is decentralized and does not require a trusted central authority to verify transactions. The word "public" means that anyone can join the blockchain network with read and write access permission. It is a permissionless platform where anyone can join and trade. A private blockchain is also known as a permission-based blockchain. An entity controls the block with read and write access. In this type of blockchain, access permissions are often restricted. Only authorized participants can access the chain network. The miners or validators are predefined in the private blockchain. The proposed blockchain mechanism is built on a private network that provides access to authorized users only. Hybrid Blockchain uses both the benefits of Private Blockchain's access control and the transparency features of Public Blockchain. It allows businesses to choose what information they want to keep private and what information they want to make public. Finally, Consortium Blockchain It is known as a semi-decentralized blockchain. It is not set up as a single person/organization private blockchain; instead, it is set up with a group of approved persons/institutions. In addition, a consortium blockchain is a predefined group of nodes on the network.

A private blockchain can be used as an isolated network of the IoT that can protect it from the outside world. In this study, a Private Blockchain structure was created considering the security, transaction speed, scalability, and ownership criteria and considering it the most suitable for WSN [55,56]. Private blockchains have fewer nodes, so the time taken to verify a transaction is less. Furthermore, the network sizes of private blockchains can be customized as desired.

The data in the blockchain network must exist in synchronous form in all blocks. Therefore, a network-wide consensus is required for this to occur. Blockchain platforms show different approaches in this regard. Examples of these consensus mechanisms are Proof of Work (PoW), Proof of Stake (PoS), Proof of Activity (PoA), Delegated Proof of Stake (DPoS), Practical Byzantine Fault Tolerance (PBFT), Proof of Existence (PoE), and Proof of Authentication (PoAh). These mechanisms ensure that all blocks contain the same information and no inconsistent data [57].

Adding a transaction to all nodes as a block in the blockchain network generally consists of seven steps. These steps are as follows:

1. A node sends a transaction request to the Chain network.
2. A new block containing the requested transaction is created and forwarded to the nodes in the Chain network.
3. Nodes in the network verify and validate the block.
4. The block is approved by the consensus protocol.
5. The verified block is sent to all nodes for inclusion in the existing chain.
6. A new block is added to all nodes.
7. The process is completed.

This study uses the Proof of Authentication (PoAh) consensus mechanism [58,59]. The PoAh consists of two steps. In the first step, the source of the block is authenticated. In the second step, the trust value of each authenticating node is increased by one. If the node authenticates incorrectly, the trust value is decreased by one. Then, the validated block is forwarded to all nodes for updating. The reason for using PoAh in this study is that it is more efficient according to energy consumption, process requirements, and delay criteria compared to mechanisms such as PoW, PoS, and PoA.

4. System Model

The proposed WSN System model is given in Figure 2.

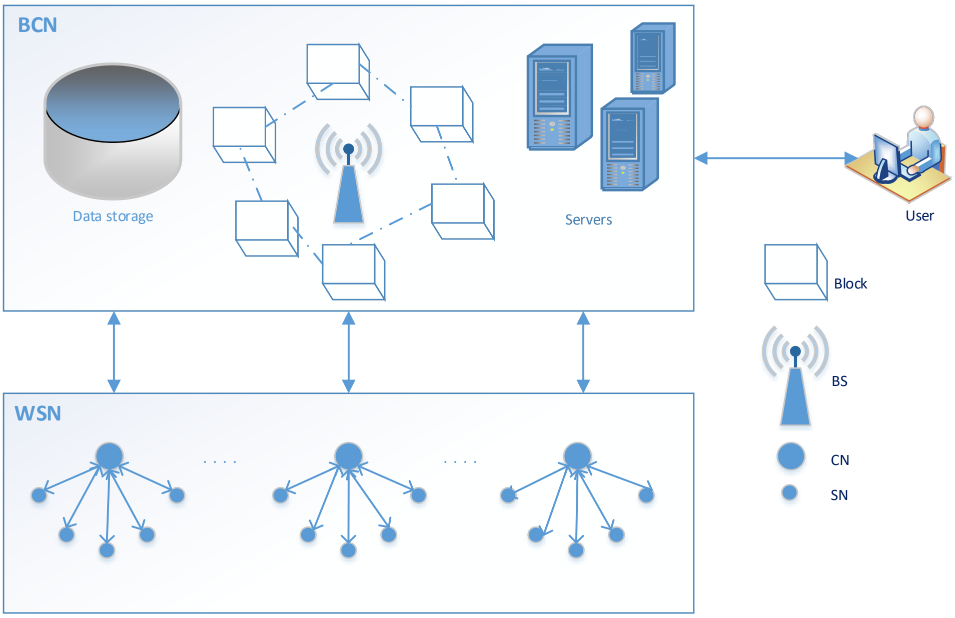

Figure 2. System model.

Wireless Sensor Networks consist of sensor nodes, cluster nodes, a base station, and a user. SNs have limited computing capabilities, limited energy, and limited storage capacity. The SNs perform the detection function and transmit it to their leader CN. The CNs receive the transmitted data and forward them to the BS.

In the proposed system model, there are four different actors. These are the Sensor Node (SN), Cluster Node (CN), Base Station (BS), and User (U).

SN: It refers to the sensor nodes in the environment. These nodes transmit the values they perceive from the environment to the CN of which they are members. Processing capacities and energies are limited.

CN: It refers to the Cluster Node. It transmits the data sent by the SNs in its cluster to the BS. Processing capacities and energies are limited in CNs as SNs because CNs act as routers between the SN and BS.

BS: It refers to the Base Station. It receives data transmitted by CNs. These data are also processed on the blockchain network. The BS is considered unlimited in terms of energy, memory, and processing capacity.

U: It refers to the end user. It can monitor the WSN by connecting to the network whenever it wishes.

There are three different communications in the WSN: SN–CN, CN–BS/BCN, and U–BS/BCN. These communications are bidirectional.

Implementing blockchains in the WSN is a major challenge, given resource-constrained devices. Because blocks are held at each node, the larger the block size, the longer the consensus mechanism will be, and the greater the need for storage. Except for the BS in the WSN, SNs or CNs have insufficient capacity to hold these blocks. Even if CNs are strengthened with additional hardware, considering that the number of nodes in WSNs is excessive, the cost will increase. In this case, it is not suitable for the nature of the WSN. Therefore, the model in Figure 2 has been proposed considering that it is suitable for the WSN. As seen in Figure 2, the storage of the BC takes place at the BS level.

5. Proposed Protocol

The proposed protocol consists of four stages, which are the initialization section, where the initial values are generated, the registration section, where the nodes in the network are registered, the authentication section, where the nodes in the network are verified, and the unregistration section, which is the removal of nodes leaving the network for any reason. The operations at these stages are automatic. The whole process is carried out under the command of the base station. The same operations are repeated for the relevant nodes if new nodes are added to the network. Finally, the newly joined node information is announced to the network. All necessary information for the network such as the nodes' identities and SN-CN mappings are reported to the nodes by the base station.

Moreover, smart contracts are computer programs that can carry out transactions and agreements between anonymous parties reliably and consistently and cannot be changed retrospectively. In this study, smart contracts are written on nodes as code. In this context, the term "smart contracts" is used. First of all, time information is checked in all transactions. This way, it can be evaluated whether the relevant transaction is up-to-date. The current time information is always visible in the BS. The BS provides this information when needed in the CN and SN nodes.

5.1. Initialization

At this stage, the BS makes all the nodes ready. Each node has its own unique ID. The ID of the sensor node i is specified as IDSNi. The ID of cluster node i is specified as IDCNi, while the ID of the BS node is specified as IDBS. The BS generates public and private keys for SN-CN and itself. The public and private keys of the BS node are specified as PBKBS, PVKBS, the public and private keys of the CN node are specified as iPBKCNi, PVKCNi, and the public and private keys of the SN node i are specified as PBKSNi, PVKSNi.

Keys are used to verify the integrity of messages sent during verification and registration. The ID and PVK information of the sensor and cluster nodes are transmitted in the form of ID, and PVK in a secure environment to be stored at the relevant nodes. IDcard is produced for CNs. IDcard includes a signature created using IDCNi, PVKBS, and the Elliptic Curve Digital Signature Algorithm (ECDSA). As it is known, the Elliptic Curve Digital Signature Algorithm (ECDSA) is a Digital Signature Algorithm (DSA) that uses elliptic curve encryption. In Figure 3, the sequence diagram of the initialization part is given.

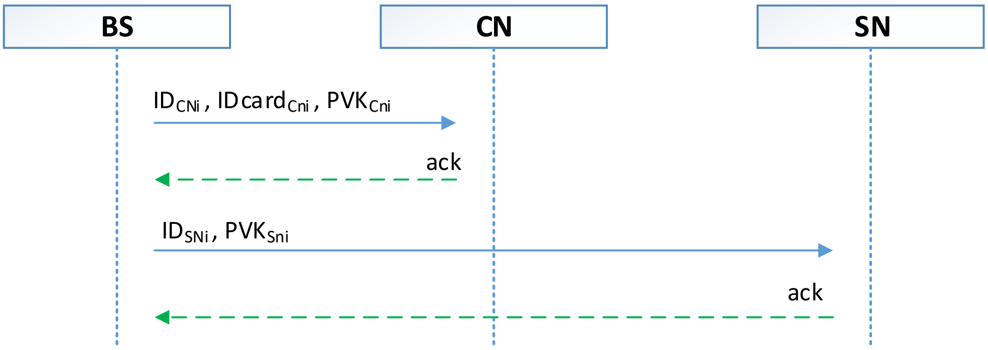

Figure 3. Sequence diagram of the initialization.

5.2. Registration

After the initialization of the network, it is time to enroll. The CNs request registration by forwarding IDCNi, IDcardCni, and Time information to BS. Then, the smart contract (Algorithm 1) in the BCN is triggered. First, the Time information is checked. Next, it is checked whether the CN is registered in the BCN. Finally, IDCNi and PBKBS are used to authenticate the IDcard. If verification takes place in all of these processes, the CN will be registered with the BCN.

Algorithm 1 CN registration

```
begin
    if time_check = error; Return error();
    if $ID_{CNi}$_check = error; Return error();
    if $IDcard_{Cni}$_check = error; Return error();
    register($ID_{CNi}$, $IDcard_{Cni}$);
end
```

Although smart contracts can be used in CN-BS/BCN communications, these transactions were carried out with ECC since SN-CN communications have insufficient storage, processing capacity, and energy. Elliptic Curve Cryptography is preferred because it provides high security with low transaction costs [60–63]. Each SN in the WSN is a member of only one CN. The SNs transmit IDSNi, Messageencyrypted, and Time information to predetermined CNs. The CNs first check the time information. Then, using the node's own PVKSNi, they verify the encrypted message with PBKSNi. If there is no problem so far, the CN sends IDCNi, IDSNi, IDcardCni, and Time information to the BS and requests the SN's registration request. Then, the smart contract (Algorithm 2) in the BCN is triggered. First, the Time information is checked. Next, whether the CN and SN are registered in the BCN is checked. Finally, IDCNi and PBKBS are used to authenticate the IDcard. If verification occurs in all of these processes, the relevant SN is registered with the BCN. In Figure 4, the sequence diagram of the registration part is given.

Algorithm 2 SN registration

```
begin
    if time_check = error; Return error();
    if $ID_{CNi}$_check = error; Return error();
    if $ID_{SNi}$_check = error; Return error();
    if $IDcard_{Cni}$_check = error; Return error();
    register($ID_{SNi}$, $ID_{Cni}$);
end
```

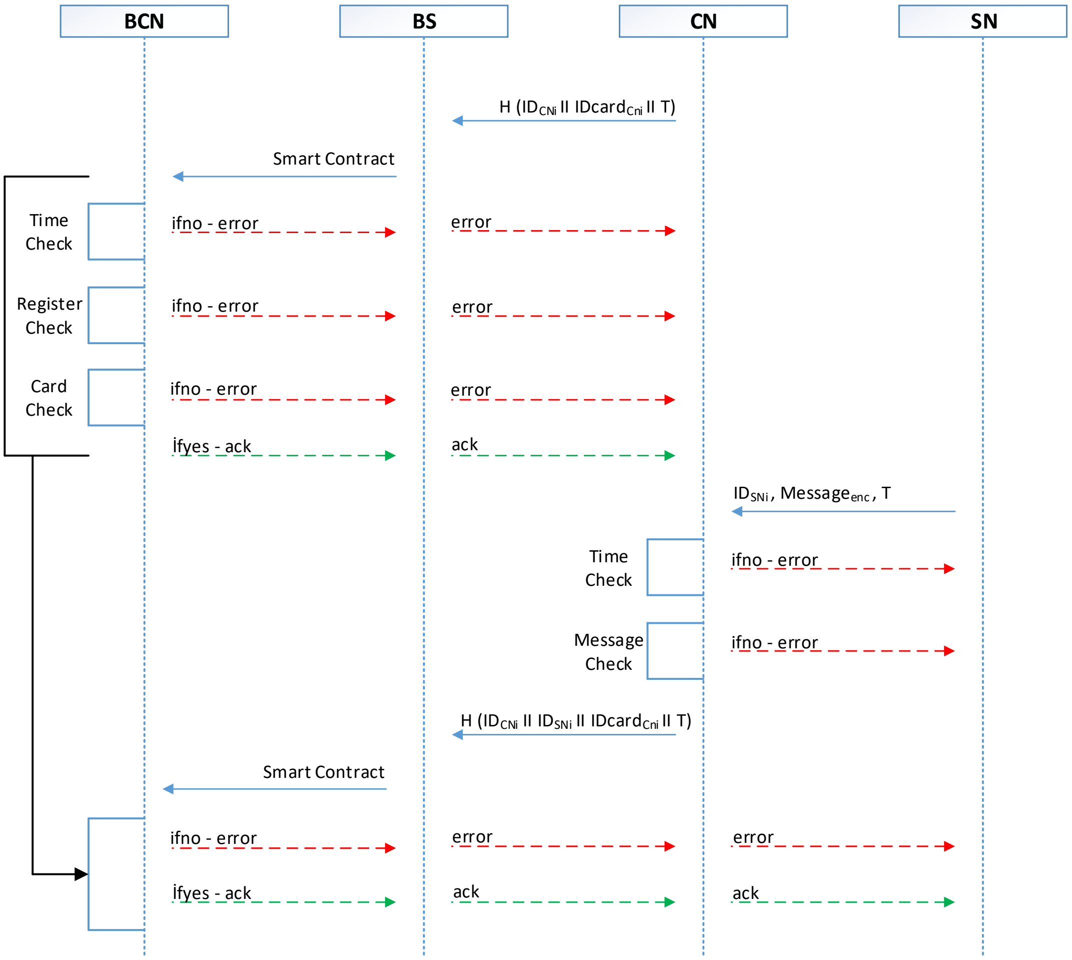

Figure 4. Sequence diagram of the registration.

5.3. Authentication

When SN number i wants to interact with the CN of which it is a member, a two-way authentication must be performed by establishing an IDSNi—IDCNi secure channel between two nodes. IDSNi sends a connection request message IDSNi, encrypted message, Time to the CN of which it is a member. The CN first checks the time information. Then, using the node's own PVKSNi, it verifies the encrypted message with PBKSNi. If there is no problem so far, the CN sends IDCNi, IDSNi, IDcardCni, and Time information to the BS and requests verification. Then, the smart contract (Algorithm 3) in the BCN is triggered. First, the Time information is checked. Then, whether the CN and SN are registered in the BCN is checked. Next, IDCNi and PBKBS are used to authenticate the IDcard. Finally, it is checked whether the IDSNi is a member of the IDCNi. If verification takes place in all of these processes, a secure communication channel is established between the relevant SN-CN and CN-BS.

Algorithm 3 CN-SN authentication

```
begin
        if time_check = error; Return error();
        if $ID_{CNi}$_check = error; Return error();
        // Is the node alive?
        // Is the node registered?
        if $ID_{SNi}$_check = error; Return error();
        // Is the node alive?
        // Is SN a member of the CN here?
        if $IDcard_{Cni}$_check = error; Return error();
            // Is the signature information correct?
return true;        // secure connection
end
```

User U can request access to the BCN with the ID given to him. The smart contract (Algorithm 4) is triggered when the request comes. If agreed in this way, U can access the BCN. A secure channel is established between U and the BCN. In Figure 5, the sequence diagram of the authentication section is given.

Algorithm 4 U authentication

```
begin
        if time_check = error; Return error();
        if $ID_U$_check = error; Return error();
        // if permission ok
        return true;
        // secure connection
end
```

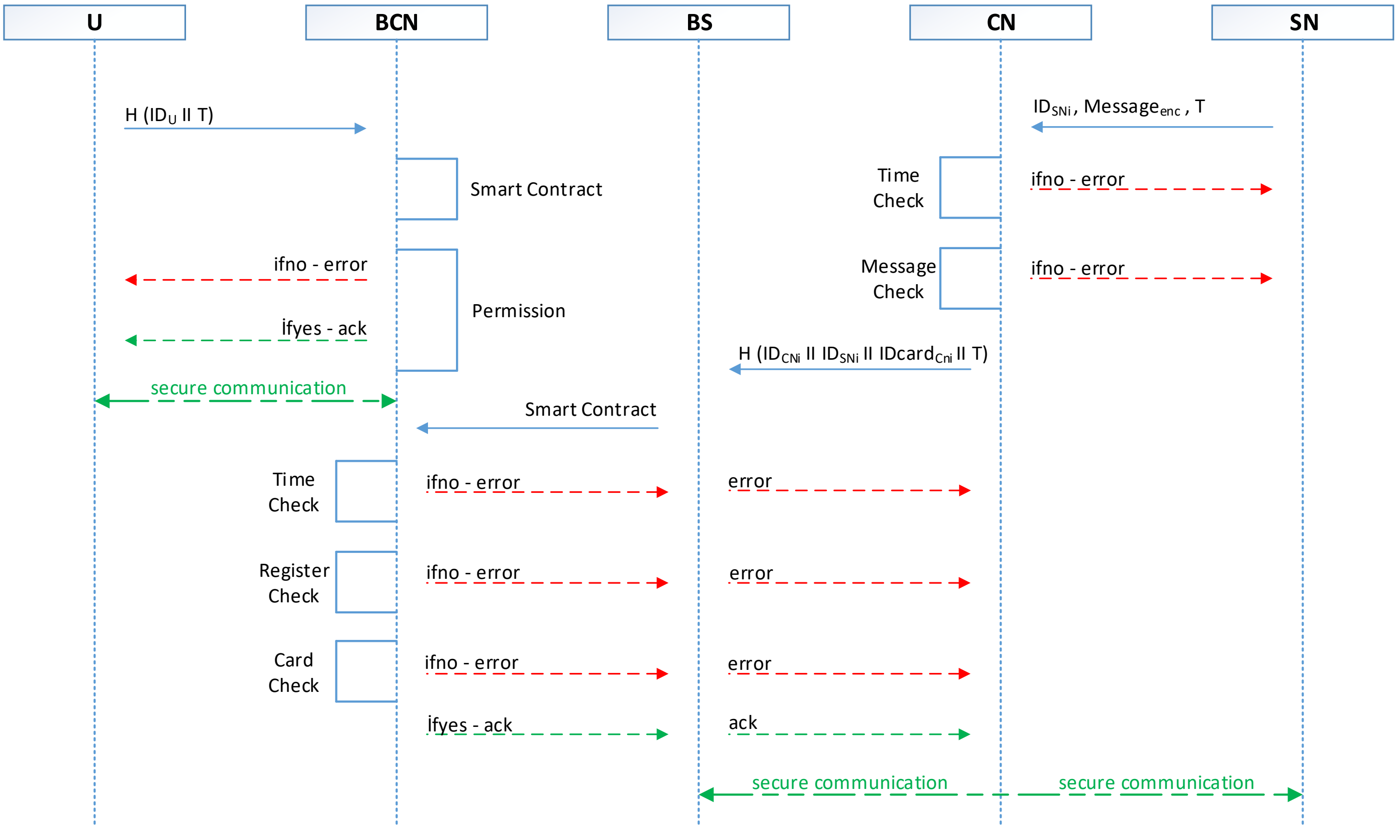

Figure 5. Sequence diagram of the authentication.

5.4. Unregistration

The SNs that are members of CNs are known by CNs. The CNs try to communicate with nodes that have not sent messages to them for a certain period of time. If the communication does not occur correctly, results such as the node's energy being exhausted, corrupted, seized, and exposed to attack can occur. In such a case, the CN applies to the BCN for cancellation of the node with the ID of the corresponding node. Then, the smart contract (Algorithm 5) is triggered and after the verification processes are completed, it performs the cancellation process.

Algorithm 5 SN unregistration

```
begin
    if time_check = error; Return error();
    if $ID_{CNi}$_check = error; Return error();
    if $ID_{SNi}$_check = error; Return error();
    if $IDcard_{Cni}$_check = error; Return error();
    delete($ID_{SNi}$);
end
```

5.5. Smart Contracts

A smart contract is basically a program. Smart contracts are simply programs stored on a blockchain that run when predetermined conditions are provided. Smart contracts follow simple "if/when ... then ... " statements written into code on a blockchain. The smart contract codes used in this study are given below.

6. Security and Efficiency Analysis

In the blockchain, public key and private key are used together and each node has a unique identity. There are features such as smart contracts, all blockchain nodes having the same data and using a consensus mechanism for addition/change, interoperability, permission participation. Therefore, with blockchain technology, Authentication, Identity Management, Authorization/Access Control, Data Integrity, Interoperability, and Privacy can be easily provided in WSNs. Detailed security analysis and efficiency analysis of the proposed protocol were carried out.

6.1. Security Analysis

Detailed security analysis of the proposed protocol is presented in Table 1.

Table 1. Security analysis.

Threat	Description	Analysis
Data Integrity	During communication, it ensures that the data sent from the source are not changed until they reach the destination.	In the proposed protocol, ECC is used for communication between SN and CN, while smart contract is used for communication between CN and BS. Communications between SN-CN cannot be changed without knowing the private keys of the nodes. Since there is a blockchain between CN-BS, data cannot be changed. Data integrity is successfully provided in the protocol. Also, data tampering, which is the act of deliberately altering (destroying, manipulating or editing) data by the attacker, cannot occur in the proposed protocol.
Scalability	It is the ability of the network to keep up with this situation without any disruption in case the number of nodes or data in the network increases or decreases.	In the proposed protocol, a new node can join the network with permission. The security level is better as there is permission participation. At the same time, a node may leave the network for any reason. This node is removed from the system. That is, the system model can be shaped according to the addition of a new node to the network or the separation of nodes. A large-size blockchain has negative effects on performance. Both the need for storage capacity and processing time are increasing. In this case, it affects scalability negatively. One of the reasons why the private blockchain model is preferred in the system and the blockchain is used only in CN-BS communications is to keep the scalability of the network at a high level. In the blockchain, as data are produced, the number of blocks increases and the chain is constantly growing. The capacity of the nodes holding these blocks should not be limited. Under normal conditions, this chain cannot be kept in SNs or CNs because there is not enough storage.

Table 1. *Cont.*

Threat	Description	Analysis
Non-Repudiation	After the data transfer from the source to the target, the source cannot deny that the data are sent and the target cannot deny that it has received the data.	In the proposed protocol, there can be no denial as communication is only through known private keys and digital signatures.
Mutual Authentication	In an authentication protocol, two parties confirm each other's identity at the same time.	The proposed protocol provides mutual authentication between SN-CN and CN-BS. Since PBK, PVK, ID, IDcard, smart contract with ECDSA are always used in the communications made by all nodes connected to the blockchain network, both the sender and the receiver are verified bilaterally. In addition, all transactions made are registered in the BCN and can be securely traced.
Sybil Attack	It is a security threat that occurs when an attacker tries to take over the network by creating multiple pseudonymous identities.	In the proposed protocol, all nodes (SN, CN) in the network are registered in the BCN. All nodes have their own unique ID, PBK, PVK, IDcard information defined and this information is also registered in the BCN. During communication, nodes are verified with smart contract using this information. At the same time, this process is safer because the private blockchain structure is used, which is permission-based. It is not possible for a node with a false identity to enter the network or impersonate nodes.
Spoofing Attack	A situation where an attacker is successfully identified as another identity by falsifying data.	As explained in the data integrity, mutual authentication, and sybil attack parts, the attacker cannot perform the relevant attack because it needs to know the private information of the nodes in the network.
Message Substitution Attack	It refers to an attacker replacing a message.	In the proposed protocol, key and signature are used in all sent messages. If the Attacker modifies a message, they must sign it with a valid private key. However, since these keys are only in their owners and they are registered in the BCN, message substitution attacks cannot succeed.
Message Replay Attack	The repetition of a valid data transmission by the attacker.	In the proposed protocol, an attacker must be authenticated before he can send a message. Only authenticated nodes can send messages on the network. On the BCN side, all blocks have a timestamp and a consensus is required for blocks to be valid. Therefore, the attacker's message is not accepted by the consensus mechanism. In this way, data freshness is ensured.
Man in the Middle Attack	It is a type of attack in which the attacker secretly transmits or changes the communication between two parties communicating directly with each other.	Since the attacker does not know the ID, PBK, PVK, IDcard information of the nodes, it will not be able to get permission from the authentication protocol to access the network or the attack process will not be terminated.
Denial of Service–Availability—Dos Attacks Resistant	It is a type of attack that aims to temporarily or indefinitely disrupt the services of the network so that a node or network resources cannot be reached by the actual users.	Since private blockchain is used in the proposed protocol, access to the network is allowed and attacking nodes do not have access to the network. Blockchain architecture is strong against DoS/DDoS attacks.

6.2. Efficiency Analysis

In order to confirm the accuracy of the proposed protocol and to perform efficiency analysis, the WiSeN sensor node [64] that we developed earlier was used. A WiSeN node (Figure 6) has a battery connection and multiple plugs. In addition, a WiSeN node is pluggable to SIM900 GSM/GPRS nodes for sending data to distinct places. In the WiSeN sensor node, MSP430G2553 and IEEE 802.15.4 [65,66] CC2530 ZigBee modules are used. Also, WiSeN has a SHT11 temperature–humidity sensor on board.

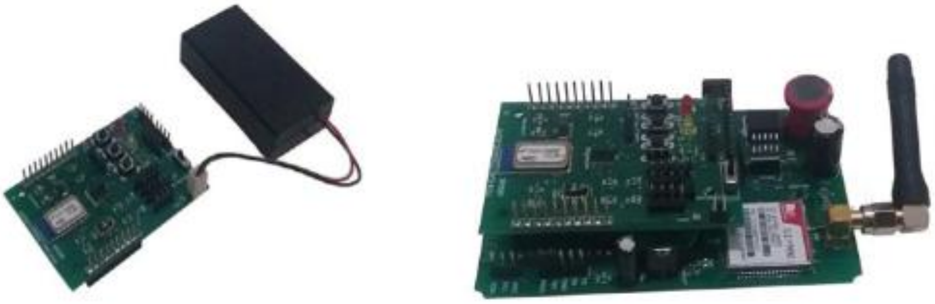

Figure 6. WiSeN sensor node.

In the realized scenario, 13 WiSeN sensor nodes were used. There are five SNs and one CN in each cluster. There are 10 SNs, 2 CNs, and 1 BS in total. The SNs released into the environment are to detect and transmit the temperature and humidity values. In the scenario, two clusters were created, each consisting of six nodes. The most suitable location among the nodes in the cluster was chosen as the CN. The WiSeN+ SIM900 GSM/GPRS node is also used as the BS. The WiSeN sensor nodes are programmed with Code Composer Studio (CCS) Integrated Development Environment (IDE), open source and provided by Texas Instruments, on a personal computer with an Intel i5 processor, 8GB RAM, and Windows operating system. The representation of the WSN used in the scenario is given in Figure 7.

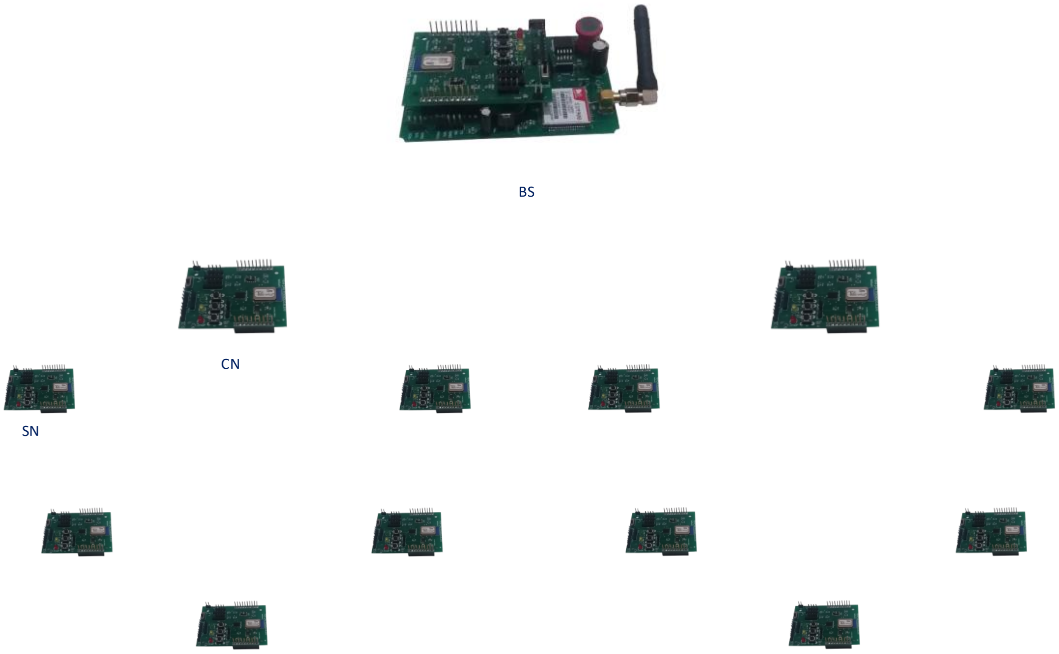

Figure 7. The WSN used in this study.

There are not enough studies in the literature on blockchain-based authentication protocol research for WSNs yet. In order to make an experimental comparison, studies [50,51] that make blockchain-based authentication in the WSN are discussed. Only the message sizes transmitted during blockchain transactions are given for energy analysis in these studies. The message sizes in the second study are the same as in the first study. At the same time, the given energy, graphs, etc., are not convincing in the second study. The references compared are not included in the reference list. No comments were made on the graphics. Therefore, only the message sizes transmitted during blockchain transactions were compared with other studies.

In addition, in the created WSN, traditionally, normal results were obtained without any additions, and then the results were obtained by implementing the recommended protocol. Then, the normal results and the obtained results were compared. Finally, the additional load of the proposed protocol to the WSN was analyzed.

The IEEE 802.15.4 protocol runs on the WiSeN sensor node, as in TelosB and MicaZ nodes. This protocol carries out network participation, message sending, and authentication. By default, this protocol is available on all nodes. The traditional situation means that the WiSeN sensor node typically works without any add-on, that is, over the 802.15.4 protocol. Blockchain-based refers to the current WiSeN sensor node, after the proposed solution is coded.

6.2.1. Latency

The following procedure is followed to obtain the latency values. After the initialization and registration processes, message sending is started. The time counter is started in the first message-sending process of the nodes and the time counter is stopped at the 100th message sending. Then, the number 100 is divided by the time difference obtained. This process is repeated 5 times, the average value is found and the latency value is obtained. The results are given in Table 2.

Table 2. Latency.

	Increase	**Normalize**
Traditional	5.16 ms	1.00
Blockchain-based	6.27 ms	1.21

Since the solutions of the proposed protocol are added to the existing 802.15.4 protocol, there will inevitably be a delay. While WiSeN nodes spend 5.16 ms for a message under normal conditions over 802.15.4 protocol, this value increases to 6.27 ms when the proposed protocol is implemented. When the results are normalized and the traditional situation is accepted as 1.00, the proposed protocol becomes 1.21.

6.2.2. Memory Usage

In the WSN, the capacities of BSs are considered unlimited, while the capacities of SNs and CNs are limited.

In the proposed protocol, ID-PVK is kept in SNs and ID-PVK-IDcard is kept in CNs. The proposed protocol has been implemented on the WiSeN node. The RAM capacity of the WiSeN node is 512 bytes, while its ROM capacity is 16 K = 16 × 1024 = 16,384 bytes. The memory usage results of the proposed protocol are given in Table 3.

Table 3. Memory usage.

	Increase	
	ROM	**RAM**
Blockchain-based	25%	6.64%

The proposed protocol uses 34 bytes of RAM and 4 K = 4 × 1024 = 4096 bytes of code memory. Therefore, the proposed protocol uses 6.64% of RAM and 25% of ROM.

6.2.3. Energy

Energy analysis is also performed to see the additional load of the proposed protocol on the WSN. A digital multimeter is used for energy measurements. An Excel Alkaline battery is used as energy in the nodes. The following procedure is followed for comparison. Before starting the nodes, the first energy measurements (first) of the nodes are made.

Then, the nodes are started and run for 1 h. After 1 h, the nodes are closed and energy measurements (last) are made again. The result of the last-first operation gives the total energy consumption in 1 h. This process is repeated 5 times and average results are obtained. As already stated in the literature [67], making measurements based on the mAH value increases the accuracy of the measurement when two batteries have an equal amount of voltage. The mAH value denotes the total amount of energy consumption in one hour. The results are given in Table 4.

Table 4. Energy.

	Energy (mAH)	**Increase**
Traditional	0.000147	-
Blockchain-based	0.000156	6.0%

While the energy consumption was 0.000147 mAH in the traditional case, this value is obtained as 0.000156 mAH when the proposed protocol is implemented. There is an increase of 6%.

6.2.4. Message Size

In other studies, it has been stated that the energy consumption of the nodes in the WSN is mainly due to the transmission of messages, and the message sizes transmitted by all the actors (SN, CN, BS) in the WSN during the registration and authentication processes are given. In the proposed protocol, message sizes are obtained during blockchain transactions and the comparison results are given in Figures 8 and 9.

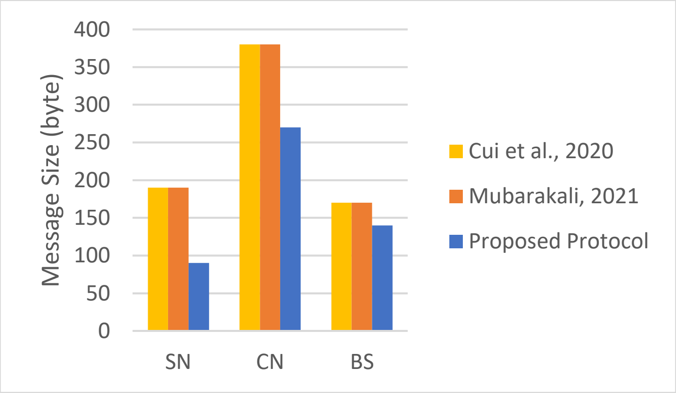

Figure 8. Comparison of message sizes in registration ([50,51]).

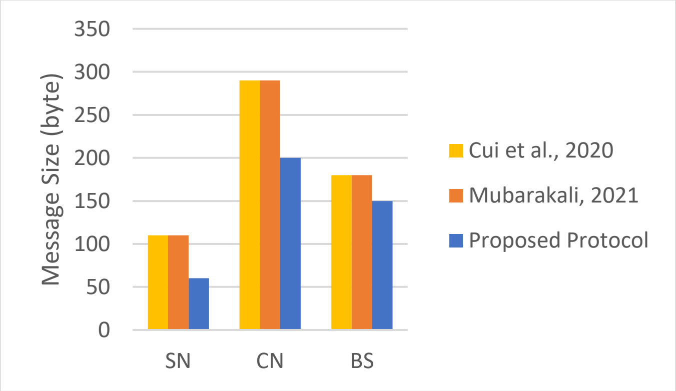

Figure 9. Comparison of message sizes in authentication ([50,51]).

The evaluations of the graphics of Figures 8 and 9 are as follows:

- In the registration process, while the message sizes in other studies are 190 bytes of SN, 380 bytes of CN, and 170 bytes of the BS, in the proposed protocol they are 90 bytes of SN, 270 bytes of CN, and 140 bytes of the BS.
- In the authentication process, while the message sizes in other studies are 110 bytes of SN, 290 bytes of CN, and 180 bytes of the BS, in the proposed protocol they are 60 bytes of SN, 200 bytes of CN, and 150 bytes of the BS.
- In the proposed protocol, IDcard is kept only in CNs. Only small-size IDs and PVKs are kept in SNs. In other studies, IDcards are kept both in SNs and CNs. This is the reason why the message size is low in the SN.
- The proposed protocol uses the ECC algorithm for transactions between SN-CN. The reason for this situation is the insufficient capacity of the nodes, as explained earlier.
- The size of the message increases because it is used in the digital signature in smart contract transactions.
- Other studies' use of blockchain at the SN-CN level is unsuitable for the WSN's structure. This situation may be the reason for the higher results obtained by other studies.
- During the registration and authentication stages, the message size of CNs is significant because they communicate with both SNs and the BS.
- In other studies, blocks are held on CNs, while in ours they are held on the BS.
- In other studies, transactions are slower because blocks are kept at the CN level. As the number of blocks increases, problems arise in terms of time and efficiency.
- The most important difference is that they use the public blockchain (permissionless) structure and we use the private blockchain (permissioned) structure.

6.3. General Evaluation

The number of studies involving blockchain-based WSNs is limited in the literature. Comparisons were made with studies [50,51], since there was no sufficient safety-efficiency analysis result in the study numbered [35]. Comparison results are given in Table 5. The meanings of the + and − signs in Table 5 are as follows: The + sign indicates that the specified criterion is met, and the − sign indicates that the specified criterion is not met.

Table 5. General analysis.

	[50]	**[51]**	**Proposed Protocol (BBAP-WSN)**
Data Integrity	+	+	+
Scalability	Low	Low	High
Non-Repudiation	+	+	+
Mutual Authentication	+	+	+
Sybil Attack	+	+	+
Spoofing Attack	+	-	+
Message Substitution Attack	+	+	+
Message Replay Attack	+	+	+
Man in the Middle Attack	+	+	+
Denial of Service	+	+	+
Implementation	−	−	+
Blockchain's type	Public + Private	Public + Private	Private
Consensus mechanism	Not specified	Not specified	PoAh
Latency	High	High	Low

Table 5. *Cont.*

	[50]	[51]	**Proposed Protocol (BBAP-WSN)**
Efficiency	Low	Low	High
Throughput	Low	Low	High
Energy Consumption	High	High	Low
Transaction Cost	High	High	Low
Transaction Speed	Slow	Slow	Fast

Blockchain requires a lot of storage capacity and transaction speed. Although it provides high security, it causes high energy consumption. Especially, scalability is a big issue. As the number of nodes increases, the naturally generated data will also increase, increasing the number of blocks. As the number of blocks increases, the transaction speeds will slow down, and the power consumption and storage space requirements will increase. Therefore, it is unthinkable for SNs and CNs with limited processing capacity, memory, and energy to keep these blocks in their memory.

Other studies have noted that block data are also kept in their CNs. Therefore, their scalability is low. In the proposed protocol, blocks are not kept in CNs. The CNs can access the BCN by communicating with the BS.

The study comes to the fore with a proposed new system model that uses only Private Blockchain in CN-BS communication and checks with ECC primarily in SN-CN communications.

The use of Public Blockchain at the BS level, while other studies use Private Blockchain at the CN level, has reduced the effectiveness of these studies.

In addition, using PoAh as a consensus mechanism further increased the effectiveness of this study.

Public blockchain can be a risk for WSNs in uncontrolled environments simultaneously. Anyone can join the network in the public blockchain. It increases the risk against a 51% attack in this case.

All participants are allowed and known in a private blockchain.

In the proposed protocol, SNs only save their IDs and PVKs, which take up very little space; CNs can only download the required node credentials from the base station for the corresponding authentication when necessary.

In addition, the implementation of the work performed is a valuable issue.

As can be seen from the results, a certain amount of energy-process-memory requirement increases according to the traditional method. However, in the traditional method, the WSN is open against all attacks, which is not the case in the proposed protocol. Therefore, the proposed protocol can be used for WSN applications that have high-security needs.

7. Conclusions

Considering the shortcomings of the authentication protocols in the WSN and the advantages of blockchain technology, there is a focus on the necessity of using this technology in the WSN. However, implementing blockchain in WSN has several challenges such as power consumption, processing time, and storage. Blockchain needs high processing power and energy while the WSN has limited capacity nodes. The size of blocks increases as transactions are made, requiring high storage space in the blockchain. However, despite all this, efforts to integrate the high-level security aspect of blockchain technology into WSN applications that require high security should be increased. In this direction, a new blockchain-based authentication protocol has been developed for WSN applications that require high security. The proposed protocol gave successful results in both security and efficiency analysis. While this study brings high security, it can also be seen that it is efficient when the latency-energy-memory usage criteria are taken into account. In future studies, the aim is to use all existing consensus algorithms, try other digital signature algorithms, implement other encryption algorithms instead of ECC and compare according to various block sizes/data size amounts. Thus, it is the aim to carry out research in order to obtain more successful results by making improvements in the authentication protocol that has already been developed efficiently.

Author Contributions: Conceptualization, M.D. and A.O.; Methodology, M.D. and A.O.; Software, M.D.; Investigation, M.D.; Writing – review & editing, M.D. and A.O.; Project administration, M.D. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data sharing not applicable.

Conflicts of Interest: No conflict of interest was declared by the authors.

Abbreviations

IoT	Internet of Things
WSN	Wireless Sensor Network
Temp	Temperature
Hum	Humidity
PoAh	Proof of Authentication
SN	Sensor Node
CN	Cluster Node
BS	Base Station
BCN	Blockchain Network
U	User
ECDSA	Elliptic Curve Digital Signature Algorithm
ECC	Elliptic Curve Cryptography
ID	Identity
MAC	Media Access Control
PBK	Public Key
PVK	Private Key
DoS	Denial-of-Service
DDoS	Distributed Denial-of-Service

References

1. Lazarescu, M.T. Design of a WSN Platform for Long-Term Environmental Monitoring for IoT Applications. *IEEE J. Emerg. Sel. Top. Circuits Syst.* **2013**, *3*, 45–54. [CrossRef]
2. Gautam, A.K.; Kumar, R. A comprehensive study on key management, authentication and trust management techniques in wireless sensor networks. *SN Appl. Sci.* **2021**, *3*, 1–27. [CrossRef]
3. Ferrag, M.A.; Maglaras, L.A.; Janicke, H.; Jiang, J.; Shu, L. Authentication Protocols for Internet of Things: A Comprehensive Survey. *Secur. Commun. Netw.* **2017**, *2017*, 6562953. [CrossRef]
4. El-hajj, M.; Fadlallah, A.; Chamoun, M.; Serhrouchni, A. A Survey of Internet of Things (IoT) Authentication Schemes. *Sensors* **2019**, *19*, 1141. [CrossRef] [PubMed]
5. Khan, M.A.; Salah, K. IoT security: Review, blockchain solutions, and open challenges. *Future Gener. Comput. Syst.* **2018**, *82*, 395–411. [CrossRef]
6. Hammi, M.T.; Hammi, B.; Bellot, P.; Serhrouchni, A. Bubbles of Trust: A decentralized blockchain-based authentication system for IoT. *Comput. Secur.* **2018**, *78*, 126–142. [CrossRef]
7. Salman, T.; Zolanvari, M.; Erbad, A.; Jain, R.; Samaka, M. Security Services Using Blockchains: A State of the Art Survey. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 858–880. [CrossRef]
8. Reyna, A.; Martín, C.; Chen, J.; Soler, E.; Díaz, M. Onblockchain and its integration with IoT. Challenges and opportunities. *Future Gener. Comput. Syst.* **2018**, *88*, 173–190. [CrossRef]
9. Kumari, S.; Khan, M.K.; Atiquzzaman, M. User authentication schemes for wireless sensor networks: A review Ad Hoc. *Networks* **2015**, *27*, 159–194. [CrossRef]

10. Patil, S.D.; Vijayakumar, B.P. A Public Key Distribution and Broadcast Authentication Scheme for Wireless Sensor Networks. *Int. J. Comput. Commun. Technol.* **2015**, *6*, 133–137. [CrossRef]
11. Darbandeh, F.G.; Safkhani, M. A New Lightweight User Authentication and Key Agreement Scheme for WSN. *Wirel. Pers. Commun.* **2020**, *114*, 3247–3269. [CrossRef]
12. Nguyen, C.V.; Nguyen, M.T.; Le, T.T.H.; Tran, T.A.; Nguyen, D.T. Blockchain Technology in Wireless Sensor Network: Benefits and Challenges. *ICSES Trans. Comput. Netw. Commun.* **2021**, 1–4.
13. Liu, C.H.; Chung, Y.F. Secure user authentication scheme for wireless healthcare sensor networks. *Comput. Electr. Eng.* **2017**, *59*, 250–261. [CrossRef]
14. Riaz, R.; Gillani, N.A.; Rizvi, S.; Shokat, S.; Kwon, S.L. SUBBASE: An Authentication Scheme for Wireless Sensor Networks Based on User Biometrics. *Wirel. Commun. Mob. Comput.* **2019**, *2019*, 6370742. [CrossRef]
15. Lu, Y.; Zhai, J.; Zhu, R.; Qin, J. Study of Wireless Authentication Center with Mixed Encryption in WSN. *J. Sens.* **2016**, *2016*, 9297562. [CrossRef]
16. Dahshan, M.H. Robust data authentication for unattended wireless sensor networks. *Telecommun. Syst.* **2017**, *66*, 181–196. [CrossRef]
17. Sen, A.; Chatterjee, T.; DasBit, S. LoWaNA: Low overhead watermark based node authentication in WSN. *Wirel. Netw.* **2016**, *22*, 2453–2467. [CrossRef]
18. Kumaran, U.S.; Ilango, P. Secure authentication and integrity techniques for randomized secured routing in WSN. *Wirel. Netw.* **2015**, *21*, 443–451. [CrossRef]
19. Zhang, X.; Wen, F. A novel anonymous user WSN authentication for Internet of Things. *Soft Comput.* **2019**, *23*, 5683–5691. [CrossRef]
20. Chinnaswamy, S.; Annapurani, K. Trust aggregation authentication protocol using machine learning for IoT wireless sensor networks. *Comput. Electr. Eng.* **2021**, *91*, 1–13. [CrossRef]
21. Arivarasi, A.; Ramesh, P. An improved source location privacy protection using adaptive trust sector-based authentication with honey encryption algorithm in WSN. *J. Ambient Intell. Humaniz. Comput.* **2021**, *13*, 9. [CrossRef]
22. Krishna, M.B.; Doja, M.N. Deterministic K-means secure coverage clustering with periodic authentication for wireless sensor networks. *Int. J. Commun. Syst.* **2017**, *30*, 1–16. [CrossRef]
23. Liao, R.F.; Wen, H.; Wu, J.; Pan, F.; Xu, A.; Jiang, Y.; Xie, F.; Cao, M. Deep-Learning-Based Physical Layer Authentication for IndustrialWireless Sensor Networks. *Sensors* **2019**, *19*, 2440. [CrossRef] [PubMed]
24. Sureshkumar, C.; Sabena, S. Fuzzy-Based Secure Authentication and Clustering Algorithm for Improving the Energy Efficiency in Wireless Sensor Networks. *Wirel. Pers. Commun.* **2020**, *112*, 1517–1536. [CrossRef]
25. Qiu, J.; Tian, Z.; Du, C.; Zuo, Q.; Su, S.; Fang, B. A Survey on Access Control in the Age of Internet of Things. *IEEE Internet Things J.* **2022**, *7*, 4682–4696. [CrossRef]
26. Bao, Z.; Shi, W.; He, D.; Choo, K.R. IoTChain: A Three-Tier Blockchain-based IoT Security Architecture. *arXiv* **2018**, arXiv:1806.02008v2.
27. Pajooh, H.H.; Rashid, M.; Alam, F.; Demidenko, S. Hyperledger Fabric Blockchain for Securing the Edge Internet of Things. *Sensors* **2021**, *21*, 359. [CrossRef]
28. Yavari, M.; Safkhani, M.; Kumari, S.; Kumar, S.; Chen, C.M. An Improved Blockchain-Based Authentication Protocol for IoT Network Management. *Secur. Commun. Netw.* **2020**, *2020*, 8836214. [CrossRef]
29. Alan, C.H.L.; Yeung, K.H.; Yan, F. Blockchain-based authentication in IoT networks. In Proceedings of the 2018 IEEE Conference on Dependable and Secure Computing (DSC), Kaohsiung, Taiwan, 10–13 December 2018; pp. 1–8.
30. Uddin, M.A.; Stranieri, A.; Gondal, I.; Balasurbramanian, V. A Lightweight Blockchain Based Framework for Underwater IoT. *Electronics* **2019**, *8*, 1552. [CrossRef]
31. Li, D.; Peng, W.; Deng, W.; Gai, F. A Blockchain-based authentication and security mechanism for IoT. In Proceedings of the 2018 27th International Conference on Computer Communication and Networks (ICCCN), Hangzhou, China, 30 July–2 August 2018; pp. 1–6.
32. Dong, S.; Yang, H.; Yuan, J.; Jiao, L.; Yu, A.; Zhang, J. Blockchain-based cross-domain authentication strategy for trusted access to mobile devices in the IoT. In Proceedings of the 2020 International Wireless Communications and Mobile Computing (IWCMC), Limassol, Cyprus, 15–19 June 2020; pp. 1–3.
33. Goyat, R.; Kumar, G.; Saha, R.; Conti, M.; Rai, M.K.; Thomas, R.; Alazab, M.; Hoon-Kim, T. Blockchain-based Data Storage with Privacy and Authentication in Internet-of-Things. *IEEE Internet Things J.* **2020**, *9*, 14203–14215. [CrossRef]
34. Yazdinejad, A.; Parizi, R.M.; Srivastava, G.; Dehghantanha, A.; Choo, K.K.R. Energy efficient decentralized authentication in internet of underwater things using blockchain. In Proceedings of the 2019 IEEE Globecom Workshops (GC Wkshps), Waikoloa, HI, USA, 9–13 December 2019; pp. 1–6.
35. Hong, S. P2P networking based internet of things (IoT) sensor node authentication by Blockchain. *Peer-Peer Netw. Appl.* **2020**, *13*, 579–589. [CrossRef]
36. Almadhoun, R.; Kadadha, M.; Alhemeiri, M.; Alshehhi, M.; Salah, K. A User Authentication Scheme of IoT Devices using Blockchain-enabled Fog Nodes. In Proceedings of the 2018 IEEE/ACS 15th International Conference on Computer Systems and Applications (AICCSA), Aqaba, Jordan, 28 October–1 November 2018; pp. 1–8.

37. Latif, S.; Idrees, Z.; Ahmad, J.; Zheng, L.; Zou, Z. Ablockchain-based architecture for secure and trustworthy operations in the industrial Internet of Things. *J. Ind. Inf. Integr.* **2021**, *21*, 1–12. [CrossRef]
38. Rathee, G.; Balasaraswathi, M.; Chandran, K.P.; Gupta, S.D.; Boopathi, C.S. A secure IoT sensors communication in industry 4.0 using blockchaintechnology. *J. Ambient Intell. Humaniz. Comput.* **2021**, *12*, 533–545. [CrossRef]
39. Lin, C.; He, D.; Huang, X.; Choo, K.K.R.; Vasilakos, A.V. BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0. *J. Netw. Comput. Appl.* **2018**, *116*, 42–52. [CrossRef]
40. Esposito, C.; Ficco, M.; Gupta, B.B. Blockchain-based authentication and authorization for smart city applications. *Inf. Process. Manag.* **2021**, *58*, 1–16. [CrossRef]
41. Lin, C.; He, D.; Kumar, N.; Huang, X.; Vijayakumar, P.; Choo, K.K.R. HomeChain: A Blockchain-Based Secure Mutual Authentication System for Smart Homes. *IEEE Internet Things J.* **2020**, *7*, 818–829. [CrossRef]
42. Ferreira, C.M.S.; Garrocho, C.T.B.; Oliveira, R.A.R.; Silva, J.S.; Cavalcanti, C.F.M. IoT Registration and Authentication in Smart City Applications with Blockchain. *Sensors* **2021**, *21*, 1323. [CrossRef]
43. Alsaedy, S.; Alraddadi, S.; Owais, A. A Review on Using Blockchain in Wireless Sensor Networks. *J. Theor. Appl. Inf. Technol.* **2020**, *98*, 3879–3887.
44. Moinet, A.; Darties, B.; Baril, J.L. Blockchain based trust & authentication for decentralized sensor networks. *arXiv* **2017**, arXiv:1706.01730v1.
45. Ren, Y.; Liu, Y.; Ji, S.; Sangaiah, A.K.; Wang, J. Incentive Mechanism of Data Storage Based on Blockchain for Wireless Sensor Networks. *Mob. Inf. Syst.* **2018**, *2018*, 6874158. [CrossRef]
46. Mateen, A.; Tanveer, J.; Khan, N.A.; Rehman, M.; Javaid, N. One step forward: Towards a blockchain based trust model for WSNs. In Proceedings of the International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, Fukuoka, Japan, 28–30 October 2020; pp. 57–69. [CrossRef]
47. Al-Mubayedh, D.; Al-Khalis, M.; Al-Azman, G.; Zagrouba, R. Security Control Based on Blockchain in the Wsn Network. *Int. J. Adv. Comput. Eng. Netw.* **2019**, *7*, 7–13.
48. Guerrero-Sanchez, A.E.; Rivas-Araiza, E.A.; Gonzalez-Cordoba, J.L. Blockchain Mechanism and Symmetric Encryption in a Wireless Sensor Network. *Sensors* **2020**, *20*, 2798. [CrossRef] [PubMed]
49. Hsiao, S.J.; Sung, W.T. UtilizingBlockchain Technology to Improve WSN Security for Sensor Data Transmission. *Comput. Mater. Contin.* **2021**, *68*, 1899–1918.
50. Cui, Z.; Xue, F.; Zhang, S.; Cai, X.; Cao, Y.; Zhang, W.; Chen, J. A Hybrid BlockChain-Based Identity Authentication Scheme for Multi-WSN. *IEEE Trans. Serv. Comput.* **2020**, *13*, 241–251. [CrossRef]
51. Mubarakali, A. An Efficient Authentication Scheme Using Blockchain Technology for Wireless Sensor Networks. *Wirel. Pers. Commun.* **2021**, *127*, 255–269. [CrossRef]
52. Awan, S.; Sajid, M.B.; Amjad, S.; Aziz, U.; Gurmani, M.U.; Javaid, N. Blockchain based authentication and trust evaluation mechanism for secure routing in wireless sensor networks. In Proceedings of the International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, Asan, Republic of Korea, 1–3 July 2021; pp. 96–107.
53. Awan, S.; Javaid, N.; Ullah, S.; Khan, A.U.; Qamar, A.M.; Choi, J.G. Blockchain Based Secure Routing and Trust Management in Wireless Sensor Networks. *Sensors* **2022**, *22*, 411. [CrossRef]
54. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 11 November 2022).
55. Peck, M.E. Blockchain world-do you need a blockchain? This chart will tell you if the technologycan solve your problem. *IEEE Spectr.* **2017**, *54*, 38–60. [CrossRef]
56. Lin, I.C.; Liao, T.C. A Survey of Blockchain Security Issues and Challenges. *Int. J. Netw. Secur.* **2017**, *19*, 653–659.
57. Wu, M.; Wang, K.; Cai, X.; Guo, S.; Guo, M.; Rong, C. A Comprehensive Survey of Blockchain: From Theory to IoT Applications and Beyond. *IEEE Internet Things J.* **2019**, *6*, 8114–8154. [CrossRef]
58. 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, Berlin, Germany, 8–11 September 2019; pp. 1–5.
59. Puthal, D.; Mohanty, S.P. Proof of authentication: IoT-friendly blockchains, Smart Consumer Electronics Systems. *IEEE Potentials* **2019**, *38*, 26–29. [CrossRef]
60. Kasyoka, P.; Kimwele, M.; Angolo, S. Multi-user broadcast authentication scheme for wireless sensor network based on elliptic curve cryptography. *Eng. Rep.* **2020**, *2*, e12176. [CrossRef]
61. Sogani, A.; Jain, A. Energy aware and fast authentication scheme using identity based encryption in wireless sensor networks. *Clust. Comput.* **2019**, *22*, 10637–10648. [CrossRef]
62. Chang, Q.; Zhang, Y.; Qin, L. A node authentication protocol based on ECC in WSN. In Proceedings of the 2010 international conference on computer design and applications, Qinhuangdao, China, 25–27 June 2010; pp. 1–4.
63. Sheng, W.F. Research of cloud platform data encryption technology based on ECC algorithm. In Proceedings of the 2018 International Conference on Virtual Reality and Intelligent Systems (ICVRIS), Zhangjiajie, China, 10–11 August 2018; pp. 125–129.
64. Dener, M. WiSeN: A new sensor node for smart applications with wireless sensor networks. *Comput. Electr. Eng.* **2017**, *64*, 380–394. [CrossRef]

65. *IEEE-TG15.4*; Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personel Area Networks (LR-WPANs). IEEE Computer Society: Los Alamitos, CA, USA, 2003; pp. 1–26.
66. Koubaa, A.; Alves, M.; Tovar, E. IEEE 802.15.4: A Federating Communication Protocol for Time-Sensitive Wireless Sensor Networks. In *Sensor Networks and Configurations: Fundamentals, Tecniques, Platforms and Experiments*; IEEE Computer Society: Los Alamitos, CA, USA, 2007; pp. 19–49.
67. Karlof, C.; Sastry, N.; Wagner, D. TinySEC: A link layer security architecture for wireless sensor networks. In Proceedings of the 2nd ACM Conference on Embedded Networked Sensor Systems SENSYS, Seoul, Republic of Korea, 4–5 November 2004; pp. 162–175.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.