EAI Endorsed Transactions
on Industrial Networks and Intelligent Systems
Research Article **EAI.EU**

A Framework of Deploying Blockchain in Wireless Sensor Networks

Hoang T. Tran[1], Cuong V. Nguyen[2], Minh T. Nguyen[3,*]

[1]Center of Electrical Engineering, Duy Tan University, Da Nang 550000, Viet Nam
[2]Department of Electronics Engineering, Thai Nguyen University of Information and Communication Technology, Thai Nguyen, 240000, Viet Nam
[3]Department of Electrical Engineering, Thai Nguyen University of Technology, Thai Nguyen, 240000, Viet Nam

Abstract

The most critical needs for wireless sensor networks (WSNs) are security, privacy, dependability, and autonomy. The networks might be vulnerable to hostile users and harmful usage if these problems are not ensured. Attacks and hazards are higher with centralized WSNs, particularly when data is shared with other businesses and sent between devices. In this paper, a WSN model with integrated blockchain security technology is proposed. Blockchains store the identity of each node. The validation is done by public blockchains and private blockchains. For sensor nodes, the authentication is implemented on the private blockchain. The public blockchain is used to authenticate cluster heads. Performing network attacks can easily be performed by unregistered nodes to access resources in the network. Broadcasting false information on the path of malicious nodes can increase packet latency and reduce packet delivery rate. In this paper, the model recommends the most secure nodes in the network to be used for secure routing. The main purpose is to reduce the attack of hackers from outside the network, improve the efficiency of detecting malicious nodes.

Received on 23 May 2022; accepted on 31 July 2022; published on 04 August 2022

Keywords: Blockchain, Blockchain in WSNs, Centralize, Distributed.

doi:10.4108/eetinis.v9i32.1125

1. INTRODUCTION

The application of wireless sensor networks is becoming more and more popular and important in people's lives. However, they still have a lot of remaining problems related to energy [1–3], communications [4, 5], data collection and processing [6, 7], and especially security issues [8, 9]. Security issues in the network play a role in determining the success or failure of the application. In the wireless sensor network model, the nodes can be deployed in many different ways, which can be random or according to a precomputed model. Regardless of how they are deployed, sensor nodes always interact with their surroundings intimately. In addition, these sensor nodes operate completely freely, meaning that they are not controlled or monitored by any monitoring centers. Therefore, they are very vulnerable to hackers. There are many ways for hackers to attack the network such as attack from outside, or attack from inside the network [10–12]. In addition, just a small mistake in the network deployment can also create an opportunity for hackers to attack the network [13, 14]. Besides, it is difficult to implement complex algorithms in sensor networks due to limitations of the network such as computational capacity and small capacity. Meanwhile, synchronizing the entire system is very difficult because different network architectures are deployed for different applications. When designing wireless sensor networks, we all have common security requirements as outlined in the paper [15–17].

Blockchain is one of the most modern security and data storage technologies available today. Blockchain is a distributed database that stores all the transactions that have been made in all participating devices in the networks [18, 19]. Blockchain keeps track of transactions and communications as blocks in an electronic ledger. Additionally, blockchain is maintained by

*Corresponding author: Assoc.Prof. Minh T. Nguyen, PhD.
Email: nguyentuanminh@tnut.edu.vn

all users of the network, and messages are broadcast to all users for authentication. Multiple messages are gathered together to form a block and added to the blockchain if they pass the authentication test. A transaction is considered successful when it is agreed upon by all network nodes participating in the network. All transactions that have been done, they will be stored in the blockchain and the information of any transaction cannot be modified. This is one of the most advantageous features of blockchain technology to ensure data security. In paper [20] presents the use of blockchain technology of Bitcoin. In paper [21, 22] the author proposes a data storage architecture for wireless sensor networks using blockchain technology. This architecture has two functions, the first is to store the data of the nodes, the second is to control the data access. In addition, in paper [23] the author proposed a reliable routing method and improved routing performance by combining the deep blockchain and Markov decision process.

Thanks to the integration of blockchain technology, the security and data storage capacity of not only mobile ad-hoc networks, flying ad-hoc networks, but also wireless sensor networks are much improved. Other sensing operations may be made more safe, autonomous, adaptable, and potentially lucrative by combining blockchain technology with other distributed systems, such as robotic swarm systems [24, 25]. In [26] the authors use a small number of nodes in the network to authenticate routing by other nodes based on the dynamic mechanism of blockchain technology in mobile ad-hoc networks [27]. In [28] the authors propose a security structure using blockchain technology for unmanned aerial vehicle (UAV) networks [29]. A large number of transactions between sensor nodes can be processed quickly, thanks to the distributed model of blockchain technology. Therefore, the cost of operating a centralized data center will be significantly reduced. Simultaneously, computing and storage needs are shared to all devices in the network. In paper [30, 31] the authors proposed a wireless sensor network structure using blockchain technology. With the integration of blockchain technology, the centralized server-client model is eliminated. Because we can interact peer-to-peer, distributing data automatically between sensor devices.

The article proposes to use blockchain technology for security in wireless sensor networks. Initially implemented the SHA-256 hash algorithm. This is one of the algorithms with complexity and high security.

The rest of this paper is organized as follows. Section 2 presents the system model. The blockchain structure is shown in Section 3. Section 4 details the hash algorithm. Section 5 outlines the structure of a sensor network based on blockchain technology. The simulation results are presented in Section 6. Section 7 provides conclusions and future work .

2. System model

The authentication processes and security mechanisms in the network are proposed in this paper. The sensor network topology consists of sensor nodes (SNs), cluster heads (CHs), base stations (BSs) and end-users as shown in Figure 1.

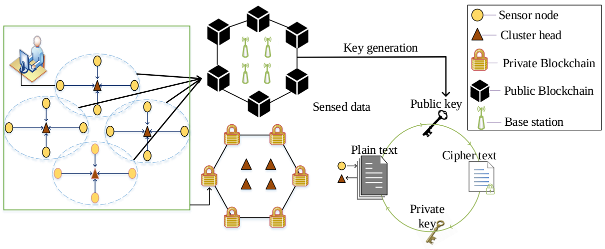


Figure 1. The proposed system model

Sensor nodes have common characteristics of computing power and storage space. Data will be sent from sensor nodes to female cluster heads, which have the higher computing power and storage space. The private blockchain is implemented on cluster heads. The public blockchain is implemented on base stations.

All nodes in the network are initialized by the base station. The registration process is fully implemented in the steps of initialization, registration, and authentication. The public keys and private keys of the base station, cluster heads, and sensor nodes are generated by the base station. These keys are generated to verify the integrity of the data. Each node has a unique address. Smart contracts are deployed on public blockchains. The cluster heads use these smart contracts to perform the registration process. Whether the clusters already exist or not is verified by these smart contracts. The MAC address of the cluster heads will be checked for correctness and validity. After successful authentication, the ID (identity) of the cluster heads will be recorded in the public blockchain. An error message is sent back if the other verification failed. Meanwhile, the registration process of sensor nodes will be done on the private blockchain. After successful registration, sensor nodes will be allowed to take part in the network. The registration process of sensor nodes and clusters heads is done in the same way. After deploying the sensor nodes will connect to their cluster heads.

There are two common forms of attack on wireless sensor networks, which are external attacks and internal attacks. Thanks to the registration and authentication of nodes, external attacks are reduced because hackers are not allowed to enter the network.

3. Blockchain Structure

The term “Blockchain” refers to a technology that includes: a growing list of data structures, called blocks, connected and secured by cryptography. Blockchain technologies allow the secure transmission of data based on an extremely complex encryption system. It is similar to a company’s ledger, where money is closely monitored and every peer-to-peer record is recorded. Each block contains information about the time of creation and is associated with the previous block, accompanied by a time code and transaction data. Once the data is accepted by the network, there is no way to change it. Blockchain is designed to combat fraud and alteration of data.

Each transaction is stored in a block, which is linked together into a chain. Each block contains the current block header, previous block address, transaction execution time, random number (nonce), and value of the current block. The data quantity and data details obtained are mainly contained in the block body. The data in the blockchain is permanently recorded and can be accessed at any time after that. Thanks to the use of digital signatures of the Merkle tree, it is guaranteed that the data obtained is never confused and duplicated. In blocks, the Mekle-root value is unique because the received data is processed by the Merkle-tree hash function. Figure 2 shows the structure of the blockchain.

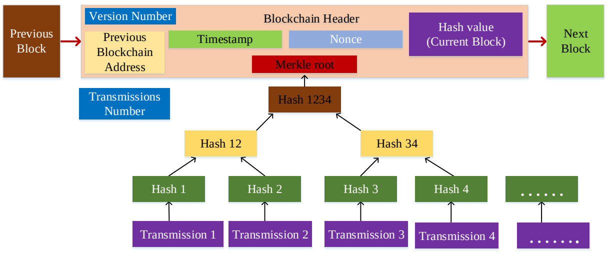


Figure 2. General structure of blockchain

3.1. Blockchain types

Currently, based on the ownership and the audience allowed to participate in the process of block verification and addition, blockchain systems have been broadly categorized into three types as shown in Figure 3.

Public blockchain: In a public blockchain, all the records are visible to the public, and everyone is allowed to take part in the consensus process. Public blockchain have the highest immutability as compared to the other two types since the number of participants is very high. However, public blockchain have lower efficiency as compared to private and consortium blockchain.

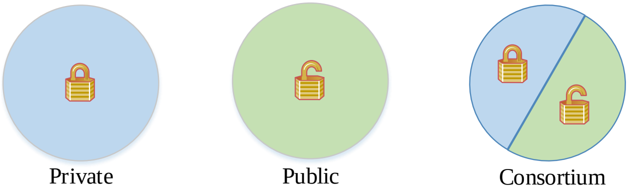


Figure 3. Types of keys in blockchain

Private blockchain: In a private blockchain, only those nodes which come from one specific organization are allowed to join the network and the consensus process, it means it has a permission consensus process. It is also regarded as a centralized network since it is fully under the control of one organization. Such networks have high efficiency but can be tampered with relatively easily as compared to public blockchain because of the lesser number of participants.

Consortium blockchain: A consortium blockchain also has a permission consensus process, but unlike a private blockchain, only a few selected organizations can participate in it. Therefore, it is a partially decentralized system. It also has high efficiency but can be tampered with relatively easily as compared to public blockchain.

3.2. Information in each block

The data structure within a block of blockchain is shown in Figure 4.

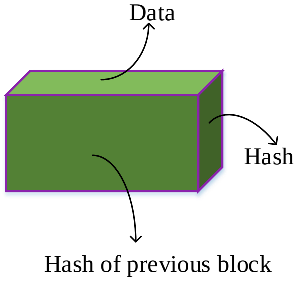


Figure 4. Types of keys in blockchain

The data in each block depends on the type of blockchain, for example, bitcoin’s blockchain contains information about transactions such as the sender, receiver information, and the number of bitcoins traded. The health insurance blockchain will store information about the insured, health history of that person.

Each block has a hash code that identifies a block and the data in it. This code is unique, it is similar to a fingerprint. Any change in the block changes the hash code.

The hash of the previous block (which is the code of the previous block) will form the chain. Any change to one block will cause the next blocks to be inconsistent.

3.3. Mechanism of action

Blockchain technology is a ledger that records and stores information on transactions. Blockchain, it can be said that this is a database organized into a chain of information blocks, allowing it to grow and expand over time, whenever new data is available, a new block is added. When each block is loaded into the ledger, it is linked to the previous block using their function hashes. This forms a completely trackable and non-tamper-proof record in the blockchain.

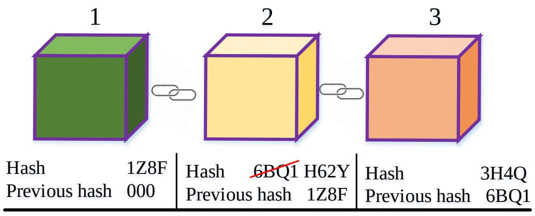


Figure 5. Blockchain's anti-change mechanism

We look at the Figure 5. The first block is the starting block, when the information on the second block is changed, the third block and the following blocks will no longer match, or in other words, the links by the matching hash code will be wrong. The second block has information changed, the hash of the block will change according to (second block changed hash from 6BQ1 to H62Y). So the link between second block and third block by hash code 6BQ1 is incompatible. With this design, blockchain helps prevent data changes. In principle, once data has been written to the blockchain, there is no way to change that data. Blockchain has used a consensus algorithm, in which there are two commonly implemented consensus algorithms: Proof of Work Algorithm (PoW) and Proof of Stake Algorithm (PoS). Proof of Work (PoW): PoW's mechanism is to slow down the process of forming new blocks. In the case of Bitcoin, for example, it takes about 10 minutes to compute the proof of work, after which a new block is added. With this PoW mechanism, tampering seems impossible, because when changing the data of one block, the tamper interferer will have to recalculate all the proof of work of the next blocks. Each block to recalculate takes at least 10 minutes, with hundreds or thousands of blocks, it will take a lot of time.

Proof of Stake (PoS): in contrast to PoW, the PoS algorithm is another way to verify transactions. With PoS, new block creators are selected at random, based on the value of their stakes. This person is responsible for validating the new blocks. To become a validator, this person has to deposit a certain amount (which is a stake, and this will be lost if this person validates a fraudulent transaction) and the validator can only deposit a certain amount of money exploit. Upon successful confirmation of a block, validators will receive a reward of the associated fees of the respective transactions in that block. If this person does not want to continue as a validator, after a certain period of time to authenticate this person does not make any fake claims, their shares and earnings will be refunded. As such, it will take time and money to perform a validation of a fake block.

4. The cryptography hash function SHA-256

In the SHA-2 family of hash functions, we have four standard lengths of 224, 256, 384 and 521 bits. That is, we have SHA-224, SHA-256, SHA-384, and SHA-512. A detailed description of the SHA-256 algorithm is presented in paper [32] , The value of the hash is calculated as follows:

$$H_0 = IV, H_{l+1} = CF(M_l, H_l) 0 \leqslant l < L \tag{1}$$

where H_l is a 256-bit string of values; $CF(M_l, H_l)$ is a compression function. $CF(M_l, H_l)$ has two parts the message expansion and the state update transformation [33].

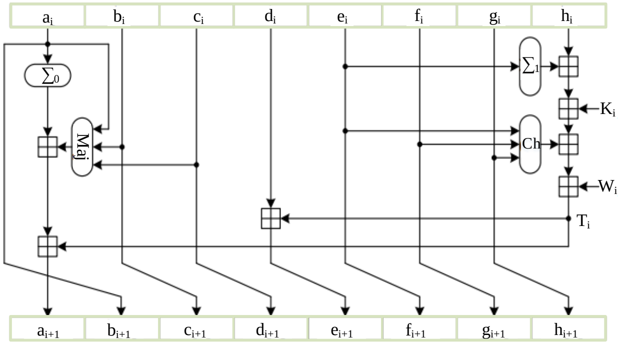


Figure 6. The implementation steps of SHA-256

$$W_i \leftarrow \begin{cases} m_i & 0 \leqslant i < 16 \\ \sigma_1(W_{i-2}) + W_{i-7} + \sigma_0(W_{i-15}) + W_{i-16} & 16 \leqslant i < 63 \end{cases} \tag{2}$$

$$\sigma_0(x) \leftarrow (x \ggg 7) \bigoplus (x \ggg 18) \bigoplus (x \gg 3), \tag{3}$$

$$\sigma_1(x) \leftarrow (x \ggg 17) \bigoplus (x \ggg 19) \bigoplus (x \gg 10), \tag{4}$$

where $\bigoplus$ is the representation for XOR, $\ggg$ is representing the left rotation, $\gg$ represents left shift. Figure 6 shows the change of steps i. The functions T_i, $Ch(x, y, z)$,$Maj(x, y, z)$, $\sum_0$ and $\sum_1$ are given by the following formula:

$$T_i = h_i + \sum_1 (e_i) + Ch(e_i, f_i, g_i) + K_i + W_i, \qquad (5)$$

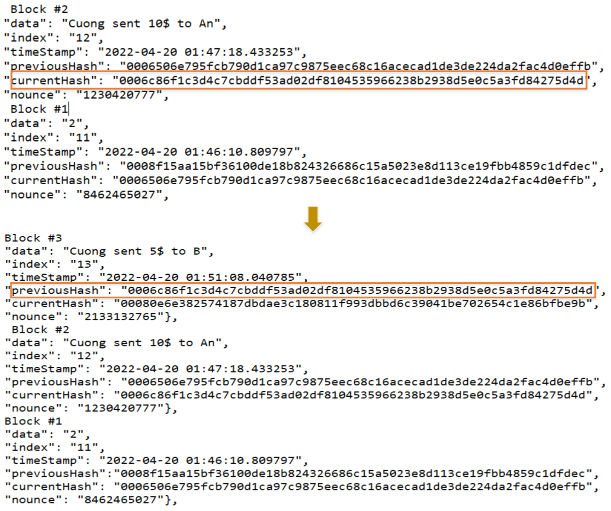
$$Ch(x, y, z) = (x \wedge y) \bigoplus (\rightarrow x \wedge z), \qquad (6)$$

$$Maj(x, y, z) = (x \wedge y) \bigoplus (y \wedge z) \bigoplus (x \wedge z), \qquad (7)$$

$$\sum_0 (x) = (x \ggg 2) \bigoplus (x \ggg 13) \bigoplus (x \ggg 22), \qquad (8)$$

$$\sum_1 (x) = (x \ggg 6) \bigoplus (x \ggg 11) \bigoplus (x \ggg 25). \qquad (9)$$

When using the SHA-256 algorithm to generate secure keys for transactions in the blockchain, we have the results as shown in Figure 7.



```
 Block #2
"data": "Cuong sent 10$ to An",
"index": "12",
"timeStamp": "2022-04-20 01:47:18.433253",
"previousHash": "0006506e795fcb790d1ca97c9875eec68c16acecad1de3de224da2fac4d0effb",
"currentHash": "0006c86f1c3d4c7cbddf53ad02df8104535966238b2938d5e0c5a3fd84275d4d",
"nounce": "1230420777",
 Block #1
"data": "2",
"index": "11",
"timeStamp": "2022-04-20 01:46:10.809797",
"previousHash": "0008f15aa15bf36100de18b824326686c15a5023e8d113ce19fbb4859c1dfdec",
"currentHash": "0006506e795fcb790d1ca97c9875eec68c16acecad1de3de224da2fac4d0effb",
"nounce": "8462465027",

Block #3
"data": "Cuong sent 5$ to B",
"index": "13",
"timeStamp": "2022-04-20 01:51:08.040785",
"previousHash": "0006c86f1c3d4c7cbddf53ad02df8104535966238b2938d5e0c5a3fd84275d4d",
"currentHash": "00080e6e382574187dbdae3c180811f993dbbd6c39041be702654c1e86bfbe9b",
"nounce": "2133132765"},
 Block #2
"data": "Cuong sent 10$ to An",
"index": "12",
"timeStamp": "2022-04-20 01:47:18.433253",
"previousHash": "0006506e795fcb790d1ca97c9875eec68c16acecad1de3de224da2fac4d0effb",
"currentHash": "0006c86f1c3d4c7cbddf53ad02df8104535966238b2938d5e0c5a3fd84275d4d",
"nounce": "1230420777"},
Block #1
"data": "2",
"index": "11",
"timeStamp": "2022-04-20 01:46:10.809797",
"previousHash":"0008f15aa15bf36100de18b824326686c15a5023e8d113ce19fbb4859c1dfdec",
"currentHash": "0006506e795fcb790d1ca97c9875eec68c16acecad1de3de224da2fac4d0effb",
"nounce": "8462465027"},
```

Figure 7. Use SHA-256 create code in transactions

In the Figure 7, we see that every time a transaction is made, the system will generate and save all the information related to the transaction. Every transaction we create fields "data", "index", "timestamp", "previoushash", "currenthash", "nounce". These fields have codes that follow the working principle of blockchain technology as outlined and analyzed above.

5. Blockchain- Based WSNs Structure

Thanks to the feature of not being able to record data, data transmission on the blockchain is highly secure. This is one of the strengths of WSNs when using this security technology. Sensor devices such as sensor 1, 2, 3, 4, 5, 6 are connected to a block in the chain as shown in Figure 8. Besides, in addition to collecting and storing data of its sensor devices , then these blocks also collect data from the sensors of other blocks. As such, all blocks hold their own sensor data and the sensor data of other blocks as well. There is no central block.

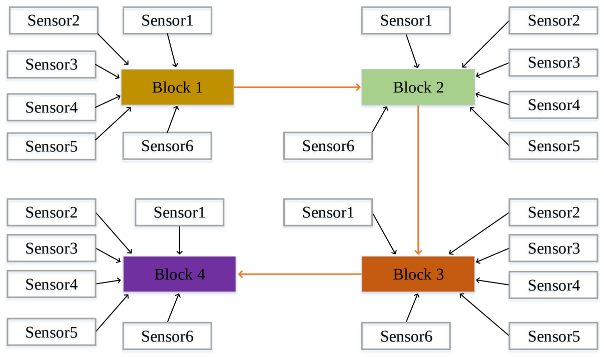


Figure 8. WSNs use blockchain technology

The blocks in the chain are linked together as shown in Figure 9. Fields like previous hash, current hash are all contained in a block. The codes generated by hash functions are very long strings of words, but for simplicity we assume the form of a code snippet consisting of numbers and letters as shown in Figure 9.

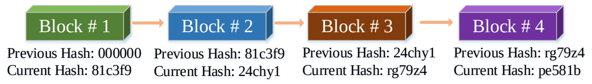


Figure 9. Nodes in WSNs are linked together in the blockchain under normal cases

Figure 10 shows a block in the chain that contains an incorrect code in the previous hash field, namely that the code has changed from "24chyl" to "23th01" in the 3rd block. When this condition occurs will result in an error link. The system will close the link and close the data transmission on that blockchain immediately. The system will then take some time to wait for the chaining connection to complete with the aim to ensure that the data in each cluster is fully uploaded.

6. Simulation Results

In this paper we use SHA-256. SHA-256 is the latest hashing algorithm of the secure hashing algorithm (SHA) family. The SHA256 algorithm will generate a 256-bit hash value for every message regardless of the message length. The generated 256-bit hash

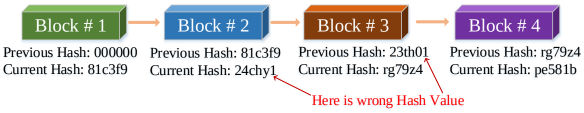
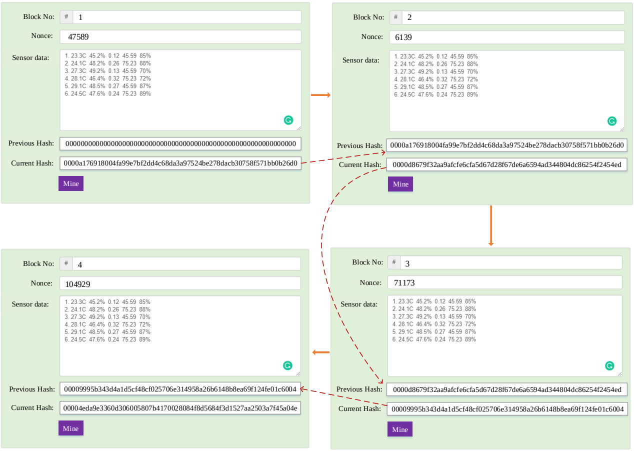


Figure 10. Nodes in the WSNs are linked together in the blockchain under abnormal cases

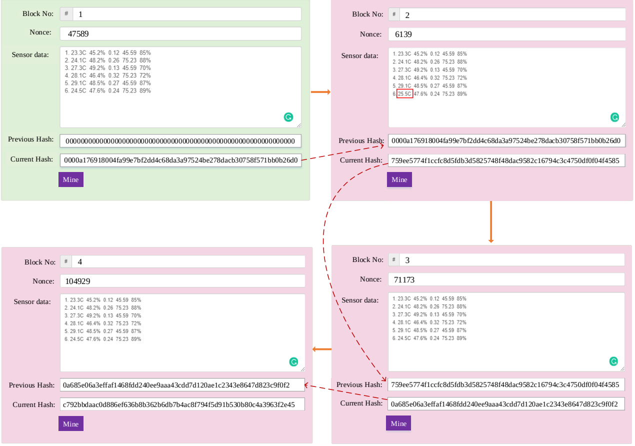
value is called a message digest. The message digest is equivalent to an array with a length of 32 bytes, usually represented by a hexadecimal string with a length of 64 characters. The SHA256 algorithm uses eight initial hash values and 64 hash constants. The implementation of blockchain in a wireless sensing network is as follows.



```
Block No: # 1
Nonce: 47589
Sensor data:
1. 23.3C  45.2%  0.12  45.59  85%
2. 24.1C  48.2%  0.26  75.23  88%
3. 27.3C  49.2%  0.13  45.59  70%
4. 28.1C  46.4%  0.32  75.23  72%
5. 29.1C  48.5%  0.27  45.59  87%
6. 24.5C  47.6%  0.24  75.23  89%
Previous Hash: 0000000000000000000000000000000000000000000000000000000000000000
Current Hash: 0000a176918004fa99e7bf2dd4c68da3a97524be278dacb30758f571bb0b26d0
Mine

Block No: # 2
Nonce: 6139
Sensor data:
1. 23.3C  45.2%  0.12  45.59  85%
2. 24.1C  48.2%  0.26  75.23  88%
3. 27.3C  49.2%  0.13  45.59  70%
4. 28.1C  46.4%  0.32  75.23  72%
5. 29.1C  48.5%  0.27  45.59  87%
6. 24.5C  47.6%  0.24  75.23  89%
Previous Hash: 0000a176918004fa99e7bf2dd4c68da3a97524be278dacb30758f571bb0b26d0
Current Hash: 0000d8679f32aa9afcfe6cfa5d67d28f67de6a6594ad344804dc86254f2454ed
Mine

Block No: # 3
Nonce: 71173
Sensor data:
1. 23.3C  45.2%  0.12  45.59  85%
2. 24.1C  48.2%  0.26  75.23  88%
3. 27.3C  49.2%  0.13  45.59  70%
4. 28.1C  46.4%  0.32  75.23  72%
5. 29.1C  48.5%  0.27  45.59  87%
6. 24.5C  47.6%  0.24  75.23  89%
Previous Hash: 0000d8679f32aa9afcfe6cfa5d67d28f67de6a6594ad344804dc86254f2454ed
Current Hash: 00009995b343d4a1d5cf48cf025706e314958a26b6148b8ea69f124fe01c6004
Mine

Block No: # 4
Nonce: 104929
Sensor data:
1. 23.3C  45.2%  0.12  45.59  85%
2. 24.1C  48.2%  0.26  75.23  88%
3. 27.3C  49.2%  0.13  45.59  70%
4. 28.1C  46.4%  0.32  75.23  72%
5. 29.1C  48.5%  0.27  45.59  87%
6. 24.5C  47.6%  0.24  75.23  89%
Previous Hash: 00009995b343d4a1d5cf48cf025706e314958a26b6148b8ea69f124fe01c6004
Current Hash: 00004eda9e3360d306005807b4170028084f8d5684f3d1527aa2503a7f45a04e
Mine
```

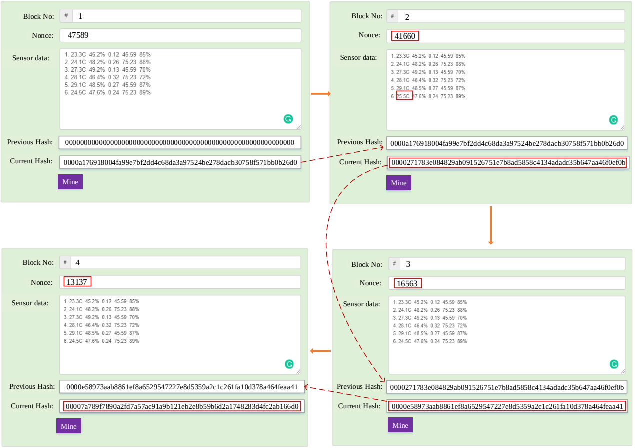
Figure 11. Result when normal

We assume 4 transactions, then each transaction will correspond to a block as shown in Figure 11. Each block in this study contains the block number, sensor data, and a hash value of the previous block, as shown in Figure 11. Also, each block is the basic unit of the blockchain. The message content of each block includes block number, nonce value, data sensor, previous hash, current hash. When the first block of chain is generated, the hash value of the previous block is set to zero as shown in Figure 11. When the operator presses the mine button, the system starts the mining process. The hash value of this block is the hash value generated by our system. When a new block is added, it stores the code in the current hash field of the previous block in the previous hash field of the following block. Therefore, the blocks in the chain will be linked together as shown in Figure 11. When a block in the chain is changed, all the blocks in the chain will not be data homogenous and give an error as shown in Figure 12. We change the data of sensor 6 from 24.5^0 C to 25.5^0 C in the 2nd block, we see all the following blocks will give an error because when reusing the data the system will save the modification and generate a different code. If we agree to this data change, we will have to update all the hashes in the blocks to get a homogenous data chain as shown in Figure 13.



```
Block No: # 1
Nonce: 47589
Sensor data:
1. 23.3C  45.2%  0.12  45.59  85%
2. 24.1C  48.2%  0.26  75.23  88%
3. 27.3C  49.2%  0.13  45.59  70%
4. 28.1C  46.4%  0.32  75.23  72%
5. 29.1C  48.5%  0.27  45.59  87%
6. 24.5C  47.6%  0.24  75.23  89%
Previous Hash: 0000000000000000000000000000000000000000000000000000000000000000
Current Hash: 0000a176918004fa99e7bf2dd4c68da3a97524be278dacb30758f571bb0b26d0
Mine

Block No: # 2
Nonce: 6139
Sensor data:
1. 23.3C  45.2%  0.12  45.59  85%
2. 24.1C  48.2%  0.26  75.23  88%
3. 27.3C  49.2%  0.13  45.59  70%
4. 28.1C  46.4%  0.32  75.23  72%
5. 29.1C  48.5%  0.27  45.59  87%
6. 25.5C  47.6%  0.24  75.23  89%
Previous Hash: 0000a176918004fa99e7bf2dd4c68da3a97524be278dacb30758f571bb0b26d0
Current Hash: 759ee5774f1ccfc8d5fdb3d5825748f48dac9582c16794c3c4750df0f04f4585
Mine

Block No: # 3
Nonce: 71173
Sensor data:
1. 23.3C  45.2%  0.12  45.59  85%
2. 24.1C  48.2%  0.26  75.23  88%
3. 27.3C  49.2%  0.13  45.59  70%
4. 28.1C  46.4%  0.32  75.23  72%
5. 29.1C  48.5%  0.27  45.59  87%
6. 24.5C  47.6%  0.24  75.23  89%
Previous Hash: 759ee5774f1ccfc8d5fdb3d5825748f48dac9582c16794c3c4750df0f04f4585
Current Hash: 0a685e06a3effaf1468fdd240ee9aaa43cdd7d120ae1c2343e8647d823c9f0f2
Mine

Block No: # 4
Nonce: 104929
Sensor data:
1. 23.3C  45.2%  0.12  45.59  85%
2. 24.1C  48.2%  0.26  75.23  88%
3. 27.3C  49.2%  0.13  45.59  70%
4. 28.1C  46.4%  0.32  75.23  72%
5. 29.1C  48.5%  0.27  45.59  87%
6. 24.5C  47.6%  0.24  75.23  89%
Previous Hash: 0a685e06a3effaf1468fdd240ee9aaa43cdd7d120ae1c2343e8647d823c9f0f2
Current Hash: c792bbdaac0d886ef636b8b362b6db7b4ac8f794f5d91b530b80c4a3963f2e45
Mine
```

Figure 12. Result when have change data



```
Block No: # 1
Nonce: 47589
Sensor data:
1. 23.3C  45.2%  0.12  45.59  85%
2. 24.1C  48.2%  0.26  75.23  88%
3. 27.3C  49.2%  0.13  45.59  70%
4. 28.1C  46.4%  0.32  75.23  72%
5. 29.1C  48.5%  0.27  45.59  87%
6. 24.5C  47.6%  0.24  75.23  89%
Previous Hash: 0000000000000000000000000000000000000000000000000000000000000000
Current Hash: 0000a176918004fa99e7bf2dd4c68da3a97524be278dacb30758f571bb0b26d0
Mine

Block No: # 2
Nonce: 41660
Sensor data:
1. 23.3C  45.2%  0.12  45.59  85%
2. 24.1C  48.2%  0.26  75.23  88%
3. 27.3C  49.2%  0.13  45.59  70%
4. 28.1C  46.4%  0.32  75.23  72%
5. 29.1C  48.5%  0.27  45.59  87%
6. 25.5C  47.6%  0.24  75.23  89%
Previous Hash: 0000a176918004fa99e7bf2dd4c68da3a97524be278dacb30758f571bb0b26d0
Current Hash: 0000271783e084829ab091526751e7b8ad5858c4134adadc35b647aa46f0ef0b
Mine

Block No: # 3
Nonce: 16563
Sensor data:
1. 23.3C  45.2%  0.12  45.59  85%
2. 24.1C  48.2%  0.26  75.23  88%
3. 27.3C  49.2%  0.13  45.59  70%
4. 28.1C  46.4%  0.32  75.23  72%
5. 29.1C  48.5%  0.27  45.59  87%
6. 24.5C  47.6%  0.24  75.23  89%
Previous Hash: 0000271783e084829ab091526751e7b8ad5858c4134adadc35b647aa46f0ef0b
Current Hash: 0000e58973aab8861ef8a6529547227e8d5359a2c1c261fa10d378a464feaa41
Mine

Block No: # 4
Nonce: 13137
Sensor data:
1. 23.3C  45.2%  0.12  45.59  85%
2. 24.1C  48.2%  0.26  75.23  88%
3. 27.3C  49.2%  0.13  45.59  70%
4. 28.1C  46.4%  0.32  75.23  72%
5. 29.1C  48.5%  0.27  45.59  87%
6. 24.5C  47.6%  0.24  75.23  89%
Previous Hash: 0000e58973aab8861ef8a6529547227e8d5359a2c1c261fa10d378a464feaa41
Current Hash: 00007a789f7890a2fd7a57ac91a9b121eb2e8b59b6d2a1748283d4fc2ab166d0
Mine
```

Figure 13. The result when we revise each block

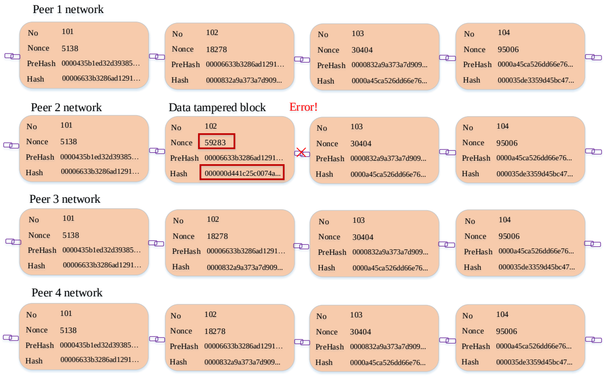

Peer 1 network
No 101
Nonce 5138
PreHash 0000435b1ed32d39385…
Hash 00006633b3286ad1291…
No 102
Nonce 18278
PreHash 00006633b3286ad1291…
Hash 0000832a9a373a7d909...
No 103
Nonce 30404
PreHash 0000832a9a373a7d909...
Hash 0000a45ca526dd66e76...
No 104
Nonce 95006
PreHash 0000a45ca526dd66e76...
Hash 000035de3359d45bc47...
Peer 2 network
Data tampered block
Error!
No 101
Nonce 5138
PreHash 0000435b1ed32d39385…
Hash 00006633b3286ad1291…
No 102
Nonce 59283
PreHash 00006633b3286ad1291…
Hash 000000d441c25c0074a...
No 103
Nonce 30404
PreHash 0000832a9a373a7d909...
Hash 0000a45ca526dd66e76...
No 104
Nonce 95006
PreHash 0000a45ca526dd66e76...
Hash 000035de3359d45bc47...
Peer 3 network
No 101
Nonce 5138
PreHash 0000435b1ed32d39385…
Hash 00006633b3286ad1291…
No 102
Nonce 18278
PreHash 00006633b3286ad1291…
Hash 0000832a9a373a7d909...
No 103
Nonce 30404
PreHash 0000832a9a373a7d909...
Hash 0000a45ca526dd66e76...
No 104
Nonce 95006
PreHash 0000a45ca526dd66e76...
Hash 000035de3359d45bc47...
Peer 4 network
No 101
Nonce 5138
PreHash 0000435b1ed32d39385…
Hash 00006633b3286ad1291…
No 102
Nonce 18278
PreHash 00006633b3286ad1291…
Hash 0000832a9a373a7d909...
No 103
Nonce 30404
PreHash 0000832a9a373a7d909...
Hash 0000a45ca526dd66e76...
No 104
Nonce 95006
PreHash 0000a45ca526dd66e76...
Hash 000035de3359d45bc47...

Figure 14. Data of the 102th block

In addition, the sensor network data is distributed across many peer devices as shown in the Figure 14. When the data is repaired, we must correct it on all devices if we want to have a consensus block in the chain. Therefore, data tampering is not possible because it takes too much time.

As shown in the Figure 14, the same blocks in different peers will store the same information. It means that data is stored in many peer devices in the network. When there is a forgery or change of data it causes inconsistency in a chain and inconsistency among peers.

7. Conclusion and future work

Integrating blockchain technology to solve the security problem of applications has many benefits. It also can prevent the risk of data tampering due to the use of a decentralized consensus mechanism. We provide the model the security system to support WSNs. In addition, scenarios are provided including simulation results to process data for security purposes. The simulation results show some promising points. The data of a sensor node can be stored in many devices in the network and has transaction time. Hence, it becomes much more difficult to change or tamper with the data.

In the design of a wireless sensor network that integrates blockchain technology, we would to pay attention to the cause of increased data transmission latency when integrating this security technology. Because the validation process is conducted over many steps. Therefore, we need to increase processing speed, reduce packet sizes, and also deploy new algorithms in the transaction confirmation process.

Acknowledgments

The authors would like to thank Thai Nguyen University of Information and communication technology, Viet Nam, Project ĐH2021-TN07-02 for the support.

References

[1] T. Q. Duong, N.-S. Vo, and C. Zhu, "Wireless communications and networks for smart cities," *Mobile Networks and Applications*, vol. 23, no. 6, pp. 1522–1524, 2018.

[2] V. T. Vu, T. V. Quyen, L. H. Truong, A. M. Le, C. V. Nguyen, and M. T. Nguyen, "Energy efficient approaches in wireless sensor networks," *ICSES Transactions on Computer Networks and Communications*, vol. 6, no. 1, pp. 1–10, 2020.

[3] H. T. Tran, M. T. Nguyen, G. Ala, F. Viola, *et al.*, "Hybrid solar-rf energy harvesting mechanisms for remote sensing devices," *International Journal of Renewable Energy Research (IJRER)*, vol. 12, no. 1, pp. 294–304, 2022.

[4] M. T. Nguyen, K. A. Teague, and N. Rahnavard, "CCS: Energy-efficient data collection in clustered wireless sensor networks utilizing block-wise compressive sensing," *Computer Networks*, vol. 106, pp. 171–185, 2016.

[5] M. Nguyen, H. Nguyen, A. Masaracchia, and C. Nguyen, "Stochastic-based power consumption analysis for data transmission in wireless sensor networks," *EAI Endorsed Transactions on Industrial Networks and Intelligent Systems*, vol. 6, no. 19, 2019.

[6] M. T. Nguyen, K. A. Teague, and S. Bui, "Compressive wireless mobile sensing for data collection in sensor networks," in *2016 International Conference on Advanced Technologies for Communications (ATC)*, pp. 437–441, 2016.

[7] C. V. Nguyen, A. E. Coboi, N. V. Bach, A. T. Dang, T. T. Le, H. P. Nguyen, and M. T. Nguyen, "Zigbee based data collection in wireless sensor networks," *Int J Inf & Commun Technol ISSN*, vol. 2252, no. 8776, p. 213.

[8] D. E. Boubiche, S. Athmani, S. Boubiche, and H. Toral-Cruz, "Cybersecurity issues in wireless sensor networks: current challenges and solutions," *Wireless Personal Communications*, vol. 117, no. 1, pp. 177–213, 2021.

[9] C. Cao, Y. Tang, D. Huang, W. Gan, and C. Zhang, "Iibe: an improved identity-based encryption algorithm for wsn security," *Security and Communication Networks*, vol. 2021, 2021.

[10] A. Becher, Z. Benenson, and M. Dornseif, "Tampering with motes: Real-world physical attacks on wireless sensor networks," in *International Conference on Security in Pervasive Computing*, pp. 104–118, Springer, 2006.

[11] D. R. Raymond and S. F. Midkiff, "Denial-of-service in wireless sensor networks: Attacks and defenses," *IEEE Pervasive Computing*, vol. 7, no. 1, pp. 74–81, 2008.

[12] J. P. Walters, Z. Liang, W. Shi, and V. Chaudhary, "Wireless sensor network security: A survey," *Security in distributed, grid, mobile, and pervasive computing*, vol. 1, no. 367, p. 6, 2007.

[13] F. Anjum and P. Mouchtaris, *Security for wireless ad hoc networks*. John Wiley & Sons, 2007.

[14] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," *Communications of the ACM*, vol. 47, no. 6, pp. 53–57, 2004.

[15] T. Zia and A. Zomaya, "Security issues in wireless sensor networks," in *2006 International Conference on Systems and Networks Communications (ICSNC'06)*, pp. 40–40, IEEE, 2006.

[16] S. Singh and H. K. Verma, "Security for wireless sensor network," *International Journal on Computer Science and Engineering*, vol. 3, no. 6, pp. 2393–2399, 2011.

[17] A. MANJUNATHA *et al.*, "Review on security in wireless sensor network," *Journal of Critical Reviews*, vol. 7, no. 11, pp. 3533–3536, 2020.

[18] T.-H. Kim, R. Goyat, M. K. Rai, G. Kumar, W. J. Buchanan, R. Saha, and R. Thomas, "A novel trust evaluation process for secure localization using a decentralized blockchain in wireless sensor networks," *IEEE Access*, vol. 7, pp. 184133–184144, 2019.

[19] F. J. Haro-Olmo, J. A. Alvarez-Bermejo, A. J. Varela-Vaca, and J. A. López-Ramos, "Blockchain-based federation of wireless sensor nodes," *J. Supercomput.*, vol. 77, p. 7879–7891, jul 2021.

[20] A. Stanciu, "Blockchain based distributed control system for edge computing," in *2017 21st International Conference on Control Systems and Computer Science (CSCS)*, pp. 667–671, IEEE, 2017.

[21] Y. Ren, Y. Liu, S. Ji, A. K. Sangaiah, and J. Wang, "Incentive mechanism of data storage based on blockchain for wireless sensor networks," *Mobile Information Systems*, vol. 2018, 2018.

[22] O. I. Khalaf and G. M. Abdulsahib, "Optimized dynamic storage of data (odsd) in iot based on blockchain for wireless sensor networks," *Peer-to-Peer Networking and Applications*, vol. 14, no. 5, pp. 2858–2873, 2021.

[23] I. A. Abd El-Moghith and S. M. Darwish, "Towards designing a trusted routing scheme in wireless sensor networks: A new deep blockchain approach," *IEEE Access*, vol. 9, pp. 103822–103834, 2021.

[24] M. T. Nguyen, H. M. La, and K. A. Teague, "Collaborative and compressed mobile sensing for data collection in distributed robotic networks," *IEEE Transactions on Control of Network Systems*, vol. 5, no. 4, pp. 1729–1740, 2018.

[25] M. T. Nguyen and H. R. Boveiri, "Energy-efficient sensing in robotic networks," *Measurement*, vol. 158, p. 107708, 2020.

[26] M. A. A. Careem and A. Dutta, "Reputation based routing in manet using blockchain," in *2020 International Conference on COMmunication Systems & NETworkS (COMSNETS)*, pp. 1–6, IEEE, 2020.

[27] M. T. Nguyen, C. V. Nguyen, H. T. Do, H. T. Hua, T. A. Tran, A. D. Nguyen, G. Ala, and F. Viola, "Uav-assisted data collection in wireless sensor networks: A comprehensive survey," *Electronics*, vol. 10, no. 21, 2021.

[28] Y. Tan, J. Liu, and N. Kato, "Blockchain-based key management for heterogeneous flying ad hoc network," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 11, pp. 7629–7638, 2020.

[29] H. T. Do, H. T. Hua, H. T. T. Nguyen, M. T. Nguyen, and H. T. Tran, "Cooperative tracking framework for multiple unmanned aerial vehicles (uavs)," in *Advances in Engineering Research and Application*, (Cham), pp. 276–285, Springer International Publishing, 2022.

[30] E. Karafiloski and A. Mishev, "Blockchain solutions for big data challenges: A literature review," in *IEEE EUROCON 2017-17th International Conference on Smart Technologies*, pp. 763–768, IEEE, 2017.

[31] S.-Y. Wang, Y.-J. Hsu, and S.-J. Hsiao, "Integrating blockchain technology for data collection and analysis in wireless sensor networks with an innovative implementation," in *2018 International Symposium on Computer, Consumer and Control (IS3C)*, pp. 149–152, IEEE, 2018.

[32] C. M. Gutierrez, P. Gallagher, and C. F. Director, "Secure hash standard," 2008.

[33] R. Hao, B. Li, B. Ma, and L. Song, "Algebraic fault attack on the sha-256 compression function," *International Journal of Research in Computer Science*, vol. 4, no. 2, pp. 1–9, 2014.