Future Generation Computer Systems 109 (2020) 95–102

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

IoT device location information storage system based on blockchain

Defeng Li [a,b], Yuan Hu [a,*], Mingming Lan [a,*]

[a] College of Mechanical and Electrical Engineering, Henan Agricultural University, Zhengzhou 450002, Henan Province, China
[b] Collaborative Innovation Center of Biomass Energy, Henan Agricultural University, Zhengzhou 450002, Henan Province, China

ARTICLE INFO

Article history:
Received 6 January 2020
Received in revised form 15 February 2020
Accepted 8 March 2020
Available online 25 March 2020

Keywords:
Blockchain
Internet of Things
Device location
Information storage

ABSTRACT

In recent years, with the development of technologies such as the Internet, sensors and RFID, the application of the Internet of Things in various industries has deepened, resulting in a large number of new technologies, new products and new applications. There are a large number of devices in the Internet of Things. The interconnection of location information of these devices brings convenience to people's lives, and there is also the problem of leaking location privacy. Therefore, effective management of the location information of the device is crucial to the development of the Internet of Things. At present, in the aspect of device location information supervision, the traditional encryption method or the location information is generally blurred, which improves the security of the location information, but also reduces the applicability of the location information. Aiming at these problems, based on the research on the equipment positioning of the Internet of Things and the key technologies of the blockchain, this paper designs a location chain storage system for IoT devices based on blockchain, and experiments the system. The results show that the number of transactions in the block has a significant impact on the time the system provides location services. The number of transactions in the block can be reasonably set by calculating the network nodes in the blockchain. The results show that the system can protect the device. Providing location information services to users under the premise of location privacy.

1. Introduction

The Internet of Things is a network based on sensing technology for real-time sharing of information [1]. With the continuous expansion of the scale, the nodes of the Internet of Things are more and more distributed. Due to the complex application environment and limited computing and storage capabilities, the security is relatively fragile [2]. With the widespread application of the Internet of Things in the strategic basic industries of industry, energy, electricity, transportation, etc., the location information security of the Internet of Things has become an urgent problem to be solved [3]. The application of blockchain technology can effectively improve the security of location information of the Internet of Things. The distributed, uncentralized structure brought by the blockchain and the way of encrypting all transmitted data will effectively solve this problem. Question [4].

In recent years, the security of the location information of IoT devices has received extensive attention from scholars at home and abroad. In 2010, Leron Lightfoot proposed a location protection strategy that states that in the entire network, a cyclically randomly selected region is first generated centered on the sink node. When the source node needs to send monitoring data to the monitor, first, a node is randomly selected as a proxy node in the randomly selected region, and data is transmitted to the proxy node. The proxy node then becomes the new source node to send information to the sink node. When an attacker detects data transmission near the sink node and performs hop-by-hop backtracking, only the proxy node can be tracked, thereby protecting the source node location privacy [5]. In 2013, Yao Lin et al. proposed a false packet scheme FPIS. The scheme sends the actual data to the sink node according to the shortest path. The intersection of the multiple shortest paths is called the intermediate node, and the intermediate node sends the fake data to the random node, so that the attacker mistakenly thinks that the node is a sink node to achieve protection. The purpose of the sink node. The disadvantage of this scheme is that the location of the intermediate node is usually close to the real sink node, and the location of the real sink node is also easily exposed after the attacker tracks the shortest path to find the intermediate node [6]. In 2013, Shao et al. proposed a source anonymity strategy. In this strategy, a node generates a fake data packet according to the statistical rules of the actual event, and adds the actual data packet to the fake data stream, so that the attacker cannot distinguish between the real data packet and the fake data packet. The source anonymous policy reduces network power consumption, but does not solve the problem of data conflict [7]. In order to

* Corresponding authors.
E-mail addresses: defeng.li@henau.edu.cn (D. Li), huyuan@henau.edu.cn (Y. Hu), lanming@henau.edu.cn (M. Lan).

https://doi.org/10.1016/j.future.2020.03.025
0167-739X/

solve the positioning security problem based on ranging method, Shu et al. proposed a location information protection method based on least squares estimation in 2014. In this method, each reference node does not directly expose its specific location, but is a small part of the calculation, and the user estimates the current location by calculating the result of the summarized reference node. This method actually blurs the location information, and the user cannot infer the specific location of the reference node through the intermediate calculation data. Therefore, the method can simultaneously protect the location data security of the user and the reference node, but also reduces the applicability [8]. In 2014, in the face of location information security in location services, Shao et al. adopted a double encryption technology to encrypt the user's location and points of interest on the client and server, and the service provider verified the encryption location information. The user's real location data is not available regardless of whether it matches. Encryption of the location information solves the security of the location information to a certain extent, and the location information obtained by the method cannot be directly used for daily services [9]. In 2015, Chen et al. combined the false packet policy with the random routing strategy and proposed the DBT protocol and the ZBT protocol. The DBT and ZBT protocols can protect the location privacy of the source and sink nodes at the same time, but generating too many fake branches will result in greater energy consumption [10]. In 2016, Chen Juan et al. pointed out that the phantom nodes may focus on a certain area in PRLA, and proposed a source location privacy protection strategy based on source node limited flooding and an enhanced source location protection strategy to keep each packet away from each other. The source node, but the phantom nodes generated by this strategy are still concentrated in a small range, and there is still much room for improvement [11]. In 2017, Bai Leqiang et al. proposed a node location privacy protection strategy based on ellipse model, which improved the location privacy intensity of the node to some extent, but the network delay increases linearly with the distance between the source node and the sink [12].

Through the review of historical documents and the analysis of existing research, it is found that there are many research methods on the security of equipment location information of Internet of Things. These studies have achieved certain results, and some research results have been applied in practice, but the following still exist. Problem: (1) The traditional encryption method is generally double or even multiple encryption. Although the security is improved, it cannot be directly applied to daily services. (2) The fuzzy calculation method is adopted, that is, the location information of the device is blurred. It improves the security and reduces the applicability; (3) Due to the limitation of encryption technology, location information cannot be shared under the premise of ensuring information security.

A blockchain is a distributed data storage mechanism. It is a string of data blocks linked by cryptography. Each block of data records a batch of information about network transactions at the time [13]. At present, blockchain technology has a wide range of application scenarios in many fields. In the field of supply chain finance, traditional supply chain financial platforms are generally dominated by a single financial institution, making it difficult to achieve expansion and promotion among peers. Blockchain technology allows participants to focus on the business system docking blockchain platform, enabling rapid coverage across the industry. The information on financing and financing of trade information between enterprises in the supply chain, as well as the warehousing and logistics information involved in the trade process are all registered in the blockchain, and the information cannot be tampered with, ensuring the authenticity and effectiveness of the assets [14]. By accessing internal blockchain nodes, organizations can obtain complete transaction data and enhance credit collaboration between enterprises. This trustworthy value transmission system not only improves the financing ability of the demand side, but also improves the supplier's regulatory capabilities. The sensor is used to detect the logistics information, and the wireless communication network is used to send the trusted data to the blockchain verification node to ensure that the relevant conditions are automatically triggered when the contract condition is met, and the operation error is reduced [15]. In the field of accounts receivable, traditional accounts receivable are completed through offline transaction confirmation, and the existence of risks such as counterfeiting transactions and tampering with accounts receivable information reduces the trust of the trading participants. The whole process operation of accounts receivable is carried out through the blockchain platform, which realizes the full signature verification of accounts receivable transactions, and uses the intelligent contract to realize the authority and state control, making the accounts receivable more secure and controllable, and constructing A highly trusted trading platform [16]. There are a large number of participants in the accounts receivable transaction process, and the business is complex. In the face of financing applications for traditional accounts receivable, financial institutions need to conduct a large amount of trade background review. The blockchain platform records the life cycle of the entire accounts receivable through time-cutting, so that all market participants can see the flow of funds and information flow, eliminating the possibility of ticket fraud. Traditional accounts receivable have difficulties in circulation in the trading market due to mutual trust problems. The accounts receivable are stored and traded in the form of digital assets. The characteristics that are not easy to be lost and cannot be tampered with can make the new business model can be quickly promoted, reduce the cost of use while improving the efficiency of customer fund management, and form a mutual trust mechanism among different enterprises. This enables multiple financial ecosystems to interoperate and benefit through the blockchain platform, with good business value and broad development space [17]. In the bond trading industry, the bond business is a business that requires the participation of multiple organizations. In the process of its issuance, transaction, etc., the organizations need to synchronize and confirm the information through traditional mailing or message forwarding [18]. After using the blockchain technology, the system can ensure the synchronization and consistency of data by the bottom layer of the blockchain, and reduce the time, labor and capital costs of docking between different institutional systems. Moreover, many of the traditional centralized systems are enclosed within the organization, and it is impossible to timely and effectively supervise external systems. There will be blind spots in the supervision [19]. Using blockchain technology, regulators join blockchains in the form of nodes to monitor transactions on the blockchain in real time. Since the data of the blockchain is complete and unchangeable, any value exchange history can be tracked and inquired, and the process of bond transfer can be clearly viewed and controlled, thereby ensuring the security, validity and authenticity of bond transactions, and effectively preventing Market risk. At the same time, blockchain technology can avoid the work of third party reconciliation, thus effectively improving the liquidation efficiency of bond transactions [20]. In addition, the trading platform based on blockchain technology can realize real-time clearing of transactions between clearing banks and improve transaction efficiency [21]. Real-time disaster recovery is fault-tolerant. If a major fault occurs, the master node can be switched in seconds. The access point fails, and the historical data is quickly recovered through the built-in algorithm to avoid loss of transaction data. The member and the bank access terminal independently process the query, and the

data is synchronized in real time to alleviate the pressure on the master node. The supervisory node obtains relevant transaction data in real time, and the regulatory agency conducts real-time supervision of the transaction [22].

Through the discussion of the relevant applications of blockchain, blockchain technology can be used for the research of location information storage of IoT devices. In this paper, the positioning technology of equipment in the Internet of Things is discussed, and the key technologies of the blockchain are analyzed. The main research is on the related algorithms involved in the cryptography technology and distributed computing system architecture in the blockchain analysis. On this basis, the location chain storage system of IoT devices based on blockchain is designed and developed. The experimental results show that the system designed in this paper can meet the storage requirements of IoT device information, and can protect the user's location privacy, and realize location information sharing under security conditions. If applied to the actual situation, it will greatly promote the development of the Internet of Things.

2. Method

2.1. IoT device positioning

There is a variety of device information in the Internet of Things, and location information is information common to all devices. Therefore, how to locate the device becomes an important research content of the IoT perception layer. Positioning refers to the process of determining the location of a physical entity in a space–time reference system. The continuous development of positioning technology makes the application of the Internet of Things more life-oriented and popular. There are many types of positioning technologies. Due to different focus points, the required positioning performance is also different. Currently, there are two types of device positioning methods commonly used in the Internet of Things:

(1) Satellite-based positioning technology

The satellite-based positioning technology utilizes a global navigation satellite system to provide location services for user terminals. More commonly used is GPS. When positioning, the GPS first determines the time reference and obtains the propagation time of the electromagnetic wave from the satellite to the measured point, so as to obtain the distance from the satellite to the measured point [23]. The GPS receiver needs to know at least the position of the three satellites, and then use the point positioning principle to calculate the spatial position of the measured point, and finally correct the data.

(2) Network-based positioning technology

The network-based positioning technology can be further divided into a positioning based on a mobile communication network and a positioning based on a short-range wireless communication network. Mobile networks usually have devices such as base stations, access points, or coordinators. These devices can naturally serve as anchor points for the positioning system and provide reference points for the positioning of mobile terminals. At present, most mobile communication networks such as GSM, CDMA and 3G adopt a cellular network architecture, that is, the communication area in the network is divided into cells [24]. Generally, each cell has a corresponding base station, and the mobile device needs to access the network through the base station for communication. Therefore, when the mobile device performs mobile communication, the base station connected thereto can locate the location of the mobile device, which is based on mobile communication. The positioning of the network. In this positioning technique, as long as the spatial coordinates of at least three base stations and the distance between each base station and the mobile terminal are known, the position of the terminal can be calculated according to the time, angle or intensity of the signal arrival. Positioning based on wireless local area networks (WLAN or Wi-Fi) is an indoor positioning technology. In the field of wireless communication, the distinction between positioning in indoor and outdoor environments is quite obvious. In the open air environment, GPS can meet most of the needs of people. Even if it is lacking, it can be compensated by base station positioning. However, the GPS signal in the indoor environment will be blocked, and the signal of the base station positioning will be affected by the multipath effect. Positioning is not good, so indoor positioning is based on signal strength (RSS). The RSS-based positioning system does not require special equipment and can be located using a WLAN that has been erected [25].

In the positioning system, there are two physical and abstract descriptions of the location information of the device. The physical location information refers to specific location data of the object to be located, and the data should include information such as latitude, longitude, and altitude. The abstract location information is described as the location of the equipment located near a building. In real life, people often use abstract location information. Sometimes the location system needs to convert and map physical location information into abstract location information. The level of abstraction of location information required by different applications is also different. In the Internet of Things, the positioning performance of the positioning system can be evaluated from two indicators: positioning accuracy and positioning accuracy. The positioning accuracy refers to the proximity between the device position information and its real position, that is, the error between the measured value and the true value. Positioning accuracy is the credibility of the specified bit. Evaluating any aspect of the two in isolation does not make much sense. Therefore, when evaluating the performance of a positioning system, it is generally described that it can be positioned to a range of 10 m (positioning accuracy) with a probability of 95% (positioning accuracy). The higher the positioning accuracy, the lower the corresponding positioning accuracy, and vice versa, so it is usually necessary to make trade-offs between the two.

2.2. Blockchain cryptography

There is no supervision in the blockchain network. When transactions and blocks are spread across the network, how can data be protected from tampering and how the user identity is hidden in the blockchain public account. These problems can be solved by encryption. The following describes the encryption algorithm in the blockchain.

(1) Hash algorithm

With the continuous development of network applications, in addition to ensuring the confidentiality of information, information security must also ensure that information is not illegally altered during storage, use, and transmission, that is, the integrity of information. The hash algorithm can transform the input of "arbitrary length" to obtain a fixed-length output, also known as a message digest. The message digest can be used to complete the authentication function of the message, and message authentication is an important measure to ensure the integrity of the message. The following describes an implementation of the SHA256 algorithm, which is roughly divided into the following five steps:

Step 1: fill the plain text. The plaintext is filled in a fixed manner such that the number of bits in the plaintext (bits are the smallest unit of computer data storage, also referred to as bits) is a multiple of 512. For example, if an input plaintext is 112 bits long and less than 448 bits, then the first bit is padded with 1, followed by $448 - 1 - 112 = 335$ bits padding 0, and then a

64-bit unsigned integer is added to indicate plaintext padding. The length before. So there are $112 + 1 + 335 + 64 = 512$ bits. If the input plaintext length is greater than 448, such as 490, then the first digit is padded with 1, then the $960 - 1 - 490 = 469$ bit is padded with 0, and then a 64-bit unsigned integer is added to indicate the plaintext before filling length. So there are $490 + 1 + 469 + 64 = 1024$ bits.

Step 2: Parse the filled plaintext. The filled plaintext is parsed into N 512-bit packets.

Step 3: initialize the cache. Before the hash calculation, initialize 8 words of length 32 as the cache abcdefgh. Converting the final cache to a byte string or string is a message digest.

Step 4: the hash process. The SHA256 algorithm uses six kinds of logic functions to perform 64-step iterative operations on each 512-bit packet in plaintext. Each step takes the cache abcdefgh as input and then updates the cache. Each step in the calculation uses a constant K_i and a 32-bit word w_i. The six logical functions are as follows:

$$\mathrm{ch(x, y, z)} = (\mathrm{x}\hat{}\mathrm{y}) \oplus (\bar{z}\hat{}\mathrm{x})$$

$$\mathrm{maj(x, y, z)} = (\mathrm{x}\hat{}\mathrm{y}) \oplus (\mathrm{x}\hat{}\mathrm{z}) \oplus (\mathrm{y}\hat{}\mathrm{z})$$

$$\sum_{0}(x) = ROTR^{2}(x) \oplus ROTR^{13}(x) \oplus ROTR^{22}(x)$$

$$\sum_{1}(x) = ROTR^{6}(x) \oplus ROTR^{11}(x) \oplus ROTR^{25}(x)$$

$$\sigma_0 = ROTR^{7}(x) \oplus ROTR^{18}(x) \oplus SHR^{3}(x)$$

$$\sigma_1 = ROTR^{17}(x) \oplus ROTR^{19}(x) \oplus SHR^{10}(x)$$

Among them, $SHR^{n}(x)$ is defined as: $SHR^{n}(x) = x \gg n$, $ROTR^{n}(x)$ is defined as: $ROTR^{n}(x) = (x \gg n)|[x \gg (32 - n)]$
The hashing process is as follows:

Procedure 1: Generate an empty list w of length 64 for storing 64 words. The 512-bit plaintext is converted into 16 32-bit words and assigned to the first 16 elements of the list w, and then the last 48 elements of the list w are filled according to the following equation.

$$\sigma_0 = ROTR^{7}(w_{i-15}) \oplus ROTR^{18}(w_{i-15}) \oplus SHR^{3}(w_{i-15})$$

$$\sigma_1 = ROTR^{17}(w_{i-2}) \oplus ROTR^{19}(w_{i-2}) \oplus SHR^{10}(w_{i-2})$$

$$w_i = \sigma_0 + \sigma_0 = w_{i-16} + w_{i-7}$$

Among them, $15 \leq \mathrm{i} \leq 63$.
Procedure 1: Update the cache abedefgh.
for i ← 0 to 63 do

$$\sigma_0 = ROTR^{7}(w_{i-15}) \oplus ROTR^{18}(w_{i-15}) \oplus SHR^{3}(w_{i-15})$$

$$\sigma_1 = ROTR^{17}(w_{i-2}) \oplus ROTR^{19}(w_{i-2}) \oplus SHR^{10}(w_{i-2})$$

$$w_i = \sigma_0 + \sigma_0 = w_{i-16} + w_{i-7}$$

$$\sigma_0 = ROTR^{2}(a) \oplus ROTR^{13}(a) \oplus SHR^{22}(a)$$

$$\mathrm{maj(a, b, c)} = (\mathrm{a}\hat{}\mathrm{b}) \oplus (\mathrm{a}\hat{}\mathrm{c}) \oplus (\mathrm{b}\hat{}\mathrm{c})$$

$$T_2 = \sigma_0 + \mathrm{maj(a, b, c)}$$

$$\sigma_1 = ROTR^{6}(e) \oplus ROTR^{11}(e) \oplus SHR^{25}(e)$$

$$\mathrm{ch(e, f, g)} = (\mathrm{e}\hat{}\mathrm{f}) \oplus (\bar{e}\hat{}\mathrm{g})$$

$$T_1 = h + \sigma_1 + \mathrm{ch\,(e, f, g)} + K_i + w_i$$

Then there are: h = g, g = f, f = e, e = d + T_1, d = c, c = b, b = a, a = $T_1 + T_2$.

Step 5: The resulting cache abcdefgh is converted to a byte string or a string to obtain a message digest.

(2) Public key cryptography algorithm

The public key cryptography algorithm is based on mathematical problems rather than traditional replacement and replacement methods. The current public key cryptosystem relies mainly on two types of mathematical problems: large integer factorization and discrete logarithm.

The first type of public key cryptography algorithm is proposed by Rivest, Shamir, Adleman, referred to as RSA algorithm, and its security is based on the difficulty of large integer factorization. RSA algorithm is the most typical method in public key cryptography, and it is a research hotspot. For cryptographers, it is difficult to mathematically solve the problem of knowing that ciphertexts must be factored out in large numbers. The security of the second type of public key cryptography relies on the computational difficulty of discrete logarithms (DLP problem). Let G be a finite Abel addition group, assuming g is a generator of G, a is an arbitrary integer. If g and g^a are known, how to find the integer a is mathematically called discrete logarithm problem. In general, when group G is properly selected and the integer a is sufficiently large, it is very difficult to solve such problems. Through different choices of group G, various public key cryptographic algorithms can be constructed. The elliptic curve public key cryptography algorithm is based on the computational difficulty of the discrete logarithm of the point of the elliptic curve. The elliptic curve cryptography algorithm uses an elliptic curve constructed on a finite Abel group (GF(p) or GF(2^m)). Note that the points obtained by adding the points on the two elliptic curves are still on the original elliptic curve. If P is a point on the elliptic curve, in the equation kP = P + ⋯ + P = Q, k and point P are known. It is quite easy to find the point Q. On the contrary, it is quite difficult to know the point Q and the point P to find k. The elliptic curve cryptosystem is designed using this difficult problem. For example, use Q as the public key and k as the private key.

2.3. Distributed consistency

Blockchain is an innovative application mode of computer technology in the era of Internet, such as distributed data storage, point-to-point transmission, its knowledge mechanism, and encryption algorithm. Distributed computing is the foundation of blockchain technology, and consistency is a fundamental problem in distributed systems. If a distributed cluster cannot guarantee the consistency of the processing results, then any business system built on it will not work properly. This section studies distributed computing and consistency as the basis for IoT device location information storage systems based on blockchain technology.

(1) Distributed computing system architecture

A distributed system consists of several separate computers that work together and are like a single system to the user. Its main characteristics are: the difference between various computers and the way of communication between computers is hidden from the user. Similarly, the user does not see the internal organization structure of the distributed system; users and applications whenever and where the ground can interact with distributed systems in a consistent and unified manner. The structure of a distributed system makes it easier to integrate various applications running on different computers into one system. The existing distributed system architecture can be divided into: client/server architecture, distributed object architecture, peer-to-peer network architecture, service-oriented architecture, and the like. This article focuses on the client/server architecture.

In a distributed system with a client/server architecture, processes can be divided into two groups: client and server. A client is a process that requests a service from a server. It sends a request to the server and then waits for a response from the server. The server is a process that implements a particular service, such as a file system service or a database service. A major problem with this architecture is how to clearly distinguish between the client and the server, and sometimes the boundaries between

the server and the client are blurred. The client and server can be distinguished from the three logical levels of user interface layer, processing layer and data layer. The user interface layer consists of a program that allows the end user to interact with the application. The user interface layer is generally implemented by the client; the processing layer is composed of applications; the data layer is used to maintain the actual data manipulated by the application, and it is used by the database. Or file system composition, generally implemented on the server side. In addition to data storage, the data layer is responsible for maintaining data consistency between different applications. These three logical levels of partitioning enable physical distribution of client/server applications to multiple machines.

(2) Distributed Consistency Algorithm

In the distributed consistency algorithm of blockchain, Paxos algorithm is widely used due to its simplicity. The Paxos algorithm is an algorithm that optimizes the availability to the limit under the premise of ensuring strong consistency. Any message in Paxos execution can be lost, and its consistency guarantee does not depend on the success of a particular message. The earth simplifies the design of distributed systems and closely matches the characteristics of possible network partitions in a distributed environment. The Paxos algorithm compares each data write request to a proposal. Each proposal has a separate number. The proposal is forwarded to the submitter for submission. The proposal must go through f+1 nodes in 2f+1 nodes. Acceptance will take effect. The 2f+1 nodes are called the voting committee for this proposal. The nodes in the voting committee are called acceptors. The execution flow of the Paxos algorithm can be divided into two phases:

The first stage: the proposer sends a prepare message to more than half of the acceptors in the network, and the acceptor normally has the same promise message.

The second stage: When receiving more than half of the acceptor reply promise message, the proposer sends an accept message, and the acceptor replies to the accepted message under normal circumstances.

The Paxos algorithm states that as long as f+1 nodes of 2f+1 nodes in the system are available, the system as a whole is available, and the data is guaranteed to be strong, which is great for usability improvement.

2.4. Overall system design

The IoT device location information storage system based on blockchain technology can be divided into three modules, namely, a client module, a blockchain storage module and a service provider module. The system function module diagram is shown in Fig. 1. The following describes the functional modules to which these three modules belong.

(1) Device initialization function, node initialization function and service provider identity initialization function. A unique public–private key pair is added to the new device by an asymmetric encryption algorithm, and the public key is used to identify the device identity. This initialization is required when the device is first used because the location information of all devices in the entire blockchain network is bound to the corresponding public key. The device's public key and location data need to be written to the blockchain block at the same time, and the ownership of the data is verified by the private key.

(2) Device location data collection function. Device location data is the most basic content of the entire system. At present, most IoT devices have built-in positioning chips, which can conveniently provide positioning services for users. Even if the IoT device does not have its own positioning sensor, the user can easily obtain the positioning data by configuring related hardware devices (such as a USB locator).

(3) Formatting the device side location information. After collecting location information, the device needs to bind the information to its identity. If you share with others, you need to specify a shared object. The location information is formatted for the rational use of subsequent location information.

(4) Database storage and query functions. The system is based on a traditional database. The database is the basic service of the whole system, and the classification and storage of different behaviors are completed by creating different data tables. The query function is to complete the verification and statistics of the behavior data. Each node's database has a complete backup of the contents of the entire system.

(5) Device information transmission function. Device information transmission function. IoT devices have limited computing and storage capabilities, so location information needs to be transmitted to one node in a distributed network, and location information is tiled in the blockchain network.

(6) Constructing the function of the creation block. The creation block is the first block of the blockchain. It has no practical meaning, just for the continuity of the subsequent operations. All the blocks are connected in order with the creation block as the starting point.

(7) Building asset block functions. The asset block contains the location information related content, and the building block is to ensure that the location information in the block cannot be falsified.

(8) Block voting function. All nodes in the blockchain network need to vote on the new block, complete the rationality verification of the new block, and ensure the "distributed consensus" within the entire network.

(9) Querying the historical location information of the device. The device can only query the location information bound to its own public key, and does not have the permission to obtain the location data of other devices, ensuring the isolation and security of data between devices.

(10) Real-time location query by the service provider. The service provider can only query the location information bound to its own public key, which is provided by the device in a shared form, so this information also has the device's public key information. After obtaining the location information, the service provider filters the query results based on the public key and the request time of the device to obtain device location information of the service.

3. Experiment

According to the key technology of the blockchain studied above and the designed IoT device location information storage system, the performance of the system designed in this paper is verified by carrying hardware devices and setting the development environment.

3.1. Hardware equipment

The hardware devices used in the experimental part of this paper mainly include physical host and Raspberry Pi development tools. The roles of the two physical hosts are as follows: one physical host deploys a three-node pseudo-distributed blockchain network based on the virtual machine, and the other physical host is used to simulate the service provider end to obtain the shared location of the IoT device information. The Raspberry Pi is the size of a credit card, and basically has the function of a computer. Therefore, it is also called a "micro PC". The Raspberry Pi development board is shown in Fig. 2. Connecting the GPS module development board to the Raspberry Pi development board constitutes a simple IoT device that can be used to collect location information of the device.

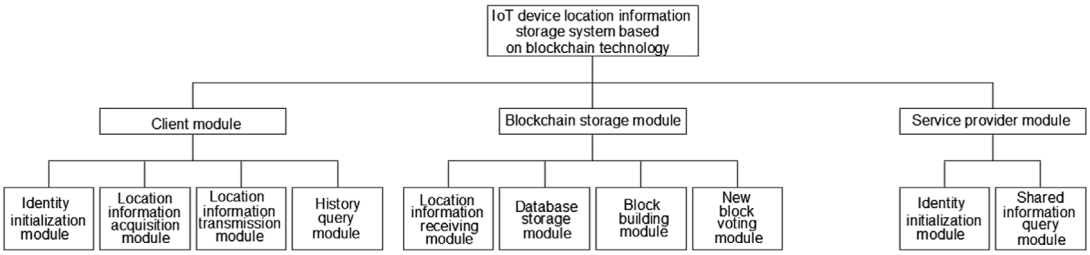


Fig. 1. System function module.

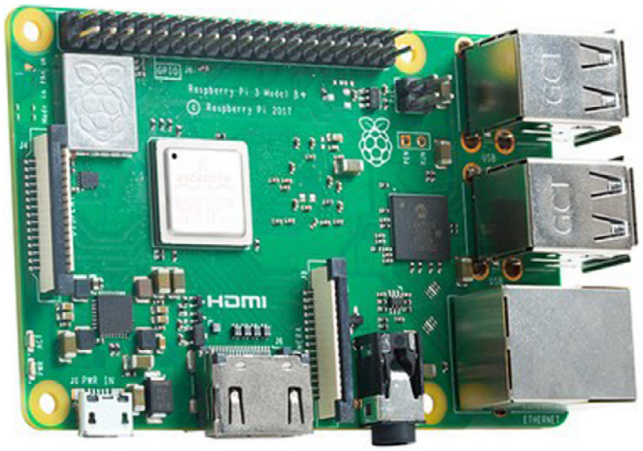


Fig. 2. Raspberry Pi development board.

3.2. Development environment

The operating system of the hardware device selected in this paper is Ubuntu16.06. Using MongoDB as the underlying database, the blockchain-related services and interactive interfaces are developed based on the Python language. MongoDB is a distributed file storage-based database written in the C++ language. Python is an object-oriented, interpreted computer programming language.

The distributed blockchain storage system is built by using the ansible automated operation and maintenance tool, so that each node blockchain service is connected with the MongoDB database of other nodes to ensure the synchronization of the three node databases. The interaction process in this structure includes:

(1) The Raspberry Pi hardware selects a node in the blockchain network to perform SOCKET communication, and performs location information uploading and history query operation.

(2) The Raspberry Pi hardware communicates with the service provider to exchange the public key information of the two.

(3) The service provider initiates a request to the blockchain network to query specific device location information.

3.3. Experimental procedure

First, the device location information storage system is initialized, including initialization of devices, nodes, and service provider identities. After the relevant initialization work is completed, the location information collection can be started to obtain accurate device location information. After obtaining the location information, the storage system begins to form a blockchain, which includes the generation of transaction behavior, construction of blocks, and the like. Finally, the location information query includes device-side location information query and service provider shared location information query.

After the verification of the system function is completed, the delay performance of the system is also verified. By setting different maximum transaction volume numbers (MAX_NUM), the delays generated by the three processes of transaction behavior generation, block generation, and block voting are calculated when the number of transaction behaviors is 500, 1000, and 2000 respectively.

4. Results and discussion

4.1. System function verification

(1) Related initialization

Identity information generation is a prerequisite for the operation of the entire system. In the identity initialization experiment, the storage system prevents the identity information from being tampered with or repeatedly generated by writing text, which ensures the uniqueness and permanence of the identity information. After starting the MongoDB service, the system creates the location_info database, and creates blocks, transactions, votes tables, and related secondary indexes in the database, which facilitates subsequent information query. Blockchain service initialization involves building a creation block of blockchains. After the system creates the creation zone, it starts the block, voter, and other processes. It can detect the update of the current blockchain status at the same time, and open its own node address and connection service of the specific interface to the whole network.

(2) Equipment location information collection

After the gspd service is started, the storage system uses the Python development libraries serial2 and pymnea2 to retrieve and parse the GPS data. After analyzing the obtained data, the exact information such as time, latitude value, latitude direction, longitude value and longitude direction is obtained, and the accurate location information of the device is realized.

(3) Formation of blockchain

After the system forms a transaction behavior and sends it to the blockchain node, the blockchain service allocates a certain amount of transaction behavior to a node in the blockchain network within a timeout period, and packages the transaction behavior into blocks. Then the whole network voted on the new block to confirm the legitimacy of the new block. This marks the successful formation of a blockchain in the storage system.

(4) Location information inquiry

After extracting the device public key and private key stored in the local file system, the device signs a piece of plaintext information with its own private key, and finally sends the device public key, plaintext, and signature information to the blockchain

Table 1
System delay statistics at MAX_NUM = 500.

Test group	Number of trading activities	Trading behavior time	Block generation time	Block voting time
Group 1	500	5.67 s	0.16 s	2.12 s
Group 2	1000	6.24 s	0.14 s	2.31 s
Group 3	2000	9.37 s	0.17 s	2.18 s

Table 2
System delay statistics at MAX_NUM = 1000.

Test group	Number of trading activities	Trading behavior time	Block generation time	Block voting time
Group 1	500	5.18 s	0.14 s	2.11 s
Group 2	1000	5.22 s	0.13 s	2.21 s
Group 3	2000	8.36 s	0.16 s	2.17 s

network. The blockchain network verifies the authenticity of the device identity by verifying that the device public key, plaintext, and signature information match. The same authentication mechanism is followed when the service provider queries for specific device location information. This indicates that the storage system realizes location information sharing under the premise of ensuring security.

4.2. System performance analysis

Tables 1 and 2 are experimental data when MAX_NUM is 500 and 1000, respectively. It can be seen from Tables 1 and 2 that when the number of transactions does not exceed the maximum limit, there will be no excessive delay in the three processes of transaction generation, block generation, and block voting; if the number of transactions exceeds the maximum limit, There will be a significant delay in the generation of trading behavior, and the greater the excess, the greater the delay. In addition, as can be seen from the data in the table, whether the number of transactions exceeds the maximum limit has little effect on the two processes of block generation and block voting.

5. Conclusion

In recent years, with the reform and innovation of technology, the Internet of Things technology has become an important means for many industries to obtain "secondary development". However, the security of device location information in the Internet of Things has greatly restricted the further development of the Internet of Things. In this paper, based on the objective analysis of the existing research, this paper proposes to apply the blockchain technology to the device location information processing in the Internet of Things. After analyzing and researching the key technologies of blockchain, the location information storage system of IoT devices based on blockchain technology is designed. Experiments show that the storage system designed in this paper effectively solves the security problem of device location information in the Internet of Things, and realizes location information sharing under the premise of ensuring that user privacy is not leaked. In addition, this paper also analyzes the delay problem of the system through relevant experiments, which is of guiding significance for the practical application of the system.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

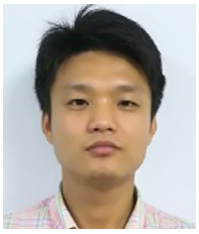
Acknowledgments

This work was supported by the Key Technology Research Program of the Higher Education Institutes of Henan Province, China (Grant No. 18B580002 and 20B430008); the Key Science and Technology Program of Henan Province, China (Grant No. 162102210272).

References

[1] Jie Gao, Research on key technologies of internet of things based on RFID technology, Jiangxi Commun. Sci. Technol. (1) (2018).
[2] Jun Tan, Focus on IoT Security Don't let your device be vulnerable, Comput. Netw. 44 (577(9)) (2018) 53–54.
[3] Meng Zhang, Analysis of industrial IoT security risk and countermeasures, China Ind. Rev. (4) (2017) 42–50.
[4] Anonymous, Application of blockchain in IoT privacy protection, Logist. Technol. 37 (7) (2018) 39–44+139.
[5] L. Lightfoot, Y. Li, J. Ren, Preserving source-location privacy in wireless sensor network using STaR routing, in: Global Telecommunications Conference, 2010 IEEE, IEEE, 2010, pp. 1–5.
[6] L. Yao, L. Kang, P. Shang, et al., Protecting the sink location privacy in wireless sensor networks, Pers. Ubiquitous Comput. 17 (5) (2013) 883–893.
[7] M. Shao, Y. Yang, S. Zhu, B. Urgaonkar, Towards statistically strong source anonymity for sensor networks, ACM Trans. Sensor Netw. 9 (3) (2013) 34.
[8] T. Shu, Y. Chen, J. Yang, et al., Multi-lateral privacy-preserving localization in pervasive environments, in: IEEE INFOCOM 2014-IEEE Conference on Computer Communications, IEEE, 2014, pp. 2319–2327.
[9] J. Shao, R. Lu, X. Lin, FINE: A fine-grained privacy-preserving location-based service framework for mobile devices, in: IEEE INFOCOM, IEEE, 2014, pp. 244–252.
[10] H. Chen, W. Lou, On protecting end-to-end location privacy against local eavesdropper in wireless sensor networks, Pervasive Mob. Comput. 16 (2015) 36–50.
[11] Juan Chen, Binxing Fang, Lihua Yin, et al., Source location privacy protection protocol based on source node finite flooding in sensor networks, Chinese J. Comput. 33 (09) (2016) 1736–1747.
[12] Leqiang Bai, Ling Li, Shiguang Qian, et al., Source location privacy protection algorithm for wireless sensor networks based on elliptic model, Control Decis. 32 (02) (2017) 255–261.
[13] Yingchen Su, Blockchain technology behind bitcoin, Sci. Technol. Econom. Guide (29) (2017) 134.
[14] Wei Lin, Hong Lin, Research on the influence of blockchain on online supply chain finance, J. Inn. Mong. Univ. Finance Econom. (5) (2017) 11–14.
[15] Yan Zhu, Guohua Gan, Di Deng, et al., Security research in key technologies of blockchain, Inform. Secur. Res. 2 (12) (2016) 1090–1097.
[16] Shengqi Wang, On the risk control of enterprise receivables, China Mark. (7) (2018) 167–168.
[17] Haosi Meng, The enlightenment of blockchain technology to receiving funds financing service platform, North. Finance (10) (2017) 30–33.
[18] Qiong Lu, Risk identification and econometric analysis of bond business, Finance Account. (19) (2017) 223–224.
[19] Shuo Bai, Blockchain technology and its application, Bond (71(5)) (2018) 83–87.
[20] Shenghui Wen, Research on the application prospect of blockchain in asset securitization, Bond (3) (2018) 56–60.
[21] Lili Yang, Rongrong Wang, Lin Lu, Application research of blockchain technology in equity trading platform, Times Finance (30) (2017) 124.

[22] Chunwei Ren, Qingjiang Meng, Blockchain and securities clearing and settlement, China Finance (05) (2017) 63–64.
[23] Yinxiang Chen, Jun Zhang, Xiang Liu, Application of GPS in satellite tracking (SST) technology, Fire Control Radar Technol. 46 (2) (2017) 15–21.
[24] Jingjing Zhang, Ruijuan Sun, China mobile communication technology, Green Build. Mater. (4) (2018) 249–250.
[25] Wenzhao Yu, A research method of WIFI indoor positioning based on RSS, Sci. Technol. Vis. (230(8)) (2018) 279–282.



Defeng Li was born in Xinxiang, Henan Province, P.R. China, in 1984. He completed his doctorate at the Harbin Institute of Technology. Now, he works in the school of mechanical and electrical engineering, Henan Agricultural University. His research interests includes intelligent transportation systems and polymer composite.
E-mail: defeng.li@henau.edu.cn.

Yuan Hu, Ph.D. is a senior lecturer in the school of mechanical and electrical engineering, Henan Agricultural University. He completed his doctorate at the University of Pittsburgh. His research work includes intelligent transportation systems, computational intelligence and visual computing. He earned his master of science in civil engineering at the University of Pittsburgh in 2014 and his bachelor of science in engineering from the North China University of Water Resources and Electric Power in 2012.
E-mail: huyuan@henau.edu.cn.

Mingming Lan, Ph.D. was born in Zhengzhou, Henan Province, P.R. China, in 1984. He completed his doctorate at the Beihang University. His research work includes intelligent manufacturing systems and Bio manufacturing technology.
E-mail: lanming@henau.edu.cn.