

Utilizing Blockchain Technology to Improve WSN Security for Sensor Data Transmission

Sung-Jung Hsiao¹ and Wen-Tsai Sung^{2,*}

¹Department of Information Technology, Takming University of Science and Technology, Taipei City, 11451, Taiwan

²Department of Electrical Engineering, National Chin-Yi University of Technology, Taichung, 41170, Taiwan

*Corresponding Author: Wen-Tsai Sung. Email: songchen@ncut.edu.tw

Received: 05 December 2020; Accepted: 05 February 2021

Abstract: This paper proposes a method for improving the data security of wireless sensor networks based on blockchain technology. Blockchain technology is applied to data transfer to build a highly secure wireless sensor network. In this network, the relay stations use microcontrollers and embedded devices, and the microcontrollers, such as Raspberry Pi and Arduino Yun, represents mobile databases. The proposed system uses microcontrollers to facilitate the connection of various sensor devices. By adopting blockchain encryption, the security of sensing data can be effectively improved. A blockchain is a concatenated transaction record that is protected by cryptography. Each section contains the encrypted hash of the previous section, the corresponding timestamp, and transaction data. The transaction data denote the sensing data of the wireless sensing network. The proposed system uses a hash value representation calculated by the Merkel-tree algorithm, which makes the transfer data of the system difficult to be tampered with. However, the proposed system can serve as a private cloud data center. In this study, the system visualizes the data uploaded by sensors and create relevant charts based on big data analysis. Since the webpage server of the proposed system is built on an embedded operating system, it is easy to model and visualize the corresponding graphics using Python or JavaScript programming language. Finally, this study creates an embedded system mobile database and web server, which can utilize JavaScript program language and Node.js runtime environment to apply blockchain technology to mobile databases. The proposed method is verified by the experiment using about 1600 data records. The results show that the possibility of data being changed is very small, and the probability of data being changed is almost zero.

Keywords: Blockchain; embedded system; big data analysis; python; javascript; node.js

1 Introduction

This study, which is a wide stride forward in innovation, applies blockchain technology to a wireless sensor network (WSN). The proposed solution represents an improvement of the solution



This work is licensed under a Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

presented in [1] with additional extensions. The current wireless networks are built on the Internet of Things (IoT) structure and denoted as blockchain IoT [2]. When blockchain is integrated with the Web platform technology, it is defined as a blockchain Web of Things [3,4]. The advantage of blockchain is decentralization, which means that data are not dependent on a single server. Besides, using blockchain for filing distribution minimizes risks related to data storage [5]. Many studies have shown that blockchain technology is reliable and has the potential to become the key to new IoT technologies [6,7]. This paper proposes a blockchain method based on the WSN structure. The overall system architecture adopted in this study is presented in Fig. 1. The devices on the left side in Fig. 1 are sensors for measuring different parameters, such as temperature, humidity, and brightness. The proposed system uses an embedded hardware model for data measurement and a related artificial intelligence (AI) algorithm for initial data sorting [8]. After initial data sorting, the data are saved in the database according to their type. Additionally, the system conducts data analysis and subsequently maps the data to webpage images using Python or JavaScript programming language. Then, the system awaits a user login to the cloud network to analyze and browse the graphical representation of the sensor data. Because the sensor data are accessed via Internet browsers, the proposed system is compatible with the operating systems of any mobile device. As long as a mobile device is equipped with a browser app, the user can conveniently log-in to the system and analyze the sensor data and graphical statistics [9,10].

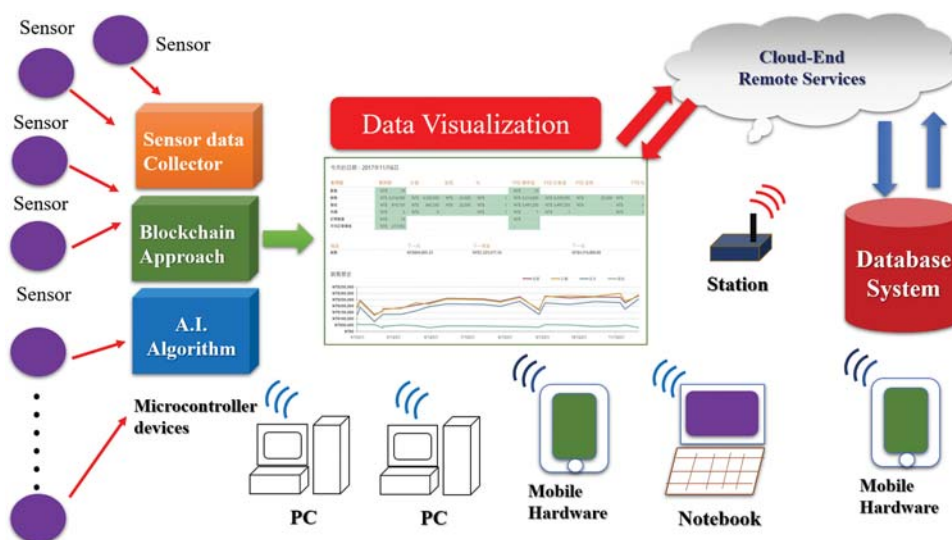


Figure 1: The proposed WSN with blockchain technology

This paper applies many of the blockchain advantages. The most important characteristic of the proposed system is that decentralized and transmitted messages are not easily modified. Due to the use of distributed accounting and storage, there is no centralized hardware or management organization, the rights and obligations of all nodes are equal, and the data blocks in the system are jointly maintained by the nodes with maintenance functions in the entire system [11,12]. When the information is verified and added to the blockchain, it is stored permanently [13–15]. Unless it can simultaneously control more than 51% of nodes in the system, the modification of the database on the single node is invalid, so the blockchain data are extremely stable and reliable. Therefore, the sensing data of the proposed system are very safe and complete [16–19].

2 Blockchain Structure

The most distinctive feature of blockchain technology is the use of a peer-to-peer (P2P) network architecture to achieve decentralization. Early blockchain technology based on P2P networking has improved the decentralized network architecture [20,21]. Much of the current research uses the familiar term “application” when referring to software programming. However, the programming application represents software used to define a specific target. Currently, millions of software applications have been in use, most of which follow the centralized server-client model. Although most network types are distributed, a few novel network architectures are decentralized [22,23]. Traditional transactions on both client and server sides rely on credible central financial institutions serving as an intermediary, and any transaction through this centralized organization is recorded and regulated. In contrast, Bitcoin uses the P2P network protocol so that transactions can be made directly between users without the need for an intermediary [24–26].

In this study, the blockchain transaction record is modified into a sensor data record and stored in data blocks. The block header encapsulates the current version number, the previous block address, timestamp, random number (nonce), target block value of the current block (bits), and the Merkle tree, such as a root value (Merkle-root). The block body mainly contains the data count and details of the obtained data. In the blockchain system, each piece of data are permanently recorded in a data block and can be queried later, similar to the information recorded in a book. The Merkle tree in a data block is digitally signed for each piece of data, thus ensuring that each piece of the obtained data are unforgettable and that no duplicate transactions are recorded. All acquired data are then processed by the Merkle-tree hash function to generate unique Merkle-root values in the block header [27,28]. The structure of the blockchain is presented in Fig. 2.

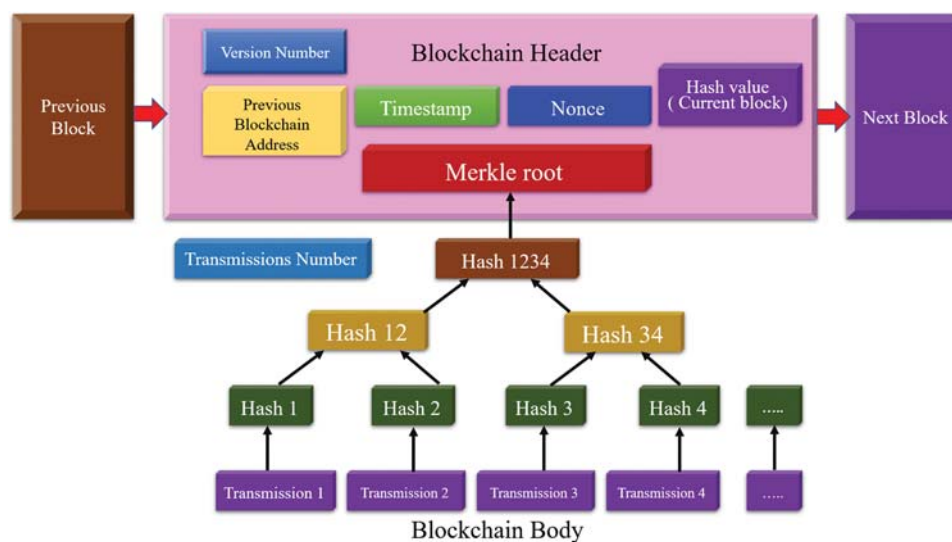


Figure 2: Blockchain structure

The timestamp and data cannot be modified, which is the most representative feature of the blockchain architecture.

3 Cryptography Technology Application to Blockchain System

The secure hash algorithms (SHAs) are a family of cryptographic hash functions and secure hash algorithms certified by the FIPS. A SHA algorithm can calculate different input data and produce a fixed-length string that is also called a message digest, which corresponds to a digital message [29,30]. Hash functions have important applications in blockchain systems. The advantages of hash functions for storing blockchain data are as follows:

- The data processed by a hash function are unidirectional, and it is almost impossible to calculate the original input values from the processed output values.
- A hash function, such as SHA256, blocks the data to be processed, with each block containing 512 bytes, and the SHA256 uses the Merkle–Damgård conversion function to input the initial vector (256 bytes) and the first block data to generate 256 bytes. Furthermore, the Merkle–Damgård conversion is performed for the initial vector and the next number, and this process is repeated until the last data block. The final result is a 256-byte hash. Therefore, the longer the input data are, the longer the hash function will be.
- If there are many different (even if only one byte is different) input values of a hash function, the output result will be considerably different. The most commonly used hash function in blockchain systems is a dual SHA256 hash function. In general, raw data of different lengths are processed using two SHA256 hash functions, and binary numbers with a length of 256 bits are output for unification [31,32]. The blockchain asymmetric encryption technology is presented in Fig. 3. In Fig. 3a typical asymmetric encryption algorithm, the elliptic curve cryptography (ECC) algorithm, is used. As shown in Fig. 3, the blockchain system generally accepts a 256-bit random number as a private key from a cryptographically secure random source under the operating system. The total number of private keys is 2^{256} , which makes hacking the key difficult [33–36].

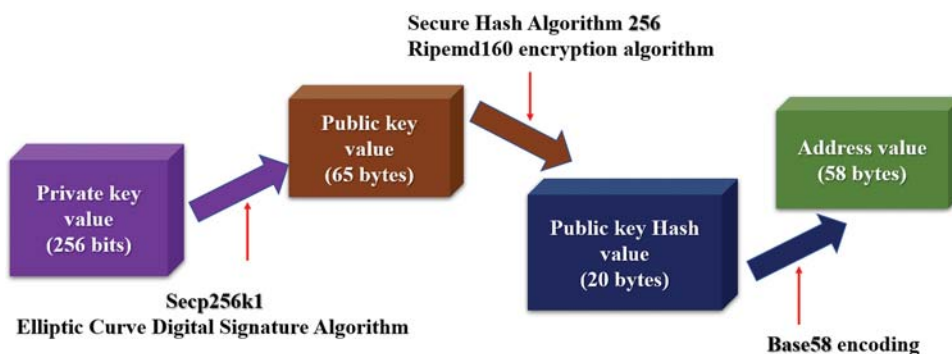


Figure 3: Blockchain asymmetric encryption technology

The electronic versions of documents and fingerprints are messages and message digests. To protect the integrity of a message, the message must be processed by a cryptographic hash function algorithm, thus creating a compressed image of the message named the message digest, which is similar to a fingerprint. The process of creating a message digest is presented in Fig. 4 [37].

Although the two pairs, i.e., document-fingerprint and message–message digest, are similar, there are certain differences between them. Documents and fingerprints are physically connected, while messages and message summaries can be separated or sent separately. The most important

thing is to protect message summaries from changes. To check the integrity of a message or file, the system executes the password hash function again. The system compares the newly generated digest with the old digest. If the two are the same, the original message has not been changed. The diagram of the file integrity checking process is presented in Fig. 5.



Figure 4: Message and message digest

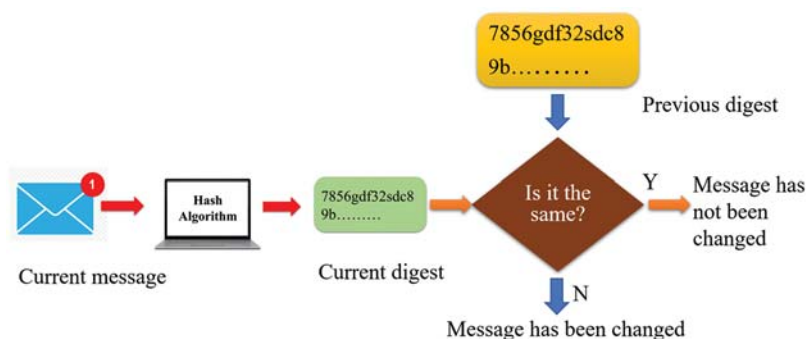


Figure 5: File integrity checking process

4 Data Fusion Algorithms

Multi-sensor data fusion refers to the fusion of data acquired by several sensors from different information sources. The system with data fusion function automatically analyzes data and performs data processing under certain criteria to achieve a better understanding of the observed phenomenon. The application of data fusion technology to water-environment monitoring and control systems to process the data provided by multiple heterogeneous sensors at multiple levels and from multiple aspects has many advantages. The water-environment detection system has many sensors, a wide distribution, and a large amount of information. In order to reduce the burden of communication lines and calculation amount in the fusion center, the system is divided into several subsystems that perform separate analyses, and then the analyses' results are integrated to obtain the fusion result of the entire system. Namely, in the proposed fusion system, a decentralized two-level fusion scheme is adopted for local fusion integrated with the global fusion, as shown in Fig. 6.

4.1 Local Fusion Algorithm

Since the number of water detection points is often small, i.e., the subsystem dimensionality is low, local fusion can be realized by using the classic vector Kalman filter algorithm. Assuming that there is a total of q water detection points, the signals from each water detection point form a q -dimensional vector $\mathbf{M}(k) = [m_1(k) m_2(k) \cdots m_q(k)]^T$. The process noise is a sequence

of independent white noise $\delta(k) = [\delta_1(k)\delta_2(k)\cdots\delta_q(k)]^T$. Then, the mathematical model of the multidimensional random signal can be expressed as:

$$\mathbf{M}(k) = \mathbf{B}\mathbf{M}(k-1) + \delta(k-1), \quad (1)$$

where $\mathbf{B} = \text{diag}(b_1b_2\cdots b_q)$ denotes the coefficient matrix.

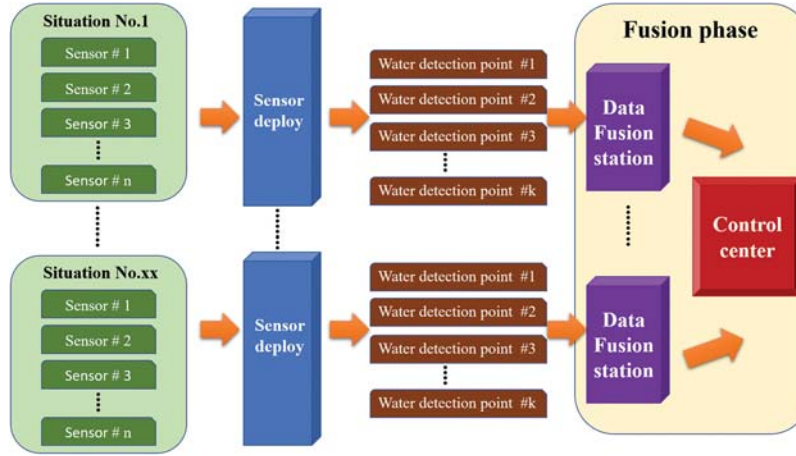


Figure 6: The structure of the fusion system

To optimally filter the q -dimensional random signal $M(k)$, the first r components of $M(k)$ ($r < q$) are measured simultaneously at time k , and an r -dimensional measurement data vector $N(k)$ can be expressed as:

$$N(k) = \mathbf{D}\mathbf{M}(k) + \mathbf{T}(k) \quad (2)$$

where $\mathbf{D} = \text{diag}(d_1d_2\cdots d_r)$ denotes the observation matrix, and $\mathbf{T}(k) = [t_1(k)t_2(k)\cdots t_r(k)]$ is an additional measurement noise sequence.

The vector Kalman filter algorithm can be expressed as follows:

$$\hat{\mathbf{m}}(Nk) = \mathbf{B}\hat{\mathbf{m}}(k-1) + \mathbf{K}(k)[\mathbf{N}(k) - \mathbf{D}\mathbf{M}\hat{\mathbf{m}}(k-1)], \quad (3)$$

$$\mathbf{K}(k) = \mathbf{P}_1(k)\mathbf{D}^T[\mathbf{D}\mathbf{P}_1(k)\mathbf{D}^T + \mathbf{R}(k)]^{-1}, \quad (4)$$

$$\mathbf{P}(k) = \mathbf{P}_1(k) - \mathbf{K}(k)\mathbf{D}\mathbf{P}_1(k), \quad (5)$$

where (3) represents the filter estimation equation, (4) represents the filter gain equation, and (5) is the filter covariance equation. In (3)–(5), $\mathbf{P}_1(k) = \mathbf{B}\mathbf{P}(k-1)\mathbf{B}^T + \mathbf{Q}(k-1)$.

The vector Kalman filter is a basic algorithm of prediction and correction as its recursive filtering. Using this algorithm, it is easy to use a computer to filter the real-time signal. The algorithm block diagrams of the main program and the subprogram of the vector Kalman filter are displayed in Figs. 7 and 8, respectively. Fig. 7 displays a state diagram of the Kalman filter with the feedback form, and Fig. 8 shows the various state calculation and conversion processes of the Kalman filter.

Assuming the output layer has a linear activation function, the output of the entire network is expressed as:

$$N = \sum_{j=1}^N \delta_{IJ}^2 m_{ni} = f(m_1, m_2, \dots, m_n). \quad (8)$$

The forward neural network training is generally conducted using the backpropagation (BP) algorithm. However, the traditional BP algorithm is essentially the least squares estimation, having poor robustness and being very sensitive to outliers, so in this work, the robust BP algorithm (RBP) is used, and it can be expressed as:

$$W_{IJ}(k+1) = W_{ij}(k) + \eta \sigma_j O_I + \alpha [W_{ij}(k) - W_{ij}(k-1)], \quad (9)$$

$$\theta_j(k+1) = \theta_j + \eta \sigma_j + \alpha [\theta_j(k) - \theta_j(k-1)], \quad (10)$$

where η denotes the learning rate, α is the inertia term constant, and $\Psi(e) = \rho'(e)$, $\rho(e)$ is the Hampel function.

The output function is denoted as O and can be expressed as:

$$O_i = f_i(\text{net}_i) = 1 + \exp\left(-\sum_j W_{ij} O_j - \theta_i\right)^{-1}, \quad (11)$$

$$\sigma_j = O_j(1 - O_j)\varphi(e) \text{ (output layer)}, \quad (12)$$

$$\sigma_j = O_j(1 - O_j) \sum_k \sigma_k W_{kj} \text{ (hidden layer)}, \quad (13)$$

where $f(m)$ represents the Sigmoid function.

5 Blockchain-Based WSN Structure

Blockchain transmits data that are not rewritable, and thus, its level of security is very high. This security is especially beneficial when applied to confidential WSNs. A WSN is built using the latest blockchain configuration [13–15]. Every main node is connected with several sensor devices, such as sensor1, sensor2, and sensor3, as presented in Fig. 9. Also, each of the main nodes has a serial number to show the order of blockchain linking. In addition to collecting its own sensor data, each blockchain collects measurement data from the nodes of the other blocks as well. That is, when a new blockchain is created for a node block, the main node also acquires the sensor data. Thus, every node keeps sensor data for its own and for other nodes, and no single node is the central node, which demonstrates the application of decentralization. All blockchain nodes are connected via a P2P network and have the safest encryption determined based on the network cryptography calculations conducted by the internet research team [16–19]. Also, each data block is controlled by an improved system program based on AI machine learning to manage the blockchain connection and overcome the shortcomings of the mining methods that were originally used by bitcoin. The connection method of blockchain nodes in a WSN is presented in Fig. 9 [20]. The node sequences labeled in Fig. 9 are connected by the asymmetrical cryptographic algorithm, which mitigates the mining time and increases the processing efficiency. The proposed blockchain node linking is shown in Fig. 10, where each node includes the hash

function of the current and previous blocks. In fact, hash functions are long strings of words, but for simplicity, they are presented as a set of four single-digit numbers in this work.

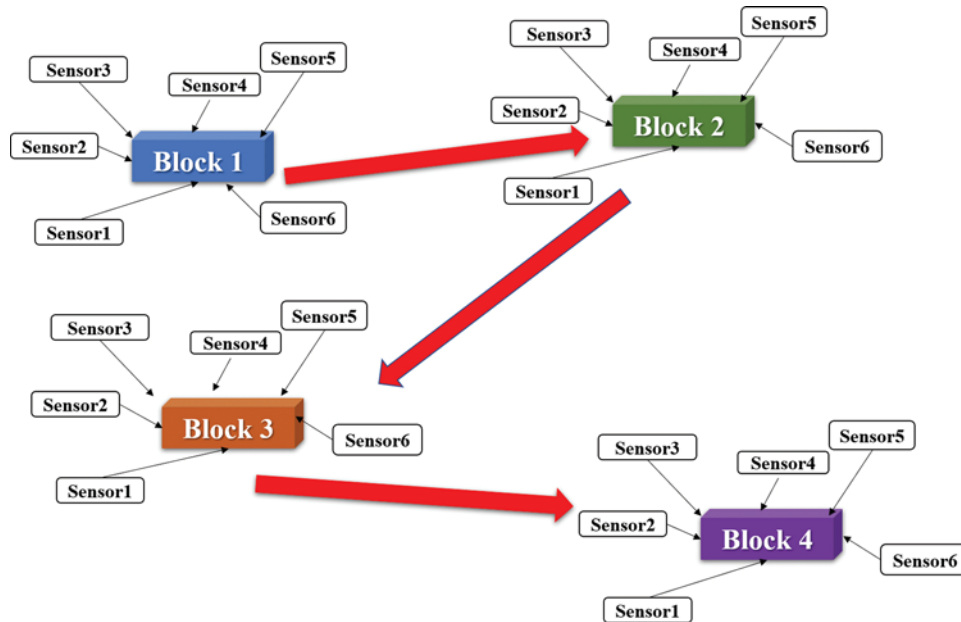


Figure 9: Integration of blockchain technology in a WSN system

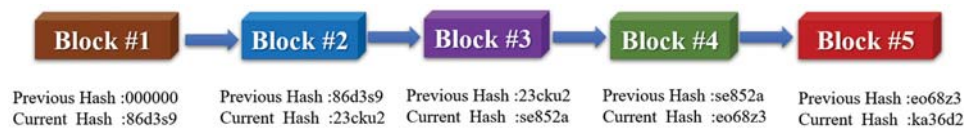


Figure 10: Normal blockchain linking of the main nodes in a WSN

The sequence of blocks with incorrect hash functions is presented in Fig. 11. In Fig. 11, the values of the nodes in the sequence are different, which signifies erroneous linking. When such erroneous linking is detected, the system immediately terminates the linking and data transmission in that blockchain. Once the blockchain linking is complete, a short waiting time is required to ensure that the WSN data in each subarea have been uploaded completely.

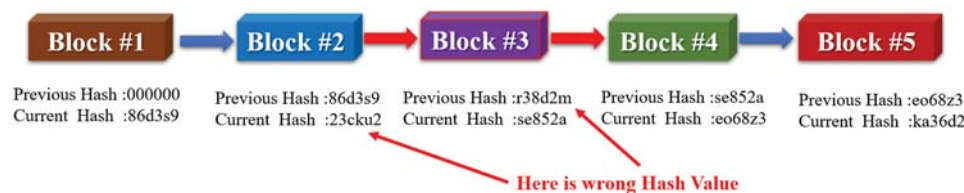


Figure 11: Abnormal blockchain linking of the main nodes in a WSN

6 Private Blockchain Implementation

The SHA256 algorithm will generate a 256-bit hash value for every messages regardless of the message length. The generated 256-bit hash 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. Among them, the initial values of the eight hashes of the SHA256 algorithm are as follows:

$h_0 := 0x6a09e667,$
 $h_1 := 0xbb67ae85,$
 $h_2 := 0x3c6ef372,$
 $h_3 := 0xa54ff53a,$
 $h_4 := 0x510e527f,$
 $h_5 := 0x9b05688c,$
 $h_6 := 0x1f83d9ab,$
 $h_7 := 0x5be0cd19.$

The initial values of hashes are derived from the decimal part of the square root of the first eight prime natural numbers, i.e., 2, 3, 5, 7, 11, 13, 17, and 19. For instance, the fractional part of $\sqrt{2}$ is approximately 0.414213562373095048 and $0.414213562373095048 \approx *16^{-1} + a * 16^{-2} + 0 * 16^{-3} + \dots$. Therefore, the decimal part of the square root of prime number two takes the first 32 bits, which corresponds to the hash value of 0x6a09e667. The 64 constants used in the SHA256 algorithm are shown in [Tab. 1](#).

Table 1: The 64 constants used in the SHA256 algorithm

27b70a85	2e1b2138	4d2c6dfc	53380d13
650a7354	766a0abb	81c2c92e	92722c85
a2bfe8a1	a81a664b	c24b8b70	c76c51a3
d192e819	d6990624	f40e3585	106aa070
19a4c116	1e376c08	2748774c	34b0bcb5
391c0cb3	4ed8aa4a	5b9cca4f	682e6ff3
748f82ee	78a5636f	84c87814	8cc70208
90befffa	a4506ceb	bef9a3f7	c67178f2
428a2f98	71374491	b5c0fbcf	e9b5dba5
3956c25b	59f111f1	923f82a4	ab1c5ed5
d807aa98	12835b01	243185be	550c7dc3
72be5d74	80deb1fe	9bdc06a7	c19bf174
e49b69c1	efbe4786	0fc19dc6	240ca1cc
2de92c6f	4a7484aa	5cb0a9dc	76f988da
983e5152	a831c66d	b00327c8	bf597fc7
c6e00bf3	d5a79147	06ca6351	14292967

Similar to the initial values of eight hashes, the constants are the first 64 prime natural numbers, and the decimal part of the cube root is taken from the first 32 bits. The implementation

of blockchain in a wireless sensing network is as follows. Each block in this study contains the block number, sensor data, timestamp, and hash value of the previous block, as shown in Fig. 12. Also, each block is the basic unit of the blockchain. The message content of each block includes:

- a. Block number,
- b. Timestamp, which represents the time when the block was generated,
- c. Measurement data of each sensor,
- d. Hash value of the previous block, and
- e. Nonce value.

Figure 12: The block interface of the proposed method

When the first block of Genesis is generated, the hash value of the previous block is set to zero. The first block implementation is completed. The proposed method calculates the block number, sensor data, timestamp, and hash value of the previous block, as listed below. The hash value has the following format: “No” + “Data” + “Timestamp” + “PreviousHashValue,” where the PreviousHashValue of the first block is 64 zeros, as shown in Fig. 13.

When the operator presses the mining button, the system starts the mining process. The hash value of this block is the hash value generated by our system, and the first four values are all ones. This nonce value is calculated using the block hash function. The condition for calculating the nonce value is that the first four characters of the block hash value are one. If the original block data are tampered with, the system will generate different nonce values, as shown in Fig. 14. The operator then mines the hash value and nonce value of the second block. The number box is filled with 2, the sensor field is filled with new data, such as the data grid, the timestamp is automatically generated by the system, and the hash value of the first block is filled. Then, the

mining button is pressed to calculate the hash value and nonce value of the second block, as shown in Fig. 15.

Blockchain Input Data

Block No : 1

Sensor measurement Data:

65.23.3C	45.2%	0.12	45.58	85%	26.1C	48.2%	0.21		
66.24.1C	48.2%	0.26	75.23	88%	25.3C	45.2%	0.31		
67.25.3C	45.2%	0.12	45.58	75%	26.1C	48.2%	0.22		
68.24.1C	48.2%	0.26	75.23	88%	25.3C	45.2%	0.33		
69.26.3C	45.2%	0.32	45.58	75%	26.1C	48.2%	0.26		
70.26.1C	48.2%	0.26	75.23	88%	25.3C	45.2%	0.32		

Current Timestamp:

2021-01-25 01:45

Previous Block Hash Value:

0000000000000000000000000000000000000000000000000000000000000000

Data Mining

Figure 13: The calculation of the hash value of a block

Blockchain Calculate Result

Block No : 1

Nonce : 17054

Sensor measurement Data:

65.23.3C	45.2%	0.12	45.58	85%	26.1C	48.2%	0.21		
66.24.1C	48.2%	0.26	75.23	88%	25.3C	45.2%	0.31		
67.25.3C	45.2%	0.12	45.58	75%	26.1C	48.2%	0.22		
68.24.1C	48.2%	0.26	75.23	88%	25.3C	45.2%	0.33		
69.26.3C	45.2%	0.32	45.58	75%	26.1C	48.2%	0.26		
70.26.1C	48.2%	0.26	75.23	88%	25.3C	45.2%	0.32		

Previous Block Hash Value:

0000000000000000000000000000000000000000000000000000000000000000

The Hash Value of this Block:

1111fa86dcb95eaa2d75cbdc56dd4ffe78f43548a913a873aec01744e4d5865f

Timestamp:

2021-01-25 01:55

Figure 14: The calculation of random nonce safety value using the mining technology

Blockchain Input Data

Block No : 2

Sensor measurement Data:

11.23.3C	45.2%	0.12	45.58	85%	26.1C	48.2%	0.21
12.24.1C	48.2%	0.26	75.23	88%	25.3C	45.2%	0.31
13.25.3C	45.2%	0.12	45.58	75%	26.1C	48.2%	0.22
14.24.1C	48.2%	0.26	75.23	88%	25.3C	45.2%	0.33
15.26.3C	45.2%	0.32	45.58	75%	26.1C	48.2%	0.26
16.26.1C	48.2%	0.26	75.23	88%	25.3C	45.2%	0.32

Current Timestamp:

2021-01-25 01:52

Previous Block Hash Value:

1111fa86db95eaa2d75cbdc56dd4ffe78f43548a913a873aec01744e4d5865f

Data Mining

Figure 15: The calculation of the second block hash value and nonce value

The hash value of block 2 is displayed in the box of the hash value of this block, and the nonce value is “59451,” as shown in [Fig. 16](#).

Blockchain Calculate Result

Block No : 2

Nonce : 59451

Sensor measurement Data:

11.23.3C	45.2%	0.12	45.58	85%	26.1C	48.2%	0.21
12.24.1C	48.2%	0.26	75.23	88%	25.3C	45.2%	0.31
13.25.3C	45.2%	0.12	45.58	75%	26.1C	48.2%	0.22
14.24.1C	48.2%	0.26	75.23	88%	25.3C	45.2%	0.33
15.26.3C	45.2%	0.32	45.58	75%	26.1C	48.2%	0.26
16.26.1C	48.2%	0.26	75.23	88%	25.3C	45.2%	0.32

Previous Block Hash Value:

1111fa86db95eaa2d75cbdc56dd4ffe78f43548a913a873aec01744e4d5865f

The Hash Value of this Block:

111118b56322174f835aa15e5e03921969e26358123f9f7c6ff330174c7c6602

Timestamp:

2021-01-25 01:58

Figure 16: The hash value and nonce value of block number 2

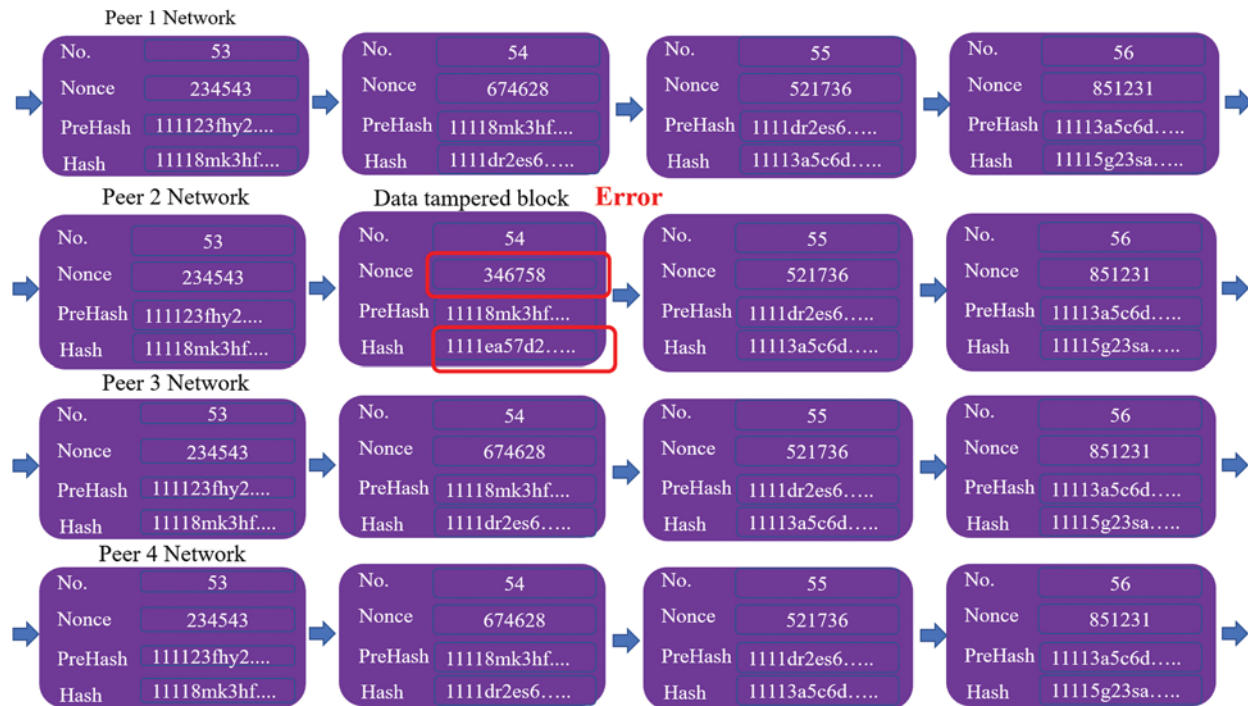


Figure 17: The 54th block data

In the experiment, a distributed network architecture was used to implement the wireless sensor network of the blockchain. The blockchain architecture proposed in this paper uses a decentralized network architecture. Assume that each block was generated every 30 min and that the proposed system had three peers when the block was generated from the first blockchain. In the peer network blockchain architecture, a block was generated every 30 min. When a block of data is tampered with, the system will immediately find the tampered place. As shown in Fig. 17, in the peer 2 Network, the nonce and hash values of the 54th block are tampered with. When the system compares the networks of peers 1, 3 and 4, it finds that the data in the 54th block of the peer 2 network are different from that in the other blocks.

7 Blockchain Pseudo-Code Description and Execution Comparison

Blockchain is the basic technology of cryptocurrency, which has gained popularity and has been successfully implemented in many fields, including virtual reality, artificial intelligence, and big data. In order to demonstrate the performance of the proposed blockchain method, it was compared with the traditional method in the WSN system. The blockchain creation pseudo-code is given in Tab. 2.

The comparison of the number of data records that can be processed every half hour between the traditional method and the proposed blockchain method is presented in Fig. 18. As shown in Fig. 18, the proposed blockchain method had a smaller number of records than the traditional method. However, it should be noted that the main objective of the proposed method is improving the security of wireless sensor networks. The comparison of the probability of data tampering between the traditional method and the proposed blockchain method is presented in Fig. 19. As shown in Fig. 19, the higher the quantity of data was, the more easily the data of the

wireless sensor network using the traditional methods could be tampered with. Generally, when the quantity of data processed by a system is high, the wireless sensing network data using the blockchain method are very difficult to tamper with and destroy.

Table 2: Blockchain creation pseudo-code

Input: The previous block hash value, the current block number, the current clock data, and timestamp
Output: Nonce value and the current block hash value
Method:
Step 1: Set the first four digits of the current block hash value to zeros (set by the system), and then mine the nonce value.
Step 2: $nonce = 0$
Step 3: **while** (the first four digits of the current block hash value are equal to zero)
{
 Step 3.1: Calculate the current block hash value
 Step 3.2: $nonce = nonce + 1$
}
Step 4: Return nonce value and the current block hash value
end

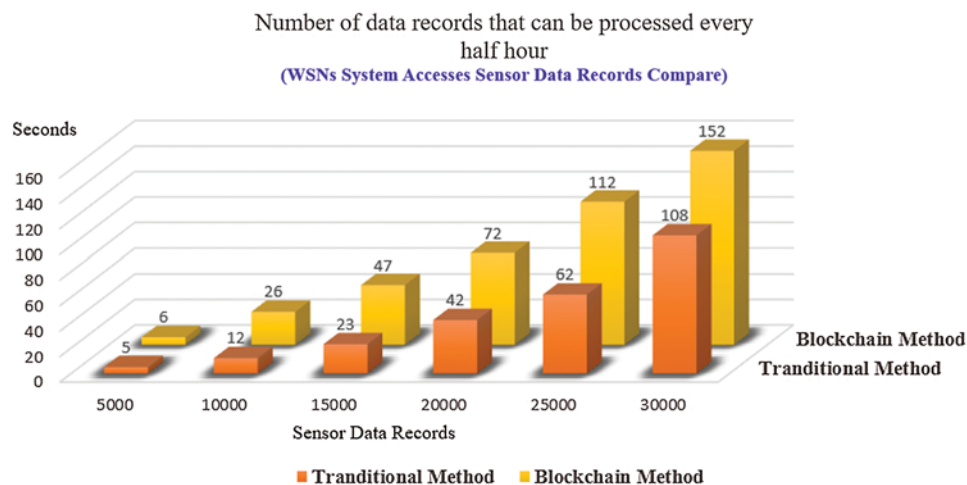


Figure 18: Comparison of the number of records between the traditional method and the proposed blockchain method

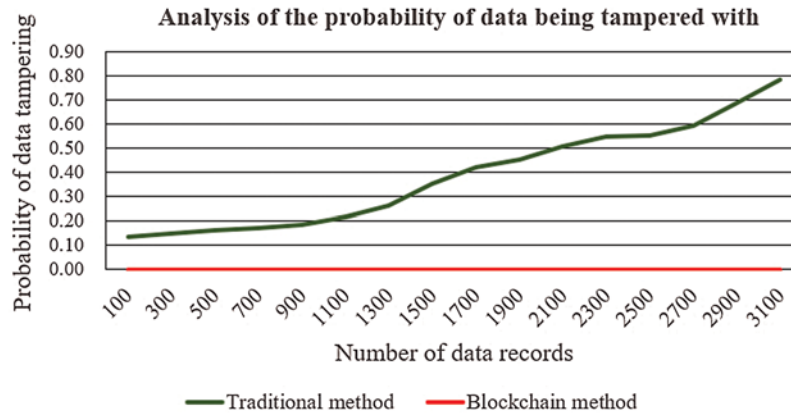


Figure 19: Comparison of the probability of data tampering between the traditional method and the proposed blockchain method

8 Results Analysis

A wireless sensing network and blockchain integration technology were used to conduct various farmland environmental sensing experiments of rice growth. The observed data included temperature and humidity in the air, the illuminance of the light, ultraviolet light, average speed of the wind, maximum speed of the wind, accumulated rainfall per hour, temperature and humidity of the soil, and power curves of the sensor battery. The microcontroller and sensor hardware are presented in Fig. 20. A total of 20 sensor nodes were placed around the rice fields. The sensor data obtained from the remote sensors are displayed in Fig. 21. The proposed system used the MySQL database system.

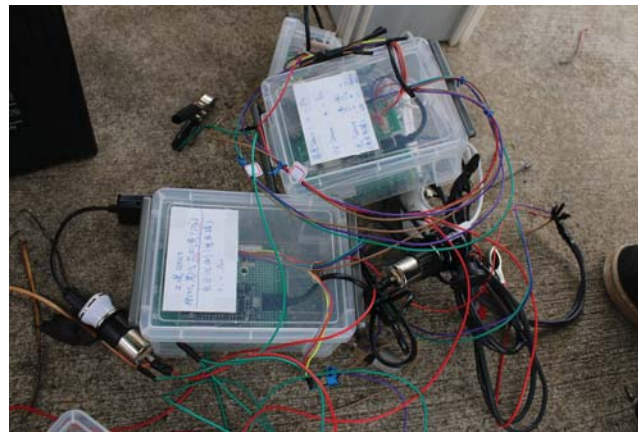
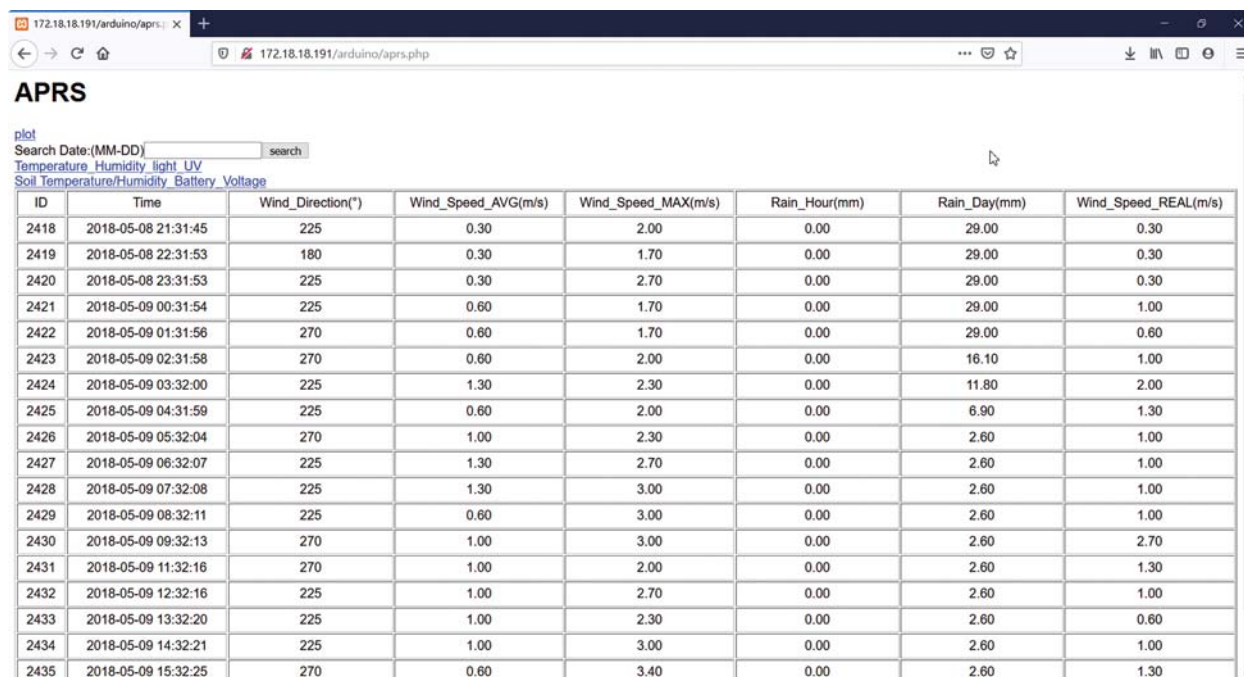


Figure 20: Actual microcontroller and sensor device

The results showed that changes in the daily temperature and humidity were relatively small, while the temperature and humidity changes in the soil were affected by water irrigation. The ultraviolet light changed with the sunrise time. The focus of the experiment was on the correct delivery of remote sensing data. These sensing data are packaged and processed from the farmland using the proposed blockchain technology. All the sensing data are correct and cannot be tampered with.



ID	Time	Wind_Direction(*)	Wind_Speed_AVG(m/s)	Wind_Speed_MAX(m/s)	Rain_Hour(mm)	Rain_Day(mm)	Wind_Speed_REAL(m/s)
2418	2018-05-08 21:31:45	225	0.30	2.00	0.00	29.00	0.30
2419	2018-05-08 22:31:53	180	0.30	1.70	0.00	29.00	0.30
2420	2018-05-08 23:31:53	225	0.30	2.70	0.00	29.00	0.30
2421	2018-05-09 00:31:54	225	0.60	1.70	0.00	29.00	1.00
2422	2018-05-09 01:31:56	270	0.60	1.70	0.00	29.00	0.60
2423	2018-05-09 02:31:58	270	0.60	2.00	0.00	16.10	1.00
2424	2018-05-09 03:32:00	225	1.30	2.30	0.00	11.80	2.00
2425	2018-05-09 04:31:59	225	0.60	2.00	0.00	6.90	1.30
2426	2018-05-09 05:32:04	270	1.00	2.30	0.00	2.60	1.00
2427	2018-05-09 06:32:07	225	1.30	2.70	0.00	2.60	1.00
2428	2018-05-09 07:32:08	225	1.30	3.00	0.00	2.60	1.00
2429	2018-05-09 08:32:11	225	0.60	3.00	0.00	2.60	1.00
2430	2018-05-09 09:32:13	270	1.00	3.00	0.00	2.60	2.70
2431	2018-05-09 11:32:16	270	1.00	2.00	0.00	2.60	1.30
2432	2018-05-09 12:32:16	225	1.00	2.70	0.00	2.60	1.00
2433	2018-05-09 13:32:20	225	1.00	2.30	0.00	2.60	0.60
2434	2018-05-09 14:32:21	225	1.00	3.00	0.00	2.60	1.00
2435	2018-05-09 15:32:25	270	0.60	3.40	0.00	2.60	1.30

Figure 21: The sensor data obtained from remote sensors

In the experiment, various environmental parameters of the experimental farm were measured. The experimental farm was the farm environment for rice cultivation. The crop measurement time was about half a year, from February to August. The measurement parameters included air temperature and humidity, soil temperature, soil moisture content, sunshine, ultraviolet light, wind speed, and other parameters.

9 Conclusion

When integrating blockchain technology into WSNs, the following problems need to be further discussed: The problem of blockchain data transmission delay and problems related to the increase in the measurement data amount.

Blockchain requires cryptography processing and public key deciphering to achieve linking. Also, creating a new blockchain requires confirmation of the link's previous and latter sequences beforehand to transmit data. Therefore, to achieve instantaneous data update and storage, some issues need to be addressed. When using blockchain technology, the hash function and encryption key calculation cannot be avoided. However, as data quantity increases, the calculation time also increases, thus reducing the data transfer efficiency. Therefore, large-scale calculations will increase data processing time. The above-mentioned shortcomings can be overcome using methods such as the resetting mechanism of blockchains, which will constantly update data transfer to the most current status. Another way to overcome the mentioned shortcomings is to use a system control mechanism and a simplified hash function calculation process. Additionally, encryption can be switched from asymmetric to symmetric for the purpose of simplification of blockchain security.

In summary, blockchain technology has several advantages. Namely, it utilizes decentralization and the common consensus mechanism to maintain a whole, distributed, and tamper-resistant ledger database with integrity. This ledger database can be considered as a measurement database

for WSNs. A block is a public record database with multi-sensors data, and a chain comprises a timestamp that cannot be counterfeited. Inherently, blockchain technology prioritizes security and reliability over efficiency. Bitcoin was released eight years ago, and since then, countless unsuccessful attempts have been made to hack the system, and there has never been a transaction error to this day. Hence, it can be concluded that the bitcoin blockchain has proven to be a reliable and robust system.

Acknowledgement: This research was supported by the Department of Electrical Engineering, National Chin-Yi University of Technology. The authors would like to thank the National Chin-Yi University of Technology, Takming University of Science and Technology, Taiwan, for supporting this research. We thank LetPub (www.letpub.com) for its linguistic assistance during the preparation of this manuscript.

Availability of Data and Materials: Data sharing not applicable to this article as no datasets were generated or analyzed during the current study.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

- [1] 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 Int. Symp. on Computer, Consumer and Control*, Taichung, Taiwan, pp. 149–152, 2018.
- [2] D. Puthal, N. Malik, S. P. Mohanty, E. Kougiannos and C. Yang, "The blockchain as a decentralized security framework [future directions]," *IEEE Consumer Electronics Magazine*, vol. 7, no. 2, pp. 18–21, 2018.
- [3] K. Fan, Y. Ren, Y. Wang, H. Li and Y. Yang, "Blockchain-based efficient privacy preserving and data sharing scheme of content-centric network in 5G," *IET Communications*, vol. 12, no. 12, pp. 527–532, 2018.
- [4] W. Yin, Q. Wen, W. Li, H. Zhang and Z. Jin, "An anti-quantum transaction authentication approach in blockchain," *IEEE Access*, vol. 6, pp. 5393–5401, 2018.
- [5] L. Thomas, C. Long, P. Burnap, J. Wu and N. Jenkins, "Automation of the supplier role in the GB power system using blockchain-based smart contracts," *CIREN Open Access Proceedings Journal*, vol. 2017, no. 1, pp. 2619–2623, 2017.
- [6] A. Anjum, M. Sporny and A. Sill, "Blockchain standards for compliance and trust," *IEEE Cloud Computing*, vol. 4, no. 4, pp. 84–90, 2017.
- [7] J. Gao, K. O. Asamoah, E. B. Sifah, A. Smahi, Q. Xia *et al.*, "Gridmonitoring: Secured sovereign blockchain based monitoring on smart grid," *IEEE Access*, vol. 6, pp. 9917–9925, 2018.
- [8] A. A. Moldovyan, N. A. Moldovyan, A. N. Berezin and P. I. Shapovalov, "Randomized pseudo-probabilistic encryption algorithms," in *2017 XX IEEE Int. Conf. on Soft Computing and Measurements*, St. Petersburg, Russia, pp. 14–17, 2017.
- [9] A. Islam, M. B. Uddin, M. F. Kader and S. Y. Shin, "Blockchain based secure data handover scheme in non-orthogonal multiple access," in *2018 4th Int. Conf. on Wireless and Telematics*, Bali, Indonesia, pp. 1–5, 2018.
- [10] J. Gu, B. Sun, X. Du, J. Wang, Y. Zhuang *et al.*, "Consortium blockchain-based malware detection in mobile devices," *IEEE Access*, vol. 6, pp. 12118–12128, 2018.

- [11] P. Fairley, "Blockchain world-feeding the blockchain beast if bitcoin ever does go mainstream, the electricity needed to sustain it will be enormous," *IEEE Spectrum*, vol. 54, no. 10, pp. 36–59, 2017.
- [12] R. Guo, H. Shi, Q. Zhao and D. Zheng, "Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems," *IEEE Access*, vol. 6, pp. 11676–11686, 2018.
- [13] Q. Lu and X. Xu, "Adaptable blockchain-based systems: A case study for product traceability," *IEEE Software*, vol. 34, no. 6, pp. 21–27, 2017.
- [14] W. Meng, E. W. Tischhauser, Q. Wang, Y. Wang and J. Han, "When intrusion detection meets blockchain technology: A review," *IEEE Access*, vol. 6, pp. 10179–10188, 2018.
- [15] Y. Zhao, Y. Li, Q. Mu, B. Yang and Y. Yu, "Secure pub-sub: Blockchain-based fair payment with reputation for reliable cyber physical systems," *IEEE Access*, vol. 6, pp. 12295–12303, 2018.
- [16] B. T. Baker, R. F. Silva, V. D. Calhoun, A. D. Sarwate and S. M. Plis, "Large scale collaboration with autonomy: Decentralized data ICA," in *2015 IEEE 25th Int. Workshop on Machine Learning for Signal Processing*, Boston, United States, pp. 1–6, 2015.
- [17] M. E. Peck, "Blockchain world-do you need a blockchain? this chart will tell you if the technology can solve your problem," *IEEE Spectrum*, vol. 54, no. 10, pp. 38–60, 2017.
- [18] A. Dorri, M. Steger, S. S. Kanhere and R. Jurdak, "Blockchain: A distributed solution to automotive security and privacy," *IEEE Communications Magazine*, vol. 55, no. 12, pp. 119–125, 2017.
- [19] J. H. Lee, "Bidaas: Blockchain based ID as a service," *IEEE Access*, vol. 6, pp. 2274–2278, 2017.
- [20] H. Jang and J. Lee, "An empirical study on modeling and prediction of bitcoin prices with bayesian neural networks based on blockchain information," *IEEE Access*, vol. 6, pp. 5427–5437, 2017.
- [21] P. K. Sharma, M. Y. Chen and J. H. Park, "A software defined fog node based distributed blockchain cloud architecture for IoT," *IEEE Access*, vol. 6, pp. 115–124, 2017.
- [22] Q. He, Y. Xu, Y. Yan, J. Wang, Q. Han *et al.*, "A consensus and incentive program for charging piles based on consortium blockchain," *CSEE Journal of Power and Energy Systems*, vol. 4, no. 4, pp. 452–458, 2018.
- [23] X. Feng, J. Ma, T. Feng, Y. Miao and X. Liu, "Consortium blockchain-based SIFT: Outsourcing encrypted feature extraction in the D2D network," *IEEE Access*, vol. 6, pp. 52248–52260, 2018.
- [24] K. Xie, W. Luo, X. Wang, D. Xie, J. Cao *et al.*, "Decentralized context sharing in vehicular delay tolerant networks with compressive sensing," in *2016 IEEE 36th Int. Conf. on Distributed Computing Systems*, Nara, Japan, pp. 169–178, 2016.
- [25] M. E. Peck and S. K. Moore, "The blossoming of the blockchain," *IEEE Spectrum*, vol. 54, no. 10, pp. 24–25, 2017.
- [26] A. Nordrum, "Govern by blockchain dubai wants one platform to rule them all, while Illinois will try anything," *IEEE Spectrum*, vol. 54, no. 10, pp. 54–55, 2017.
- [27] M. E. Peck and D. Wagman, "Energy trading for fun and profit buy your neighbor's rooftop solar power or sell your own-it'll all be on a blockchain," *IEEE Spectrum*, vol. 54, no. 10, pp. 56–61, 2017.
- [28] X. Ling, J. Wang, T. Bouchoucha, B. C. Levy and Z. Ding, "Blockchain radio access network (B-ran): Towards decentralized secure radio access paradigm," *IEEE Access*, vol. 7, pp. 9714–9723, 2019.
- [29] A. Mustafa and Hendrawan, "Calculation of encryption algorithm combination for video encryption using two layers of AHP," in *2016 10th Int. Conf. on Telecommunication Systems Services and Applications, IEEE Conf.*, Denpasar, Indonesia, pp. 1–7, 2016.
- [30] K. Kotobi and S. G. Bilen, "Secure blockchains for dynamic spectrum access: A decentralized database in moving cognitive radio networks enhances security and user access," *IEEE Vehicular Technology Magazine*, vol. 13, no. 1, pp. 32–39, 2018.
- [31] K. Kotobi and S. G. Bilén, "Blockchain-enabled spectrum access in cognitive radio networks," in *2017 Wireless Telecommunications Symp.*, Chicago, United States, pp. 1–6, 2017.
- [32] Z. Wang, Y. Tian and J. Zhu, "Data sharing and tracing scheme based on blockchain," in *2018 8th Int. Conf. on Logistics, Informatics and Service Sciences*, pp. 1–6, 2018.

- [33] X. Gou, C. Zhao, T. Yang, L. Zou, Y. Zhou *et al.*, “Single hash: Use one hash function to build faster hash based data structures,” in *2018 IEEE Int. Conf. on Big Data and Smart Computing*, pp. 278–285, 2018.
- [34] M. Kidoň and R. Dobai, “Evolutionary design of hash functions for IP address hashing using genetic programming,” in *2017 IEEE Congress on Evolutionary Computation*, pp. 1720–1727, 2017.
- [35] K. Nomura, M. Mohri, Y. Shiraishi and M. Morii, “Attribute revocable attribute-based encryption for decentralized disruption-tolerant military networks,” in *2015 Third Int. Symp. on Computing and Networking*, pp. 491–494, 2015.
- [36] F. S. Wu, “Research of cloud platform data encryption technology based on ECC algorithm,” in *2018 Int. Conf. on Virtual Reality and Intelligent Systems*, pp. 125–129, 2018.
- [37] N. Veeraragavan, L. Arockiam and S. S. Manikandasaran, “Enhanced encryption algorithm (EEA) for protecting users’ credentials in public cloud,” in *2017 Int. Conf. on Algorithms, Methodology, Models and Applications in Emerging Technologies*, pp. 1–6, 2017.